AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

S. HRG. 112–857

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 10, 2011

Serial No. J–112–19

Printed for the use of the Committee on the Judiciary

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

S. HRG. 112–857

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

HEARING

BEFORE THE

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

OF THE

COMMITTEE ON THE JUDICIARY
UNITED STATES SENATE

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

MAY 10, 2011

Serial No. J–112–19

Printed for the use of the Committee on the Judiciary

U.S. GOVERNMENT PRINTING OFFICE

86–775 PDF WASHINGTON : 2011

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

PATRICK J. LEAHY, Vermont, *Chairman*

HERB KOHL, Wisconsin
DIANNE FEINSTEIN, California
CHUCK SCHUMER, New York
DICK DURBIN, Illinois
SHELDON WHITEHOUSE, Rhode Island
AMY KLOBUCHAR, Minnesota
AL FRANKEN, Minnesota
CHRISTOPHER A. COONS, Delaware
RICHARD BLUMENTHAL, Connecticut

CHUCK GRASSLEY, Iowa
ORRIN G. HATCH, Utah
JON KYL, Arizona
JEFF SESSIONS, Alabama
LINDSEY GRAHAM, South Carolina
JOHN CORNYN, Texas
MICHAEL S. LEE, Utah
TOM COBURN, Oklahoma

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN DAVIS, *Republican Chief Counsel and Staff Director*

SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

AL FRANKEN, Minnesota, *Chairman*

CHUCK SCHUMER, New York
SHELDON WHITEHOUSE, Rhode Island
RICHARD BLUMENTHAL, Connecticut

TOM COBURN, Oklahoma
ORRIN G. HATCH, Utah
LINDSEY GRAHAM, South Carolina

ALVARO BEDOYA, *Democratic Chief Counsel*
ELIZABETH HAYS, *Republican General Counsel*

CONTENTS

STATEMENTS OF COMMITTEE MEMBERS

	Page
Witness List	49
Franken, Hon. Al, a U.S. Senator from the State of Minnesota	1
Leahy, Hon. Patrick J., a U.S. Senator from the State of Vermont	1
prepared statement	51
Coburn, Hon. Tom, a U.S. Senator from the State of Okahoma	5

WITNESSES

Rich, Jessica, Deputy Director, Bureau of Consumer Protecion, Federal Trade Commission, Washington, DC	6
prepared statement	54
Weinstein, Jason, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, Washington, DC	8
prepared statement	66
Soltani, Ashkan, Independent Privacy Researcher and Consultant, Washington, DC	21
prepared statement	99
Brookman, Justin, Director, Project on Consumer Privacy, Center for Democracy and Technology, Washington, DC	23
prepared statement	80
Tribble, Guy "Bud," M.D., Ph.D., Vice President of Software, Technology, Apple Inc., Cupertino, California	25
prepared statement	112
Davidson, Alan, Director of Public Policy, Google Inc., Washington, DC	27
prepared statement	90
Zuck, Jonathan, President, The Association for Competitive Technology, Washington, DC	28
prepared statement	125

QUESTIONS FROM HON. AL FRANKEN, HON. RICHARD BLUMENTHAL, AND HON. TOM COBURN

Questions from Hon. Al Franken to Alan Davidson and Guy "Bud" Tribble	143
Questions from Hon. Richard Blumenthal to Justin Brookman, Alan Davidson, Ashkan Soltani, and Guy "Bud" Tribble	146
Questions from Hon. Tom Coburn to Alan Davidson and Guy "Bud" Tribble	156

QUESTIONS AND ANSWERS

Responses of Justin Brookman to questions submitted by Senator Blumenthal	158
Responses of Alan Davidson to questions submitted by Senators Blumenthal, Coburn and Franken	163
Responses of Ashkan Soltani to questions submitted by Senator Blumenthal	180
Responses of Jessica Rich to questions submitted by Senator Coburn	182
Responses of Guy "Bud" Tribble to questions submitted by Senators Franken, Coburn and Blumenthal	185

MISCELLANEOUS SUBMISSIONS FOR THE RECORD

Baker, James A., Associate Deputy Attorney General, Department of Justice, Washington, DC, statement	210

Page

Franken, Hon. Al, a U.S. Senator from the State of Minnesota, and Hon. Richard Blumenthal, a U.S. Senator from the State of Connecticut, joint letter (April 12, 2011) 223
Franken, Hon. Al, a U.S. Senator from the State of Minnesota: Letter to Mr. Steve Jobs (Apple; April 20, 2011) 224
American Civil Liberties Union (ACLU), Laura W. Murphy, Director, Washington Legislative Office; Christopher Calabrese, Legislative Counsel, Washington Legislative Office and Catherine Crump, Staff Attorney, Speech, Privacy and Technology Project, Washington, DC, statement 226
Additional Documents from Hon. Al Franken, Incorporated by Reference into the Record 237
arstechnica.com, Chris Foresman, article: "Android phones keep location cache, too, but it's harder to access," May 17, 2011 238
Apple App Store Review Guidelines for Hon. Al Franken 240
Apple's July 12, 2010, letter to the Hon. Edward J. Markey and the Hon. Joe Barton from Bruce Sewell, General Counsel and Senior Vice President of Legal and Government Affairs 257
Apple's May 6, 2011, letter to the Hon. Al Franken from Bruce Sewell, General Counsel and Senior Vice President of Legal and Government Affairs 270
cnet.com, Declan McCullagh, April 22, 2011, article: "Android data tied to users? Some say yes" 281
Department of Justice, Prosecuting Computer Crimes, Michael Battle, Director, EOUSA and Michael W. Bailie, Director, OLE, reports 285
Department of Justice, Cybercrime Manual 310
Bureau of Justice Statistics Special Report: "Stalking Victimization in the United States," by Katrina Baum, Ph.D.; Shannan Catalano, Ph.D.; and Michael Rand, January 2009 334
zwillgenblog.com, April 27, 2011 article: "Are Smartphones Making Stakeouts a Thing of the Past?" 350
Wall Street Journal, *WSJ.com*, April 5, 2011, article: "Mobile-App Makers Face U.S. Privacy Investigation" 352
National Center for Victims of Crime, Mai Fernandez, Executive Director, Washington, DC, statement 355
Wall Street Journal, *WSJ.com*, November 19, 2010, article: "Insurers Test Data Profiles to Identify Risky Clients" 377
IPhone Software Agreement 382
Wall Street Journal, *WSJ.com*, April 25, 2011, article: "IPhone Stored Location in Test Even if Disabled" 387
Oreilly.com, April 27, 2011, article: "Got an iPhone or 3G iPad? Apple Is Recording Your Moves" 389
Department of Justice, Office of Legislative Affairs, Lanny A. Breuer, Assistant Attorney General, Washington, DC, May 9, 2011, letter to Hon. Al Franken 391
Levinson, Alex; article posted April 21, 2011 at *wordpress.com*: "3 Major Issues with the Latest iPhone Tracking 'Discovery'" 394
Pcmag.com, April 27, 2011, article: "Most Mobile Apps Lack Privacy Policies: Study" 399
National Network to End Domestic Violence with the Minnesota Coalition for Battered Women, Washington, DC, statement 401
nielsen.com, April 21, 2011, article: "Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location" 408
Wall Street Journal, *WSJ.com*, December 19, 2010, article: "How One App Sees Location Without Asking" 413
Wall Street Journal, *WSJ.com*, August 3, 2010, article: "Stalkers Exploit Cellphone GPS" 415
Washington Post, *Washingtonpost.com*, May 8, 2011, article: "Parting with Privacy with a Quick Click" 421
Google; patent application publication by Youssef, et al. 425
Wired.com, April 25, 2011, article: "iPhone's Location-Data Collection Can't Be Turned Off" 486
Wall Street Journal, *WSJ.com*, April 26, 2011, article "The Unique ID Android Uses in Collecting Location" 489
Wall Street Journal, *WSJ.com*, April 22, 2011, article: "Apple, Google Collect User Data" 490
Wall Street Journal, *WSJ.com*, December 17, 2010, article: "Your Apps Are Watching You" 494

Page

ADDITIONAL SUBMISSIONS FOR THE RECORD

Submissions for the record not printed due to voluminous nature, previously printed by an agency of the Federal Government, or other criteria determined by the Committee, list: 500

http://info.publicintelligence.net/GoogleWiFiSpy.pdf 500

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

TUESDAY, MAY 10, 2011

U.S. SENATE,
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY, AND THE LAW,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 10:08 a.m., in Room SD–226, Dirksen Senate Office Building, Hon. Al Franken, Chairman of the Subcommittee, presiding.

Present: Senators Franken, Leahy, Schumer, Whitehouse, Blumenthal, and Coburn.

OPENING STATEMENT OF HON. AL FRANKEN, A U.S. SENATOR FROM THE STATE OF MINNESOTA

Senator FRANKEN. This hearing will come to order, and it is my pleasure to welcome all of you to the first hearing of the Senate Judiciary Subcommittee on Privacy, Technology, and the Law. I am sorry that everyone was not able to get into the room, into the hearing room, but we are streaming live on C–SPAN, thankfully, and we thank C–SPAN for that.

I would like to turn it over to Chairman Leahy and thank you, sir, for creating this Subcommittee and giving me the opportunity to lead it.

The Chairman has a long track record on protecting privacy, and I am honored to join him in this effort.

Mr. Chairman.

STATEMENT OF HON. PATRICK J. LEAHY, A U.S. SENATOR FROM THE STATE OF VERMONT

Chairman LEAHY. Well, thank you, Senator Franken, and I want to commend you for holding what is a very timely hearing on the privacy implications of smartphones and other mobile applications.

This is actually the first hearing for the new Subcommittee on Privacy, Technology, and the Law, and so I thank Senator Franken for his dedicated leadership on consumer privacy issues as Chairman of the Subcommittee. And I thank Dr. Coburn for his commitment to such issues, too, and I appreciate the both of them working together on this.

Throughout the three decades I have been in the Senate, I have worked to safeguard the privacy rights of all Americans. Ensuring that our Federal privacy laws accomplish this goal—while at the

same time addressing the needs of both law enforcement and America's vital technology industry—has been one of my highest priorities as Chairman of the Senate Judiciary Committee. That is why I decided to establish this new Privacy Subcommittee and was delighted when Senator Franken said he would be willing to chair it. It is also why I am working to update the Electronic Communications Privacy Act—ECPA.

Now, the digital age can do some wonderful, wonderful things for all of us, but at the same time, American consumers and businesses face threats to privacy like no time before. With the explosion of new technologies, such as social networking sites, smartphones, and other mobile applications, there are, of course, many new benefits to consumers. But there are also many new risks to their privacy.

Like many Americans, and certainly in Vermont where we cherish our privacy, I am deeply concerned about the recent reports that the Apple iPhone, Google Android phone, and other mobile applications may be collecting, storing, and tracking user location data without the user's consent. I am also concerned about reports that this sensitive location information may be maintained in an unencrypted format, making the information vulnerable to cyber thieves and other criminals.

In an interview this morning, I heard somebody from the industry speaking about how this can be a very valuable thing to them, being able to sell information to various industries for advertising purposes and the amount of money they may make on that. Of course, they are charging the consumer for the use of the phones, and they will then make money from that. When I raised that point, they said they can make them aware of products that might be in the location they go. I said, "Great, we all love to get a whole lot more unsolicited ads." So it is more of a one-way street, I think.

A recent survey commissioned by the privacy firm TRUSTe found that 38 percent of American smartphone users surveyed identified privacy as their No. 1 concern with using mobile applications.

And they have good reason to be concerned. The collection, the use, and the storage of location and other sensitive personal information has serious implications regarding the privacy rights and personal safety of American consumers.

This hearing provides a good opportunity for us to talk about this and examine these pressing privacy issues and to learn more about it. I am pleased that representatives from the Department of Justice and the Federal Trade Commission are here to discuss the administration's views on the privacy implications. I am also pleased that representatives from Google and Apple will address the privacy implications of their smartphones, their tablets, and other mobile applications.

And I welcome the bipartisan support on the Committee for examining these important consumer privacy issues, and I look forward to a productive discussion.

Again, Senator Franken and Senator Coburn, I thank you both for holding this hearing.

Senator FRANKEN. Well, thank you again, Mr. Chairman, for this opportunity. I really want to just express my pleasure in working with the Ranking Member of this Committee, Senator Coburn, and

thank you for your friendship and for working on these critical issues.

Now, before we turn to the business of today's hearing, I want to take a moment to explain what I think the Subcommittee is about and where we are headed. To me, this Subcommittee is about addressing a fundamental shift that we have seen in the past 40 or 50 years in who has our information and what they are doing with it.

When I was growing up, when people talked about protecting their privacy, they talked about protecting it from the Government. They talked about unreasonable searches and seizures, about keeping the Government out of our families, out of our bedrooms. They talked about "is the Government trying to keep tabs on the books I read and the rallies I attend."

We still have to protect ourselves from Government abuses, and that is a big part of the digital privacy debate. But now we also have relationships with large corporations that are obtaining and storing increasingly large amounts of our information. And we have seen the growth of this whole other sphere of private entities whose entire purpose is to collect and aggregate information about each of us.

While we are familiar with some of these entities, the average person is not remotely aware of most of them. I bet that two months ago if you stopped a hundred people on the street and asked them, "Have you ever heard of Epsilon?" one hundred of them would have said no. I certainly had not. But suddenly, when people started getting emails in their box telling them, "Your information has been compromised," you bet they wanted to know who Epsilon was.

Now, do not get me wrong. The existence of this business model is not a bad thing. In fact, it is usually a great thing. I love that I can use Google Maps—for free, no less—and the same for the app on my iPad that tells me the weather. But I think there is a balance we need to strike, and this means we are beginning to change the way we think about privacy to account for the massive shift of our personal information into the hands of the private sector, because the Fourth Amendment does not apply to corporations; the Freedom of Information Act does not apply to Silicon Valley. And while businesses may do a lot of things better than the Government, our Government is at least, by definition, directly accountable to the American people.

Let me put it this way: If it came out that the DMV was creating a detailed file on every single trip you had taken in the past year, do you think they could go one whole week without answering a single question from a reporter?

Now, this is not a new trend, and I am hardly the first person to notice it. Twenty-five years ago, a Senator named Patrick Leahy wrote and passed a law called the Electronic Communications Privacy Act, which talked a lot about government but which also contained commercial disclosure provisions. In 1996, Congress passed a law protecting the privacy of medical records. In 1998, we passed a law protecting children's privacy, and in 1999, we passed a law protecting financial records. So we have some protections here and

there, but we are not even close to protecting all of the information that we need to.

I believe that consumers have a fundamental right to know what data is being collected about them. I also believe they have a right to decide whether they want to share that information and with whom they want to share it and when. I think we have those rights for all of our personal information.

My goal for this Subcommittee is to help Members understand the benefits and privacy implications of new technology, to educate the public, to raise awareness, and, if necessary, to legislate and make sure that our privacy protections are keeping up with our technology.

Now, today in this hearing we are looking at a specific kind of really sensitive information that I do not think we are doing enough to protect, and that is data from mobile devices: smartphones, tablets, and cell phones. This technology gives us incredible benefits. Let me say that. Let me repeat that. This technology gives us incredible benefits. It allows parents to see their kids and wish them good night even when they are halfway around the world. It allows a lost driver to get directions, and it allows emergency responders to locate a crash victim in a matter of seconds.

But the same information that allows those responders to locate us when we are in trouble is not necessarily information all of us want to share all the time with the entire world. And yet reports suggest that the information on our mobile devices is not being protected in the way that it should be.

In December, an investigation by the Wall Street Journal into 101 popular apps for iPhone and Android smartphones found that 47 of those apps transmitted the smartphones' location to third-party companies, and that most of them did this without their user's consent.

Three weeks ago, security researchers discovered that iPhones and iPads running Apple's latest operating system were gathering information about users' locations up to a hundred times a day and storing that information on the phone or tablet and copying it to every computer that the device is synced to.

Soon after that, the American public also learned that both iPhones and Android phones were automatically collecting certain location information from users' phones and sending it back to Apple and Google, even when people were not using locating applications.

In each of these cases, most users had no idea what was happening, and in many of these cases, once users learned about it, they had no way to stop it. These breaches of privacy can have real consequences for real people.

A Justice Department report based on 2006 data shows that each year over 26,000 adults are stalked through the use of GPS devices, including GPS devices on mobile phones. That is from 2006 when there were a third as many smartphones as there are today. And when I sent a letter to Apple to ask the company about its logging of users' locations, the first group to reach out to my office was the Minnesota Coalition for Battered Women. They asked, "How can we help? Because we see case after case where a stalker or an abu-

sive spouse has used the technology on mobile phones to stalk or harass their victims."

But it is not just stalking. I think today's hearing will show that there is a range of harms that can come from privacy breaches, and there is also the simple fact that Americans want stronger protections for this information.

But as I have started to look into these issues in greater depth, I have realized that our Federal laws do far too little to protect this information. Prosecutors bringing cases under the Federal anti-hacking law often rely on breaches of privacy policy to make their case, but many mobile apps do not have privacy policies, and some policies are so long and complicated that they are almost universally dismissed before being read.

In fact, once the maker of a mobile app, a company like Apple or Google or even your wireless company, gets your location information, in many cases under current Federal law these companies are free to disclose your location information and other sensitive information to almost anyone they please without letting you know. And then the companies they share your information with can share and sell it to yet others—again, without letting you know.

This is a problem. It is a serious problem. And I think that is something the American people should be aware of, and I think it is a problem we should be looking at.

Before I turn it over to the distinguished Ranking Member, I just wanted to be clear that the answer to this problem is not ending location-based services. No one up here wants to stop Apple or Google from producing their products or doing the incredible things that you do. And I thank you for testifying. You guys are brilliant. When people think of the word "brilliant," they think of the people that founded and run your companies. No. What today is about is trying to find a balance between all of those wonderful benefits and the public's right to privacy. And I, for one, think that is doable.

Now I will turn the floor over to my friend, the Ranking Member, Senator Coburn, for his opening remarks.

[The prepared statement of Senator Leahy appears as a submission for the record.]

STATEMENT OF HON. TOM COBURN, A U.S. SENATOR FROM THE STATE OF OKLAHOMA

Senator COBURN. Thank you, Mr. Chairman. I will be brief. I just wanted you to know, that weather app that you have on your phone sends me the location of all the meetings you attend, so just be forewarned.

Senator FRANKEN. That makes me very frightened.

[Laughter.]

Senator COBURN. I will thank our witnesses for being here today, both our government witnesses and our outside witnesses. Transparency in what we do in government and outside of government, when it is not fiduciary and when it is not proprietary, is important for the American people, as is the issue of privacy. And rather than making the decision on what needs to change, I think we need a whole lot more information and knowledge in terms of those of us on the legislative side before we come to conclusions about what should be or needs to be done.

So I am looking forward to our witnesses' testimony, and with that, I will shorten this up and rather would hear from our witnesses rather than to continue to propound from the dais.

Senator FRANKEN. Thank you. I think we will begin our first panel now, and I want to introduce them.

We have Jessica Rich. She is Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission. She has served as an Assistant Director in the Federal Trade Commission's Bureau of Consumer Protection since 1998, first in the Division of Financial Practices and now in the Division of Privacy and Identity Protection. She previously served as legal adviser to the Director of the Bureau of Consumer Protection. She received her law degree from New York University and her undergraduate degree from Harvard University.

Jason Weinstein is the Deputy Assistant Attorney General for the Criminal Division of the U.S. Department of Justice. Before joining the Criminal Division, Mr. Weinstein served as the Chief of the Violent Crimes Section in the U.S. Attorney's Office for the District of Maryland. He was also an Assistant U.S. Attorney in the U.S. Attorney's Office for the Southern District of New York. Mr. Weinstein attended Princeton University and George Washington University Law School, and I understand that your wife is very pregnant and that you may have to leave during your testimony or during Ms. Rich's testimony, and as Chairman, that will be fine if you have to leave.

[Laughter.]

Senator FRANKEN. Ms. Rich.

STATEMENT OF JESSICA RICH, DEPUTY DIRECTOR, BUREAU OF CONSUMER PROTECTION, FEDERAL TRADE COMMISSION, WASHINGTON, DC

Ms. RICH. Chairman Franken, Ranking Member Coburn, Chairman Leahy, and Members of the Subcommittee—let me turn on the microphone. That would help.

Senator FRANKEN. Yes.

Ms. RICH. I am Jessica Rich, Deputy Director of the Federal Trade Commission's Bureau of Consumer Protection. I appreciate this opportunity to present the Commission's testimony on mobile privacy.

The FTC is the Nation's consumer protection agency, and privacy has been an important component of our mission for 40 years. During this time, the Commission has employed a variety of strategies to protect consumer privacy, including law enforcement, regulation, outreach to consumers and businesses, and policy initiatives. Just as we have protected consumer privacy in the brick-and-mortar marketplace, on the phones, on email, on mail, and on the Internet, we are committed to protecting privacy in the rapidly growing mobile arena.

To ensure the Commission staff has the technical and practical ability to engage in law enforcement and inform policy development in the mobile space, the Commission has hired technologists to work as FTC staff. The agency also has created a mobile lab with numerous smartphone devices on various platforms and carriers as well as software and other equipment to collect and preserve evi-

dence. In addition, Commission staff have explored the key mobile consumer protection issues through workshops and reports.

What is clear from our work in this area is that the rapid growth of mobile products and services creates many opportunities for consumers, but also raises serious privacy concerns. These concerns stem from the always-on, always-with-you personal nature of mobile devices; the invisible collection and sharing of data with multiple parties; the ability to track consumers, including children and teens, to their precise location; and the difficulty of providing meaningful disclosures and choices about data collection on the small screen.

Law enforcement is, of course, critical to our consumer protection mission. The FTC's primary law enforcement tool, the FTC Act, prohibits unfair or deceptive practices. This law applies regardless of whether a company is marketing offline, through your desktop or telephone, or using a mobile device.

In the Commission's testimony, we described four recent FTC cases brought under the FTC Act that address practices in the mobile arena. Two of these cases against two of the largest players in the mobile ecosystem, Google and Twitter, highlight the FTC's efforts to challenge deceptive claims that undermine consumers' choices about how their information is shared with third parties.

In Google, the Commission alleged that the company deceived consumers by using information collected from Gmail users to generate and populate a new social network, Google Buzz. The Commission's proposed settlement contains strong injunctive relief, including independent audits of Google's privacy policies and procedures lasting 20 years, that protects the privacy of all Google customers, including mobile users.

In Twitter, the Commission charged that serious lapses in the company's data security allowed hackers to take over Twitter's accounts and gain access to users' private tweets as well as their nonpublic mobile phone numbers. As in Google, the Commission's order protects data that Twitter collects through mobile devices and requires independent audits of Twitter's practices in this case for 10 years. If either company violates its order, the Commission may obtain civil penalties of $16,000 per violation.

Similarly, in our ongoing Phil Flora litigation, the Commission obtained a temporary restraining order against a defendant who allegedly sent five million unsolicited text messages to the mobile phones of U.S. consumers. And in the Reverb case, the Commission alleged that a public relations company planted deceptive endorsements of gaming applications in the iTunes mobile app store.

The Commission's public law enforcement presence in the mobile arena is still at a relatively early stage, but we are moving forward rapidly and devoting resources to keep pace with developing technologies. Commission staff have a number of mobile investigations in the pipeline, including investigations related to children's privacy on mobile devices. I anticipate that many of these investigations will be completed in the next few months, and any complaints or public statements will be posted on our website, FTC.gov.

I want to emphasize that while the mobile arena presents new methods of data collection and new technologies, many of the privacy concerns build on those the FTC has been dealing with for 40

years. At bottom, it is all about ensuring that consumers understand and can control data collection and sharing and that their data does not fall into the wrong hands. The FTC has the authority, experience, and strong commitment to tackle these issues.

In closing, the Commission is committed to protecting consumer privacy in the mobile sphere through law enforcement and by working with industry and consumer groups to develop workable solutions that protect consumers while allowing innovation. I am happy to answer any questions.

[The prepared statement of Ms. Rich appears as a submission for the record.]

Senator FRANKEN. Thank you, Ms. Rich.

Mr. Weinstein.

STATEMENT OF JASON WEINSTEIN, DEPUTY ASSISTANT ATTORNEY GENERAL, CRIMINAL DIVISION, U.S. DEPARTMENT OF JUSTICE, WASHINGTON, DC

Mr. WEINSTEIN. Thank you, Mr. Chairman. I have asked the baby to stay put until after about 11:30, which will probably be the last time it ever listens to anything I say.

Good morning, Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee, and I thank you for the opportunity to be here today.

Over the last decade, we have witnessed an explosion of mobile computing technology. From laptops and cell phones to tablets and smartphones, Americans are using more mobile computing devices, more extensively, than ever before. We can now bank and shop and conduct business and socialize remotely with our friends and loved ones instantly almost anywhere. And now more than ever, the world is almost literally at our fingertips.

But in ways that we do not often think about, what we say and write and do with these mobile devices can be open to the world. And as the use of mobile devices continues to grow, these devices are increasingly tempting targets for identity thieves and other criminals.

So as these devices increase our connectivity, our productivity, and our efficiency, they also pose potential threats to our safety and our privacy, and those threats fall into at least three very different categories.

The first category is the threats posed by cyber criminals, identity thieves, cyber stalkers, and other criminals who seek to misuse the information that is stored in or generated by our mobile devices to facilitate their crimes. From around the corner or around the globe, skilled hackers work every single day to access the computer systems and the mobile devices of government agencies, universities, banks, merchants, and credit card companies to steal large volumes of personal information, to steal intellectual property, and to perpetrate large-scale data breaches that leave tens of millions of Americans at risk of identity theft.

In addition, some of these cyber criminals seek to infect the computers in our homes and our businesses with malicious code to make them part of a botnet, a network of compromised computers under the remote command and control of a criminal or a foreign

adversary who can capture every keystroke, every mouse click, every password, credit card number, and email that we send.

Smartphones and tablets are, in a very real sense, mobile computers, and the line between mobile devices and personal computers is shrinking every day. So these devices provide yet another computing platform for cyber criminals to target for botnets and infection by malicious code.

Unfortunately, Americans who are using infected computers and mobile devices are suffering from an extensive, pervasive invasion of their privacy at the hands of these criminals almost every single time they turn on their computers. One of the Department of Justice's core missions is protecting the privacy of Americans and prosecuting the criminals who threaten and violate that privacy. Through the dedication and skill of our prosecutors and our agents, we have had a number of major enforcement successes, including most recently the operation in Connecticut to successfully disrupt the Coreflood botnet, which was believed to have infected over two million computers worldwide.

As mobile devices become more prevalent and as they store more and more personal information about their users, we should expect that they will be increasingly targeted by criminals. It is critical, therefore, that law enforcement has the necessary tools to investigate and to prosecute those crimes, which are crimes against the privacy of all Americans.

The second category of threats to our privacy comes from the collection and disclosure of location information and other personal information by the providers themselves, including app providers. These situations may or may not be appropriate for criminal investigation and prosecution. It all depends on the circumstances. Some may best be addressed through regulatory action. And as we evaluate these matters, we must carefully consider the clarity and the scope of privacy policies and other user agreements that govern the relationship between providers and their customers.

The third category of threats comes from criminals who use mobile devices to facilitate all sorts of their own crimes, from traditional cyber crimes like identity theft to violent crimes like kidnapping and murder. As technology evolves, it is critical that law enforcement be able to keep pace. Law enforcement must be able to get the data it needs to investigate and prosecute these crimes successfully and to identify the perpetrators—what we used to call "putting fingers at the keyboard," and which I guess we should now call "putting fingers on the touchpad."

This kind of identification is already a challenge in cases involving more traditional computers where data critical to investigations of cyber criminals and child predators and terrorists and other malicious actors has too often been deleted by providers before law enforcement can obtain it through a lawful process. That challenge is even greater in cases involving mobile devices. Although we increasingly encounter suspects who use their smartphones and tablets just as they would a computer, many wireless providers do not maintain the records necessary to trace an IP address back to a suspect's smartphone. Those records are an absolutely necessary link in the investigative chain that leads to the identification of a particular suspect.

I thank you for the opportunity, Mr. Chairman, to discuss some of the challenges the Department sees on the horizon as Americans' use of smartphones and tablets continues to grow and how the Department works every day to protect the privacy of users of computers and mobile devices. We look forward at the Department of Justice to continuing to work with the Congress as it considers these issues, and I would be pleased to answer your questions.

[The prepared statement of Mr. Weinstein appears as a submission for the record.]

Senator FRANKEN. Thank you. Thank you both.

Ms. Rich, in the FTC's December 2010 Consumer Privacy Report, the Commission states that certain kinds of information are so sensitive that before any of this data is collected, used, or shared, companies should seek "express affirmative consent" from a customer. You identify four categories of data that are this sensitive: information about children, financial information, medical information, and precise geolocation data.

First of all, why does the FTC think that before a company gets or shares your location information, they should go out of their way to get your consent?

Ms. RICH. We identified those four categories because misuse of that kind of data can have real consequences for consumers. So in the case of location data, as you mentioned and your colleagues mentioned, it can lead to—if it falls into the wrong hands, it can be used for stalking. Teens and children have a lot of mobile devices, and so we are often talking about teen and children information and their location.

Location cannot just tell you where a person is at a particular time. If it is collected over time, you can also know what church somebody has gone to, what political meeting they have gone to, when and where they walk to and from school. So that is sensitive data that requires special protection.

Senator FRANKEN. Thank you.

Mr. Weinstein, let me ask you a related question. When I use my smartphone, a lot of people can and do get a hold of my location, my wireless company, companies like Apple and Google, as well as the mobile apps that I have on my phone. My understanding, Mr. Weinstein, is that in a variety of cases under current Federal law, each of those entities may be free to disclose my location to almost anyone that they please without my knowing it and without my consent. Is that right?

Mr. WEINSTEIN. That is right, Mr. Chairman. The statute, ECPA, that you made reference to that Chairman Leahy wrote 25 years ago does provide in those instances in which it covers the provider—and that is a separate question. It places a great deal of restrictions on the ability of providers to share that information with the Government, but virtually no legal restriction on providers' ability to share that with other third parties.

There may be specific types of restrictions if you are talking about data other than location, like health care data, that may be covered by other particular privacy laws. But if you are talking about location data, then there is no legal restriction.

If the company is not covered by ECPA, that is, it is not considered to be an electronic communications service provider or a pro-

vider of remote computing service, then there is no restriction at all. The company is free to share it with whoever they want.

Senator FRANKEN. Mr. Weinstein, one of the defining features of the mobile market is that you have a lot of different entities—app developers, advertisers, companies like Apple and Google—that are amassing large amounts of information about users.

Outside of any assurances that they make to their customers or the requirements of financial records laws, do the companies in this sphere have to meet certain data security standards? In other words, what is to prevent them from getting hacked?

Mr. WEINSTEIN. I am not aware, Mr. Chairman, of any legal requirement that a company that is in possession of your personal data—whether we are talking about location data or financial data or other data about your use of what you do online—secure that data in any particular way. My understanding is that that is essentially a decision made by the company based on its own business practices and its assessment of risk.

This relates to one of the arguments that you often hear when we talk about data retention, because there is also no requirement that the company retain data for any particular length of time, and that often impacts our ability to investigate and solve crimes, including crimes that threaten privacy. And when we talk to industry and when we talk to privacy groups about the need for data retention for some reasonable period of time to make sure that law enforcement could get the data it needs to protect privacy, what you often hear is that if companies are required by law to store that data for some length of time, it will put them at greater risk of being hacked. And it is an open question, certainly one for the Congress to consider, whether if there were to be a requirement for data retention, whether it is also appropriate to impose some requirement that the data be secured in some way to reduce that risk.

Senator FRANKEN. Thank you, Mr. Weinstein.

Before I turn to the Ranking Member, I want to introduce a few key pieces of testimony into the record.

First, I want to introduce joint testimony from the Minnesota Coalition for Battered Women and the National Network to End Domestic Violence, as well as testimony from the National Center for Victims of Crime. This testimony lays out how law enforcement can use this technology to find stalkers. It also cites cases of two Minnesota women who were both stalked by their partners through their smartphones. These are extreme cases, but I think there is no clearer statement on how this technology presents clear benefits and also very clearly privacy threats and how we need to be very careful in this space.

[The prepared statement appears as a submission for the record.]

Senator FRANKEN. Now I would like to turn it over to the Ranking Member, Senator Coburn.

Senator Coburn.

Senator COBURN. Thank you, Mr. Chairman.

One comment I would make—I hope after you all testify that you will hang around and listen to the second panel. What I find is in Congress a lot of time we talk past each other, and when we are observing us talking past each other, we actually learn something

if we are an outside observer. And I would hope that when we hear both sides of this today, it will actually accentuate the ability to solve the problems that are in front of us.

I want to thank you for your testimony. I have a question directed to both of you, and I would like for you to just individually answer it.

Both of you have demonstrated that under certain laws that we have on the books today you can do a lot in terms of addressing these privacy issues. My question for you is: In your opinion, what else do you need in terms of statute to actually facilitate your ability to protect the privacy of individuals in this country without diminishing the benefits that we are seeing from this technology?

Ms. RICH. The Commission has not taken a position at this point on legislation in this area; however, in the report that Senator Franken referred to, we did discuss some key protections we think should be applied across industry, including in mobile, that we believe would protect privacy while also allowing innovation to continue. First, companies should have privacy by design, meaning at the very early stages of developing their products and services, they need to give privacy serious thought so that they develop those products and services in a way that maximizes the safety to consumer data. That means not collecting more data than is needed, not retaining it for longer than is needed, providing security for it, and making sure it is accurate. Those things, if implemented early, can be done in a way that still permits innovation and still permits the business to function.

Senator COBURN. Can you do that through regulation now? Can you make those demands through regulation?

Ms. RICH. We have used Section 5 of the FTC Act, which prohibits unfair or deceptive practices, to bring enforcement against companies that do not do those things under certain circumstances.

The second piece is streamlined, easy-to-use choice for consumers. Streamlining choice and making it easy for consumers would be particularly important on mobile devices where we either do not see privacy policies, as was mentioned in the *Wall Street Journal* article, or when we do, it may take a hundred clicks to get through the terms of service to find them.

So, we have encouraged the use of icons and other ways to make it easier for consumers to exercise choice about things like sharing data with third parties.

Senator COBURN. Like writing in plain English instead of lawyerese?

Ms. RICH. Yes. And then the third piece is, of course, greater transparency overall, which means if you do have privacy policies, they should be written in a simple way so they are easy to compare. Also, potentially a consumer should be able to access the data that companies have on them.

We believe, if implemented, these protections would achieve much greater protection for consumers while also allowing innovation.

Senator COBURN. So the question I would have for you is: Do you have the ability to implement that now under the FTC guidelines?

Ms. RICH. Some of the polices can be implemented under the FTC Act, but some of them are forward-looking policy goals.

Senator COBURN. Would you mind submitting to the Committee which are which so that it can guide us in addressing where we think we might need to go?

Ms. RICH. Yes, we will.

Senator COBURN. Thank you.

[The information referred to appears as a submission for the record.]

Senator COBURN. Mr. Weinstein.

Mr. WEINSTEIN. Senator Coburn, there are four or five things that the Justice Department thinks Congress should consider in terms of legal changes, but most of them are not particular to mobile devices. A few of them are. And the reason that they are not all specific to mobile devices is I think it is important to put in perspective that the threats that you see in terms of cyber crime committed on mobile devices are really just new variations on old problems. You know, when someone puts malware on your computer because they attach it to an email, that is a threat to your computer. If someone uses an Android app as a delivery system for their malware, that is old-school cyber crime committed with new-school technology. And so what we need to protect privacy is the same thing we need to be able to fight cyber crime generally.

That being said, number one, there are a number of further fixes to 1030, to the *Computer Fraud and Abuse Act*, even beyond those that were contained in the *Identity Theft Enforcement and Restitution Act* in 2008 that we believe are appropriate and would strengthen penalties and strengthen deterrence and make sure that there were significant consequences, more significant consequences for cyber crime. Those we anticipate will be part of the cyber security package which I told Senator Whitehouse a month ago was imminent, and now it is imminent measured in terms of days instead of weeks.

The second relates to cyber stalking. The cyber stalking statute requires currently that the victim and the defendant actually be in different States, and that significantly hampers our ability to use that statute since, as you know, cyber stalkers are people who harass, whether through cyber or other means, and are frequently right down the street, not necessarily across the State line.

The third is data retention. We think that there are—although we do not have a specific proposal, there are undoubtedly—there is a reasonable period of time that Congress can require providers to retain data that would allow us to solve crimes against privacy that properly balances the needs of law enforcement, the needs of privacy, and the needs of industry.

The fourth is data breach reporting. You know, as we see, every week we see a new article in the newspaper about another significant data breach, whether it is Sony or Epsilon or RSA, and it highlights the fact that there is no legal requirement federally—although there are a number of State laws, there is no comprehensive Federal legal requirement that requires data breach reporting either to customers or law enforcement.

The fifth, which is mobile device specific, is the one I alluded to in my oral remarks, and that is that among the data that is not even maintained, let alone retained, is data that would allow us to trace back an IP address to the smartphone that was using it at

the time that a criminal conversation or other criminal conduct occurred.

The last piece—and then I will stop—is not a particular proposal but just something we encourage Congress to consider because it relates to privacy generally. As I alluded to a few minutes ago, there are significant legal restrictions on a provider's ability to share data with law enforcement. There are no restrictions, virtually no restrictions, certainly none provided by ECPA, on a provider's ability to share that information with third parties for any purpose, commercial or otherwise. And we think that Congress may wish to consider whether ECPA properly strikes that balance between privacy—the privacy balance between consumers and the providers that they are engaged in commerce with.

Senator COBURN. All right. Thank you very much.

Thank you, Mr. Chairman.

Senator FRANKEN. Thank you, Senator Coburn.

Mr. Chairman.

Chairman LEAHY. Mr. Weinstein, you mentioned ECPA, and I am glad you did because I am going to be introducing a bill very shortly to update ECPA, the *Electronic Communications Privacy Act*. I think it is a very important Act. Many of us have a concern it does not apply to the mobile applications currently available, and that can be bad for consumers and also bad for law enforcement.

Let me just point out the privacy requirements in ECPA only apply to providers of either electronic communications service providers or remote computing service providers. But if Google or Apple or other application providers collect data automatically or generates data from a smartphone, they might not fall into either of the definitions. But that would mean the government could just step in and obtain location and other sensitive information collected without obtaining a search warrant. I had mentioned a search warrant situation earlier when I spoke, but they might be able to do it without.

Does ECPA apply to providers of mobile applications? And if not, what are some of the changes we should make?

Mr. WEINSTEIN. Mr. Chairman, the answer really would be the same answer I would give if you asked me not about mobile application providers but if you asked me about Verizon or Google, or Apple, for that matter. As companies provide a broader range of services, a company may be considered a provider of electronic communications service for one service it provides, remote computing service for another service it provides, and neither for some other service it provides. So even a company like Verizon is clearly an ECS for its communications services. A company like Apple might be an RCS for the mobile media remote back-up service. Google might be for Google docs, but for—Google might be an ECS or would be an ECS for Gmail.

So a mobile app provider could be an ECS or an RCS or neither one. A lot of it depends not on the nature of the company but on the nature of the particular service. So——

Chairman LEAHY. Well, does that mean we have a gap in ECPA and we should be addressing it in the new legislation?

Mr. WEINSTEIN. I think that as all of these companies expand the range of services they provide, there are going to be gaps. There

are going to be companies, whether more traditional companies or newer companies, that provide services that do not fall in one of the two categories. And so I do not have a particular proposal, but we would certainly be happy to work with you to explore where those gaps are and how they should be filled.

Chairman LEAHY. In the scenario I suggested, is this something where law enforcement could come in and get all this information without a search warrant and without going through a court?

Mr. WEINSTEIN. Well, if a company is not covered by ECPA, then we can get stored data using a subpoena or other legal process. A search warrant would not be required—in most instances.

Chairman LEAHY. Now, you mentioned Epsilon and Sony and the breach, which, as I read more and more about it, it is more and more frightening what is there. On three occasions, the Judiciary Committee has favorably reported my comprehensive data privacy and security bill. Among other things it would establish a national standard for notifying consumers about data breaches involving their personal information, and we will try again this Congress to get this passed. But if there has been a data breach and your information is there, you would not have to rely on the good graces of the company that screwed up allowing the data breach, but they would be required to notify you of it.

How important is it for your Department and other law enforcement agencies to be notified of data security breaches so that they can look at whether it affects our criminal laws and national security? And then I will ask Ms. Rich a similar question.

Mr. WEINSTEIN. It is vital for law enforcement. If we do not know about a breach, we cannot investigate it, and if we find out about it too late, by the time we find out about it and begin investigating, the trail very well may have gone cold.

There are, as I think you know, 46 or 47 State laws that in some fashion govern breach reporting, but only a few of them require the victim to notify law enforcement. Some of our biggest hacking and identity theft cases, a number of which I testified about in front of the Crime Subcommittee a month ago, were made possible because we got early reporting from the victim companies and we got cooperation from the victim companies throughout the investigation, and that was critical to our ability to follow the trail and find the hackers and find the people who stole personal data.

The two things that law enforcement needs to be able to have a shot at making these cases are prompt victim reporting and, if there is customer notification, which there certainly should be, the opportunity to delay that notification, where appropriate, if law enforcement or national security needs dictate. But we think that breach reporting is vital to our ability to do our jobs, and we anticipate that in this imminent cyber security package there will be a data breach proposal that is contained in it.

Chairman LEAHY. Ms. Rich.

Ms. RICH. The FTC has long supported legislation to require data breach notification and data security. We play a complementary role to the Department of Justice in that they pursue the hackers, the malicious folks who get the data, but our perspective is it is extremely important to also shore up the protections of those companies that have the sensitive data. There are always going to be

criminals, but it is very important that companies secure themselves, so they are not easy targets. And we believe legislation requiring notification and security is vital to that mission.

Chairman LEAHY. Thank you. And, again, Chairman Franken, I thank you for holding this hearing. I think it is extremely important. I will go off to some budget matters now, but I appreciate your doing this.

Senator FRANKEN. Please do that. Thank you, Mr. Chairman.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Senator Franken, for your leadership. Again, thank you, Senator Leahy, for your championing many of these privacy issues over decades, literally, and providing a model of that kind of leadership for us. And I want to thank our witnesses for being here, also Apple and Google and the consultants that we have, in this profoundly important hearing. And whatever the kinds of challenging questions that we may ask, I hope that we are all on the same side of this cause, because right now what we face, in my view, is literally a Wild West so far as the Internet is concerned. We can debate the legal niceties and technicalities, but the FTC statutes that prohibit unfair and deceptive practices simply do not provide the kind of targeted enforcement opportunity that I think is absolutely necessary, and I know the Department of Justice is going to be seeking additional authority, which is absolutely necessary. And just one area pertains to young people, children, which we have not discussed so far today, but which obviously raises very discrete and powerfully important issues.

And so let me begin with Ms. Rich. Do you think that the present statutes sufficiently protect young people, children who are 13 and under, when we are talking about marketing, locational information, other kinds of privacy issues?

Ms. RICH. We do have a very strong law, the *Children's Online Privacy Protection Act*, that applies to children 12 and under, and we are undertaking a review of that right now. One of the reasons we are reviewing the Rule is to see if it is keeping up with technology, and we have not reached the end of that process. But in a workshop we had on the topic, there was a fair amount of agreement from industry and consumer groups alike that that statute is sufficiently flexible to cover a lot of mobile activities across a broad swath of technologies.

Senator BLUMENTHAL. And do you agree, Mr. Weinstein?

Mr. WEINSTEIN. I do. I was thinking this morning I have two, soon to be three, little kids, and my three-year-old is better with my iPhone than I am. And it is terrifying, actually, to think about what kind of online threats will be out there by the time he is actually old enough to really be using my iPhone with permission.

So I think that as we move into this space, I think it is important that any legal changes that we make be technology neutral to the extent possible, and one of the geniuses of ECPA is that it has been able to be flexible and adaptable over a period of 25 years as technologies change. But I do think that anything the Congress can do, I think, to protect kids in particular in this space is a worthy effort.

Senator BLUMENTHAL. And let me ask, Ms. Rich, referring to your description of privacy by design, in addition to the requirement that Senator Leahy is supporting that there be notification—and I strongly support that requirement. I think it is a basic, fundamental protection—shouldn't there be some requirement that companies design and safeguard this information when they structure these systems and also potentially liability if they fail to sufficiently safeguard that information, liability so that we provide incentives for companies to do the right thing?

Ms. RICH. Absolutely. We have brought, using Section 5, 34 cases against companies that failed to secure data, and we believe it is vital to hold companies accountable for that.

Senator BLUMENTHAL. And what about a private right of action?

Ms. RICH. The Commission has not taken a position on legislation or private right of action.

Senator BLUMENTHAL. Because we had testimony from Professor John Savage of Brown University who said to us, and I am quoting, "Computer industry insiders have solutions to many cyber security problems, but the incentives to adopt them are weak, primarily because security is expensive and there is no requirement they be adopted until disaster strikes."

Ms. RICH. Let me correct something I just said. The Commission has actually taken a position on data security. I was a little confused by the question. We strongly support data security and data breach legislation, absolutely, which includes civil penalties.

Senator BLUMENTHAL. Thank you.

My time has expired, and I will be submitting some additional questions for the record. Thank you both.

Senator FRANKEN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you, Chairman Franken.

A quick question, and then a slightly longer one. The quick question is that both of you have had a chance to look into, you might call it, the dark side of the Internet, the dark underbelly of the Internet. And you are also people who use it and have families who use it, and so you both have the experience of the regular American at dealing with the Internet and having a certain measure of confidence in it. And you have a heightened awareness based on your professional obligations.

Based on that, how well informed do you believe the average American is about the dangers and hazards that lurk out there on the Internet? And is this significant in terms of things as simple as willingness to download protective patches and get up to date with commercial off-the-shelf technology to protect yourself, setting aside other responses that the public might have if it were more informed? Can you quantify a little bit how well informed you think the average American is about these risks?

Ms. RICH. We believe that consumers really have no idea of the layers of sharing that go on behind the scenes. So, for example, many consumers may like location services, and they may want to share their location information in order to obtain them. What they do not realize is that their location data as well as the device ID may then be flowing to service providers, to advertisers, to all sorts of other parties in the chain. And we believe that is why, when certain high-profile security breaches happen to companies like Epsi-

lon who are service providers and behind the scenes, people are so shocked because they had no idea their data was there.

Senator WHITEHOUSE. Mr. Weinstein.

Mr. WEINSTEIN. You know, I think with the large population that we are talking about, I think that there is going to be great variation. But I venture to say that—and this is based on sort of professional and personal observation—the vast majority of people are not as informed as they should be. And, in fact, if nothing else comes out of the heightened awareness that the Apple and Google media frenzy has created and that this Subcommittee's interest has generated, I think it will be that people focus more on these issues.

The fact is that these kinds of situations may or may not be criminal enforcement matters, but what they do highlight is the need for everybody to be more vigilant. Undoubtedly, providers can take steps to make sure that their user agreements and their privacy policies are more transparent and are easier for the average——

Senator WHITEHOUSE. Let me jump into that, if you do not mind, a little bit.

Mr. WEINSTEIN. Sure.

Senator WHITEHOUSE. Earlier in your answer you basically set up the traditional dichotomy, if you will, between a legitimate communication or application and something that is infected with malware and is probably a law enforcement problem if it could be discovered.

We are now in a new area, kind of in between those two, where the product might actually be something that the subscriber would want. I can imagine a location application that told you whenever you were near a particular fast-food restaurant so they could ping you and say, "Come on in for a Big Mac," or whatever it would be. And that might be something that somebody would want. It also might be something that somebody would really not want at all, and I think part of the concern here is that if you are loading an app, for instance, onto a smartphone, you know that you are loading one dimension of the app. You do not know what else is being attached onto that. And what should the FTC be doing by way of disclosure requirements to make sure that when you load an app, whoever has put that app on the menu, really, for people to choose among has fully disclosed that all of the elements are in it and it is not just a Trojan horse to attract you with a particular thing when its real purpose is to find out information about you to sell to other individuals?

Where are you in terms of getting that transaction properly overseen and with some rules? I guess what you would call privacy by design in your earlier statement.

Ms. RICH. It is a challenge in the mobile sphere because of the nature of the small screen, but the FTC has called on industry to develop simplified disclosures that are embedded in the interaction. So, for example, when you are downloading an app and it is going to share the information with third parties, it should tell you that there and then, not in some privacy policy that will take you a hundred screens to download and look at.

So, I think there needs to be serious work done to improve the interaction between these companies and consumers. We also think

that if it is not necessary to share data with other companies for the business model, it should not be happening. We have also seen that even when sharing is necessary for the business model, instead of sharing the limited slice of information that is needed, pull the information off the whole device and share it with third parties. That is why privacy by design is needed.

Senator WHITEHOUSE. And from your point of view, the Trojan horse analogy for some apps is a fair one.

Ms. RICH. Yes.

Senator WHITEHOUSE. OK. Thank you.

Senator FRANKEN. Thank you, Senator Whitehouse.

I am going to have one more question here for Ms. Rich, and the Ranking Member has one more question.

Ms. Rich, in your testimony—and you were just talking about the little screen and signing off on privacy agreements. Anyway, in your testimony you emphasize the FTC's ability to protect consumers against deceptive trade practices. When an iPhone user activates her phone, they have to click and agree to a 4,144-word software license agreement, and that tells users they can withdraw their consent to Apple's collection of location information at any time by simply turning off the location services button on their phones. I will add a copy of that agreement—this is it—to the record.

[The agreement appears as a submission for the record.]

Senator FRANKEN. As it turns out, until about a week ago, turning off the switch did not stop the collection of location information by Apple, so I guess my question is: Ms. Rich, is that a deceptive trade practice?

Ms. RICH. Well, I cannot comment on a specific company's practices, but I can say that if a statement is made by a company that is false, it is a deceptive practice. Similarly, as we have shown in our cases, if there is a misleading statement and then some sort of disclaimer in fine print, that could be a deceptive practice.

So there is a lot we could do under our deception authority to challenge the types of practices you are talking about, although I am not going to comment on a specific company.

Senator FRANKEN. Thank you.

Ranking Member.

Senator COBURN. Mr. Chairman, I just have one comment. I think we need to be very careful on this idea of security because the greatest example I know is we spend $64 billion a year on IT in the Federal Government, and then on top of that, we spend tens of billions on security, and we are breached daily. So we should not be requesting a standard that we cannot even live up to at the Federal Government.

So the concern is an accurate one, but I think we are going to have to work on what that standard would be, whether it is a good-faith effort or something. But to say somebody is liable for a breach of their security when we all know almost every system in the world can be breached today, we need to be careful with how far we carry that. And that is all I would add.

Ms. RICH. Can I just address that briefly to say that we agree there is no such thing as perfect security, and we have always used a reasonableness standard. Many of the types of practices that

would prevent breaches are things like not collecting more data than you need.

Senator COBURN. I agree.

Senator FRANKEN. Senator Blumenthal, do you have another question?

Senator BLUMENTHAL. Yes, just to follow up on Senator Coburn's observation, as with any kind of liability or accountability, legal responsibility, there is a duty of care, and that duty of care can impose reasonable measures that common sense or technology would provide the means to do. And so I guess my question is: Why not some liability to ordinary consumers imposed through Federal law that would impose accountability for a standard of care that is available under modern technology with the kinds of reasonable approach, sensible responsibility?

Ms. RICH. Yes, Senator, we agree with you. In the data security sphere, it is reasonable security. It is having a good process that assesses risks and addresses those risks. It is not perfection.

Senator BLUMENTHAL. And why not also require remedies in the case of a breach where that kind of accountability is imposed, for example, insurance or credit freezes, credit monitoring, as a matter of law, so that what is increasingly becoming standard practice would be imposed on all companies and provide the incentive to do more?

Ms. RICH. Absolutely. We think that is important both to address what has happened to consumers and provide effective deterrence.

Senator BLUMENTHAL. Do you agree, Mr. Weinstein? I know you are speaking out of the consumer protection area, but——

Mr. WEINSTEIN. Well, I am trying to stay in my lane, but, look, I think from a—I will make the general observation, and I think this touches on some issues we talked about at the hearing last month. There is no perfect system. Cyber security, true cyber security, requires sort of a multi-layered approach, requires laws that breaches be reported. It undoubtedly requires providers to take as much of an effort, make as much of an effort as they can to protect their systems. It requires some public-private partnership, and I think that some of the proposals that will be in this package that you will be receiving address that issue. And it requires, I think, better work by everybody involved.

Senator BLUMENTHAL. Well, we look forward to the package, and to the package that you will be receiving in hopefully a very short time. Thank you.

Senator FRANKEN. Thank you, Senator, and I want to thank Ms. Rich and Mr. Weinstein. Mr. Weinstein, good luck and congratulations with your new baby.

We will now proceed to the second panel of this hearing. I think I will introduce our panel as they are making their transition to the table, just to move things along. Well, there seems to be a little chaos here. We will take a little moment of pause to think about the first panel and all the issues that were raised and thoughts that were expressed.

[Pause.]

Senator FRANKEN. I would like to introduce our second panel of witnesses, and I want to thank you all for being here.

Ashkan Soltani is a technology researcher and consultant specializing in consumer privacy and security on the Internet. He has more than 15 years of experience as a technical consultant to Internet companies and Federal Government agencies. Most recently, he worked as the technical consultant on the *Wall Street Journal's* "What They Know" series, investigating digital privacy issues. He has a master's degree in information science from the University of California at Berkeley and a B.A. in cognitive and computer science from the University of California at San Diego.

Justin Brookman is the director of the Project on Consumer Privacy at the Center for Democracy and Technology. He was also the chief of the Internet Bureau of the New York Attorney General's Office. Under his leadership the Internet Bureau was one of the most active and aggressive law enforcement groups working on Internet issues. He received his J.D. from the New York University School of Law in 1998 and his B.A. in government and foreign affairs from the University of Virginia in 1995.

Mr. Bud Tribble is the vice president of software technology at Apple. Tribble helped design the operating system for Mac computers. He was also the chief technology officer for the Sun-Netscape Alliance. Tribble earned a B.A. in physics at the University of California at San Diego and an M.D. and Ph.D. in biophysics and physiology at the University of Washington, Seattle.

Alan Davidson is the director of public policy for the Americas at Google. He was previously associate director for the Center for Democracy and Technology and a computer scientist working at Booz, Allen & Hamilton, where he helped design information systems for NASA's Space Station Freedom. he has an S.B. in mathematics and computer science and an S.M. in technology and policy from MIT and a J.D. from Yale Law School.

Jonathan Zuck is the president of the Association for Competitive Technology. ACT represents small- and mid-sized information technology companies. Before joining ACT, Zuck spent 15 years as a professional software developer and an IT executive. He holds a B.S. from Johns Hopkins University and a masters in international relations from the Paul H. Nitze School of Advanced International Studies at the Johns Hopkins University.

I want to thank you all for being here today, and please give your opening statements. We will start from my left and your right. Mr. Soltani.

STATEMENT OF ASHKAN SOLTANI, INDEPENDENT PRIVACY RESEARCHER AND CONSULTANT, WASHINGTON, DC

Mr. SOLTANI. Chairman Franken, Ranking Member Coburn, and distinguished Members of the Subcommittee, thank you for the opportunity to testify about mobile privacy and the location ecosystem.

My name is Ashkan Soltani. I am a technology researcher and consultant specializing in privacy and security on the Internet. I should note the opinions here are my own and do not reflect the views of my previous employers.

Mobile devices today are powerful computing machines. But unlike desktop computers, mobile devices introduce unique privacy challenges. Consumers carry their phones and tablets with them

nearly everywhere they go, from their homes to their offices, from daycare to the grocery store.

A device's location can be determined using a number of different technologies, including GPS, information about nearby cell towers and WiFi access points, and other network-based techniques. While their accuracy can vary depending on the technology being used, the resulting insights derived from this data can be sensitive and personal in nearly all the cases.

If you imagine a historical trail of your whereabouts over the course of many days, it would be reasonably easy to deduce where you work, where you live, and where you play. this information can reveal much about who you are as a person and how you spend your time. I believe this is why many consumers have been surprised by the recent stories of how their mobile devices have been collecting their location information and other sensitive data.

With the exception of GPS, the process by which a device's location is determined can actually expose the location of that device to multiple parties. These parties include the wireless carrier, for example, AT&T and Verizon; the location service provider, such as Apple, Google, or Skyhook; and even the content provider used to deliver the information about that location, such as a mapping website or service.

Researchers, including myself, recently confirmed that smartphones, such as the Apple iPhones and Google Android devices, send location information quietly in the background to Apple's and Google's servers, respectively, even when the device is not actively being used. That is, the background collection happens automatically unless the user is made aware of the practice and elects to turn it off. This is the default behavior when you purchase these devices.

Furthermore, most smartphones keep a copy of historical location information directly on the device. Until recently, Apple's iPhone would retain an approximate log of your location history for about a year, stored insecurely on the phone and on any device the computer was backed up to. Anyone with access to this file would be able to obtain a historical record of your approximate location, and there was no way to disable it.

Many mobile smartphone platforms like Apple's iOS and Google Android also allow third parties to develop applications for the device: productivity software like e-mail, social networking tools like Facebook, and, of course, games. As reported in the *Wall Street Journal* last year, many popular apps transmit location information or its unique identifiers to outside parties. For instance, if a user opens Yelp, a popular restaurant discovery app, not only does Yelp learn information about the user but so could Yelp's downstream advertising and analytics partners.

This may be surprising to most customers since they may not have an explicit relationship with these downstream partners. This information is not limited to just location. Upon installation, many of these apps would have access to a user's phone number, address book, and even text messages.

Disclosure about the collection and use of consumer information are often ineffective or at times completely absent. Many disclosures are often vague or too confusing for the average consumer to

understand, and they rarely mention specifics about data retention and information-sharing practices—things that a privacy conscious consumer would care about. Notably, a mere half of the popular apps analyzed by the *Wall Street Journal* lacked discernible privacy policies.

To conclude, in order to make meaningful choices about their privacy, consumers need to increase transparency into who is collecting information about them and why. Clear definitions should be required for sensitive categories of information, such as location and other identifiable information. Software developers need to provide consumers with meaningful choice and effective opt-outs that allow consumers to control who they share information with and for what purpose. Only in an environment that fosters and control will consumers be able to take full advantage of all the benefits that mobile technologies have to offer.

I thank the Committee for inviting me here today to testify, and I look forward to answering your questions.

[The prepared statement of Mr. Soltani appears as a submission for the record.]

Senator FRANKEN. Thank you.

Mr. Brookman.

STATEMENT OF JUSTIN BROOKMAN, DIRECTOR, PROJECT ON CONSUMER PRIVACY, CENTER FOR DEMOCRACY AND TECHNOLOGY, WASHINGTON, DC

Mr. BROOKMAN. Thank you very much, Chairman Franken, Ranking Member Coburn, Members of the Subcommittee. Thank you very much for the opportunity to testify here today. there really could not be a more timely topic for the first hearing of this Subcommittee than the issue of mobile privacy. Consumers are enthusiastically embracing mobile devices, and they offer an amazing array of functionality that truly makes our lives better.

However, many of the same privacy issues that have frustrated consumers in the online space are actually significantly heightened in the mobile environment. As opposed to websites, apps can access a far broader range of personal information such as contact information, access to a smartphone's camera or microphone, and precise geolocation information. At the same time, the tools that consumers have to see and control how apps share their personal information are actually weaker than they are on the Web.

I have been invited here today to discuss the existing laws that govern mobile data flows and whether that framework has proven adequate to safeguard consumer information. The short answer is no. There is no comprehensive privacy law in the United States. There are a few sector-specific laws that govern relatively small sets of consumers' information. In the mobile space, I think it is fair to say that there is a patchwork of outdated and inapt laws that may apply at the margins, but do not offer consumers meaningful and consistent protections.

Now, traditionally mobile devices were one area where there actually were strong protections over consumer data. The Communications Act and the associated CPNI rules historically required carriers to get a customer's affirmative permission to share or sell the relatively limited information around the traditional dumb

phones, which is who you can call and whatnot. However, as cell carriers branched out into offering data plans for smartphones, the FCC opted not to extend CPNI rules to those information services, leaving the treatment of customer information about this new usage of mobile services unregulated.

Furthermore, CPNI rules never applied to most of the players in the modern apps space, such as operating system and location providers like Apple and Google, apps makers, mobile advertising networks, and data brokers. So as the mobile data ecosystem has dramatically expanded, the relatively narrow CPNI rules, which at one point effectively covered everything, no longer offer sufficient protections for consumers in the mobile space.

There are a couple other statutes that arguably apply at the margins, but they do not consistently protect consumers here. So one would be the Electronic Communications Privacy Act, which we discussed, which generally covers Government access to information, but does have some protections around certain companies in disclosing the contents of customer communications. Unfortunately, the definitions of this law were written in 1986, well before the modern apps ecosystem developed. The law could arguably be interpreted to cover some apps, but certainly not all, and probably it does not extend to the operating systems like Apple and Google. In short, the law does not really map well to mobile privacy issues, and certainly not consistently. Even if it did apply to all the players, without additional rules to require meaningful transparency and telling consumers what you are doing with their data, companies could just bury permissions to share data in terms of service agreements that consumers would be unlikely to read.

Finally, some have tried to apply criminal statutes, like the *Computer Fraud and Abuse Act*, to mobile privacy issues. Last month, for example, it was reported that the U.S. Attorney from New Jersey was investigating certain apps for transmitting customer information without adequate disclosure. And I think I am sympathetic to the policy goals of requiring better disclosure from apps. I think it is probably not the ideal approach to use a very broad criminal statute designed to combat hacking and protect financial information to protect privacy. I may not like it when companies share my information, and I think that should be protected by the law. I do not think people should necessarily go to jail for it.

So assuming that none of these diverse laws actually applied, the baseline in this country is the FTC's prohibition on unfair or deceptive practices. The FTC has brought some incredibly important cases in this area, but the bar is still very low. The baseline rule for most consumer data is merely that companies cannot affirmatively lie about how they are treating your data, so many companies' response might just be not to make any representations at all. This is why privacy policies tend to be legalistic and vague. The easiest way for a company to get in trouble is to actually make a concrete statement about what they are doing.

Indeed, in the mobile space, as Mr. Soltani testified, many apps makers do not make representations at all. Only a small percentage actually offer any privacy policies whatsoever. And so it is just not possible in the modern environment for people to figure out how their data is being stored by apps and shared. So we have long

petitioned for a baseline comprehensive privacy law that requires companies to say what they are doing with data, to give some choice around secondary transfer of that data, secondary uses, and to tell companies to get rid of it when they are doing.

Furthermore, for sensitive information such as relating to religion or sexuality, health, financial, and most relevant to this hearing, precise geolocation information, we believe that an enhanced application of the fair information practice principles, including affirmative opt-in consent, should govern. For this type of information, we should err on the side of user privacy and against presuming assent to disclosure.

Thank you very much for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Brookman appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Brookman.

And, by the way, for all of you, your complete written testimonies will be made part of the record.

Mr. Tribble.

STATEMENT OF GUY "BUD" TRIBBLE, M.D., PH.D., VICE PRESIDENT OF SOFTWARE, TECHNOLOGY, APPLE INC., CUPERTINO, CALIFORNIA

Mr. TRIBBLE. Good morning, Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee. My name is Bud Tribble. I am the vice president for software technology for Apple. Thank you for the opportunity to further explain Apple's approach to mobile privacy, especially location privacy. I would like to use my limited time to emphasize a few key points.

First, Apple is deeply committed to protecting the privacy of all of our customers. We have adopted a single comprehensive customer privacy policy for all of our products. This policy is available from a link on every page of Apple's website. We do not share personally identifiable information with third parties for their marketing purposes without our customers' explicit consent, and we require third-party application developers to agree to specific restrictions protecting our customers' privacy.

Second, Apple does not track users' locations. Apple has never done so and has no plans to ever do so. Our customers want and expect their mobile devices to be able to quickly and reliably determine their current locations for specific activities such as shopping, traveling or finding the nearest restaurant. Calculating a phone's location using just GPS satellite can take up to several minutes. iPhone can reduce this time to just a few seconds by using prestored WiFi hotspot and cell tower location data on the phone in combination with information about which hotspots and cell towers are currently receivable by the iPhone.

In order to accomplish this goal, Apple maintains a secure crowdsourced data base containing information with known locations of cell towers and WiFi hotspots that Apple collects from millions of devices. It is important to point out that during this collection process, an Apple device does not transmit to Apple any data that is uniquely associated with the device or with that customer.

This information is used to determine the locations of cell towers and WiFi hotspots for our crowdsourced data base.

Third, by design, Apple gives customers control over collection and use of location data on all our devices. Apple has built a master location services switch into our iOS mobile operating system that makes it extremely easy to opt out entirely of location-based services. The user simply switches the location services off in the setting screen. When the switch is turned off, the device will not collect or transmit location information. Equally important, Apple does not allow any application to receive device location information without first receiving the user's explicit consent through a simple pop-up dialog box. The dialog box is mandatory and cannot be overridden. Customers may change their mind and opt out of location services for individual applications at any time by simple on-off switches. Parents can also use controls to password-protect and prevent access by their children to location services.

Fourth, Apple remains committed to responding promptly and deliberately to all privacy and technology concerns that may arise. In recent weeks, there has been considerable attention given to the manner in which our devices store and use a cache subset of Apple anonymized crowdsourced data base. The purpose of this cache is to allow the device to more quickly and reliably determine a user's location. These concerns are addressed in detail in my written testimony. I want to reassure you that Apple was never tracking an individual's actual location from the information residing in that cache.

Furthermore, the location data that was seen on the iPhone was not the past or present location of the iPhone but, rather, the location of WiFi hotspots and cell towers surrounding the iPhone's location. Apple did not have access to the cache on any individual user's phone at any time. Although the cache was not encrypted, it was protected from access by other apps on the phone. Moreover, cache location information was backed up on a customer computer. It may or may not have been encrypted, depending on what the user settings were.

While we were investigating the cache, we found a bug that caused this cache to be updated from Apple's crowdsourced data base even when the location services switch had been turned off. This bug was fixed and other issues, including the size and the back-up of the cache, have been addressed in our latest free iOS software update released last week. In addition, in our next major iOS software release, the location information stored in the device's local cache will be encrypted.

In closing, let me state again that Apple is strongly committed to giving our customers clear and transparent notice, choice, and control over their information, and we believe our products do so in a simple and elegant way. We share the Subcommittee's concern about the collection and misuse of any customer data, particularly location data, and appreciate this opportunity to explain our approach.

I would be happy to answer any questions you may have.

[The prepared statement of Mr. Tribble appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Tribble.

Mr. Davidson.

STATEMENT OF ALAN DAVIDSON, DIRECTOR OF PUBLIC POLICY, GOOGLE INC., WASHINGTON, DC

Mr. DAVIDSON. Thank you, Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee. My name is Alan Davidson, and I am the director of public policy for Google in North and South America. Thank you for this opportunity to testify at this important hearing before this new Subcommittee.

Mobile devices and location services are now used routinely by tens of millions of Americans and create enormous benefits for our society. Those services will not be used, and they cannot succeed, without consumer trust. That trust must be built on a sustained effort by our industry to protect user privacy and security. With this in mind, at Google we have made our mobile location services opt-in only, treating this information with the highest degree of care.

Google focuses on privacy protection throughout the life cycle of a product, starting with the initial design. This is the Privacy by Design concept that was discussed in the last panel.

We subscribe to the view that, by focusing on the user, all else will follow. We use information where we can provide value to our users, and we apply the principles of transportation, control, and security. We are particularly sensitive when it comes to location information.

As a start, on our Android mobile platform, all location sharing for Google services is opt-in. Here is how it works.

When I first took my Android phone out of its box, one of the initial screens I saw asked me, in plain language, to affirmatively choose whether or not to share location information with Google. A screen shot of this process is included in our testimony and on the board over here. If the user does not choose to turn it on at set-up or does not go into their settings later to turn it on, the phone will not send any information back to Google's location servers. If they opt in, if the user opts in, all location data that is sent back to Google's location servers is anonymized and is not traceable to a specific user or device, and users can later change their mind and turn it off.

Beyond this, we require every third-party application to notify users that it will be accessing location information before the user installs the app. The user has the opportunity to cancel the installation if they do not want information collected.

We believe that this approach is essential for location services: highly transparent information for users about what is being collected, opt-in choice before the location information is collected, and high security standards to anonymize and protect information. Our hope is that this becomes a standard for the broader industry.

We are doing all this because of our belief in the importance of location-based services. Many of you are already experiencing the benefits of these services, things as simple as seeing real-time traffic, transit maps to aid your commute, finding the closest gas station on your car's GPS. And it is not just about convenience. These services can be life savers. Mobile location services can help you find the nearest hospital or police station. They can let you know

where to fill a prescription at one in the morning for a sick child. And we have only scratched the surface of what is possible.

For example, Google is working with the National Center for Missing and Exploited Children to explore how to deliver AMBER alerts about missing children to those in the vicinity of the alert. And mobile services may soon be able to tell people in the path of a tornado or tsunami or guide them in an evacuation to an evacuation route in the event of a hurricane.

These promising new services will not develop without consumer trust. The strong privacy and security practices that I have described are a start, but there are several privacy issues that require the attention of government, problems industry cannot solve on its own.

As a start, we support the idea of comprehensive privacy legislation that could provide a basis framework to protect consumers online and offline. And we support action to improve data breach notification instead of the current confusing patchwork of State laws that exist.

And a critical area for Congress, and particularly for this Committee, is the issue of access, Government access, to a user's sensitive information. We live now under a 25-year-old surveillance law, ECPA, first written before web mail or text messaging was even invented. Most Americans do not understand that data stored online does not receive the Fourth Amendment protections given to that same information on a desktop. Nor do users know that the detailed location information collected by their wireless carrier can be obtained without a warrant.

Google is a founding member of the Digital Due Process Coalition, a group of companies and public interest groups seeking to update these laws to meet the needs and expectations of 21st century consumers. We hope you will review its work, and in summary, I will just say we strongly support your involvement in this issue. We appreciate the chance to be here. We look forward to working with you to build consumer trust in these innovative new services.

Thank you.

[The prepared statement of Mr. Davidson appears as a submission for the record.]

Senator FRANKEN. Thank you very much, Mr. Davidson.

Mr. Zuck.

STATEMENT OF JONATHAN ZUCK, PRESIDENT, THE ASSOCIATION FOR COMPETITIVE TECHNOLOGY, WASHINGTON, DC

Mr. ZUCK. Chairman Franken, Ranking Member Coburn, and distinguished Members of the Subcommittee, my name is Jonathan Zuck, and I am the president of the Association for Competitive Technology, and I want to thank you for holding this important hearing on privacy in the emerging mobile marketplace.

As a representative of more than 3,000 small and medium-size IT companies, a former software developer myself, and as spokesman for the people that write the applications for these mobile devices, I want to encourage you to treat the issue of privacy generally and of the mobile marketplace specifically in a holistic manner.

The science of holistic processing is really known best for faces where we are able to recognize an entire face and not just see it as a nose, two eyes, and a mouth. You only need to watch a television commercial for a mobile device, such as an iPod or a Xoom or a Droid phone, to understand that the face of mobile computing is the applications. These ads showcase the more than hundreds of thousands of applications that are available for these devices, some of which we have already heard about in previous testimony today, that allow you to find out where you are, to find services and products that are close to you, et cetera. And these are exciting and dynamic applications that have been made available to users and that many users are using today.

Location-based services and advertising offer a unique opportunity for Main Street businesses as well. A user searching for a particular product or service on their smartphone can receive an ad from a local small business based on their current location data. These ads have the benefit of reaching potential customers at the exact time a purchasing decision is being made for a much smaller cost than the newspaper circulars or TV ad that big-box stores are able to afford.

This dynamic market, valued today at about $4 billion, is projected to be the size of $38 billion by 2015. Application developers are enjoying a kind of renaissance brought by the lower cost to entry in the decision and are often consumer-facing applications. These applications we have all come to enjoy are made predominantly by small businesses—over 85 percent of them are made by small businesses—and not just in Silicon Valley.

The next time, Chairman Franken, you are drawing one of your famous maps, you will be able to reflect that over 70 percent of these applications come from outside of California, including in places such as Moorhead, Minnesota, and Tulsa, Oklahoma.

This is a national phenomenon with international implications for economic growth and recovery. We have an opportunity to meet the President's goals to double exports. We are in a period of rapid experimentation and delivery of new services with a complete focus on the customer. One benefit of small businesses taking the lead here is that they cannot afford to ignore the demands of their customers.

Second, when approaching the issue of data privacy in a holistic manner, I think it is imperative, as we heard from the earlier panel, to remember that there is a whole lot of data. To focus on a particular new type of data collection is to truly cut off our nose to spite our face. There is more data, including location data, in large company data bases than the top thousand mobile applications could hope to collect in a lifetime. In fact, to focus on a particular type of data collection in a particularly new market would necessarily discriminate against the small businesses that are responsible for so much economic growth in the mobile sector while leaving larger players largely untouched.

Finally, there are myriad laws in place to address legitimate privacy and consumer protection concerns, as was raised earlier. Whether it is unfair or deceptive trade practices at the State or Federal level, there are vehicles in place to address transgressions.

Even the use of antitrust has been used in the past to deal with privacy issues.

While I do not agree with all of the recommendations made by the Center for Democracy and Technology, I would agree that any approach to privacy legislation needs to be comprehensive and should focus on the data itself and how it is used and answer these general questions and not focus on a particular means of collection or a particular technology platform.

There is legitimate concern among American consumers about their privacy. As we heard from Chairman Leahy, a number of Americans are concerned about their privacy. I think one of the ongoing frustrations of my constituents, and of small businesses in general, is that they find themselves time and time again doing the time without really having done the crime. It is as though once a week there is some kind of a big company news, like the Sony PlayStation debacle, Epsilon's data loss, and Google with Spy-Fi, collecting children's Social Security numbers, and Buzz. These are the issues that are really causing the concern and fear among customers, not the prospect of getting one more customized ad to their phone.

Despite that fact, the rules that get created inevitably impact small businesses more than our larger brethren. The Google Buzz settlement is a good example of this phenomenon. The FTC has stated it would like to use the Google Buzz settlement as a model for regulation going forward for the entire industry. The true irony is that not only has Google brought this regulation to our doorstep, the level of vertical integration they enjoy makes them immune to most of the consequences. Who is most likely to be affected by a law that affects the transfer of information to third parties? A small business that has to form partnerships in order to provide these services in an ever-changing marketplace or a huge company that can simply buy the third party, thereby circumventing the rule?

The idea of holism dates back to Aristotle, who was the first to say the whole is more than the sum of its parts, and nowhere is that more true than in the mobile computing marketplace. Accordingly, I would like to encourage members of this Committee to take a step back from the headlines of today and look at the issue of privacy in a holistic manner.

Thank you, and I look forward to your questions.

[The prepared statement of Mr. Zuck appears as a submission for the record.]

Senator FRANKEN. Thank you, Mr. Zuck, and thank you all for being here today and for your thoughtful testimony.

Mr. Tribble, last month I asked Apple in a letter why it was building a comprehensive location data base on iPhones and iPads and storing it on people's computers—when they synched up, of course. Apple's reply to my letter will be added to the record.

[The information referred to appears as a submission for the record.]

Senator FRANKEN. But this is what Apple's CEO Steve Jobs said to the press: "We build a crowdsourced data base of WiFi and cell tower hotspots, but those can be over 100 miles away from where you are. Those are not telling you anything about your location."

Yet in a written statement issued that same week, Apple explained that this very same data will "help your iPhone rapidly and accurately calculate its location." Or as the Associated Press summarized it, "'The data help the phone figure out its location,' Apple said." But Steve Jobs the same week said, "Those are not telling you anything about your location."

Mr. Tribble, it does not appear to me that both these statements could be true at the same time. Does this data——

Mr. TRIBBLE. Senator—sorry.

Senator FRANKEN. I understand you are anticipating my question, so I will just ask and then you will answer it. Does this data indicate anything about your location, or doesn't it?

Mr. TRIBBLE. Senator, the data that is stored in the data base is the location of as many WiFi hotspots and cell phone towers as we can have. That data does not actually contain in our data bases any customer information at all. It is completely anonymous. It is only about the cell phone towers and the WiFi hotspots.

However, when a portion of that data base is downloaded onto your phone, your phone also knows which hotspots and cell phone towers it can receive right now. So the combination of the data base of where those towers and hotspots are plus your phone knowing which ones it can receive right now is how the phone figures out where it is without the GPS.

Senator FRANKEN. OK. Mr. Soltani, consumers are hearing this a lot from both Apple and Google, and I think it is confusing because Apple basically said, yes, that file has location, but it is not your location. And when it separately came out that both iPhones and Android phones were also automatically sending certain location data to Apple and Google, they both said, yes, we are getting location but it is not your location.

Mr. Soltani, tell me, whose location is it? Is it accurate? Is it anonymous? Can it be tied back to individual users?

Mr. SOLTANI. Thank you, Senator. I think that is a great question. So, yes, in many cases, the location that this data refers to is actually the location of your device or somewhere near it. While it is true that in some rural areas, this can be up to 100 miles away. In practice, for the average customer or the average consumer, it is actually much closer, on the order of about 100 feet, according to a developer of this technology, Skyhook.

If you refer to Figure 3 of my testimony, you can see an example of this location as identified by one of these WiFi geolocation data bases. I took my location based on GPS and my location based on the strongest nearby WiFi signal in the Senate lobby just out here, and the dot on the left refers to my location as determined by GPS, and then the dot on the right determines my location based on this WiFi geolocation technology, and it was about 20 feet from where I was sitting on the bench. So, you know, depending on how you want to slice it, I would consider that my location.

The files in these data bases contain time stamps that describe at what point I encountered some of these WiFi access points, so they could be used to trace a kind of trail about you.

And then, finally, to the degree that this data contains identifiers, that is sent back, so IP addresses. We heard earlier that the gentleman from the DOJ, he was claiming that IP addresses are

necessary to identify consumers—or criminals. To the degree that those IP addresses are used to identify criminals, they become identifiable, and it is really difficult to call this stuff anonymous. Making those claims I think is not really sincere.

Senator FRANKEN. Because basically if you have—I mean, this location like in your illustration, you see that you are in the Hart Building.

Mr. SOLTANI. Or near the entrance of the Hart Building.

Senator FRANKEN. Yes, yes. And so—well, let me ask Mr. Brookman the same question I asked Mr. Weinstein. My wireless company, companies like Apple and Google, and the mobile apps I have on my phone all can and do get my location or something very close to it. And my understanding, Mr. Brookman, is that in a variety of cases, under current law each of those entities may be free to disclose my location to almost anyone they want to without my knowing it and without my consent. Is that right? And if so, how exactly can they do this?

Mr. BROOKMAN. I think that's correct. As I mentioned before, the default law in this country for sharing of data is you can do whatever you want. The only thing you cannot do is what you have previously promised not to do with that data. So if someone like Apple or Google said, hey, if you give this location data to Google Maps, we promise not to share it with an advertising partner, under that scenario they would be prohibited under the FTC Act from sharing it.

Otherwise, I think for most players in this space, I think it would be very hard to make a legal argument that they were required to have an affirmative requirement not to share data.

Senator FRANKEN. Thank you.

Mr. Davidson and Mr. Tribble, let me ask you one last question because my time is running out. Your two companies run the biggest app markets in the world, and both of your companies say you care deeply about privacy. And yet neither of your stores requires that apps have a privacy policy. Would your companies be willing to commit to requiring apps in your stores to have a clear, understandable privacy policy? This would by no means fix everything, but it would be a simple first step and would show your commitment on this issue. Mr. Davidson.

Mr. DAVIDSON. Thanks. It is a great question. I would be happy to take it back. I think it is an extremely important issue that you raise about application privacy. At Google, we have tried to maximize the openness of our platform to allow lots of different small businesses to develop applications. We have relied on a permission-based model at Google so that before an application could get access to information, they have to ask permission from the user.

You are asking about the next step, which is whether we put affirmative requirements on applications, and I would just say I will take that issue back to our leadership. I think it is a very good suggestion for us to think about.

Senator FRANKEN. Mr. Tribble.

Mr. TRIBBLE. Yes, I think that is a great question. What we do currently is we contractually require third-party app developers to provide clear and complete notice if they are going to do anything with the user's information or device information. So if you want

to become an Apple developer and put an app in the app store, you sign an agreement with Apple that says you are going to do that.

Now, it does not specifically require a privacy policy, but what I will say is that a privacy policy in this general area is probably not enough. I agree with the earlier panel that what we need to do, because people may not read a privacy policy, is put things in the user interface that make it clear to people what is happening with their information, and Apple thinks this way. For example, when an app is using your location data, we put a little purple icon right up next to the battery to let the user know that. Now, we saw that in the privacy policy too, and the app should say that too. But we also could put something in the user interface to make it even more clear to the user.

We also have an arrow that shows if an app has used your location in the last 24 hours, so transparency here goes beyond just what is in the privacy policy. It is designed into the app and the system information, itself provides feedback to the user about what is happening with their information.

Senator FRANKEN. Thank you. Just a yes or no, Mr. Soltani. Isn't it true that there is no mechanism for iPhones to notify users that their apps can disclose their information to whomever they want?

Mr. SOLTANI. Yes.

Senator FRANKEN. OK. Thank you.

Mr. SOLTANI. It is true.

Senator FRANKEN. Thank you.

Senator Coburn.

Senator COBURN. Let me defer to Senator Blumenthal. I have a meeting that I have to take for about five minutes, and then I will be back in.

Senator FRANKEN. Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman. Thank you, Senator Coburn.

I want to focus on really the very broad area or issue of trust that Mr. Davidson raised, which I think goes to the core of much of what you do with the consent and acquiescence of consumers and, most particularly, the practice and goal of building wireless network maps. Both Apple and Google are engaged in that business activity, are you not?

Mr. TRIBBLE. Yes.

Mr. DAVIDSON. Yes.

Senator BLUMENTHAL. And, in particular, Mr. Davidson, I want to ask some questions about the Google Wi-Spy experience, scandal, debacle. All three terms have been used to refer to it. In particular, as you well know—and now we all know—for three years Google intercepted and collected bits of user information payload data—e-mails, passwords, browsing history, and other personal information—while driving around taking pictures of people's homes on the streets in the Street View program. The company first denied that it was collecting this information, did it not?

Mr. DAVIDSON. It did. We did not believe that we were—we did not know that we were.

Senator BLUMENTHAL. And then it denied that it was collecting it intentionally. Is that true?

Mr. DAVIDSON. I think we still believe we were not collecting it intentionally.

Senator BLUMENTHAL. And, in fact, this personal data and the interception and downloading of this personal data is contemplated, in fact, by a patent application that has been submitted by Google to both the U.S. Patent Office and internationally, does it not?

Mr. DAVIDSON. I am not specifically familiar with the details of the patent application.

Senator BLUMENTHAL. I think you have been provided with a copy——

Mr. DAVIDSON. Is that what this is here?

Senator BLUMENTHAL. Maybe you could have a look at it. Do you recognize the document? Have you seen it before?

Mr. DAVIDSON. I have not seen this document before, but I am probably roughly—I have not seen this document before.

Senator BLUMENTHAL. Are you familiar with the goal that it describes of, in fact, pinpointing the location of wireless routers to construct a wireless network map by intercepting and downloading the payload data in precisely the way that Google denies having done?

Mr. DAVIDSON. No, I am not—I apologize. I am not familiar with that aspect of this or really anything relating that to this patent's content, to the content of——

Senator BLUMENTHAL. Are you aware that this process may have been used in the Street View program to collect private confidential information and use it to construct the wireless network route?

Mr. DAVIDSON. I would be very surprised. I think it—we have tried to be very clear about the fact that it was not our policy to collect this information; it was not the company's intent to collect the content or payload information. I think we have been very specific about the fact that we never used that information.

As you indicated, people at the company were quite surprised and, honestly, embarrassed to find out that we had been collecting it. So we have said before, this was a mistake, that we did not intend to collect this information, and we have tried very hard to work with regulators to make sure we are now doing the responsible thing. We have not used it, and we are working with the regulators around the world to figure out what to do with it, and in many cases we have destroyed it.

Senator BLUMENTHAL. Why would the company then submit a patent application for the process—that very process that it denies having used?

Mr. DAVIDSON. I am sorry I cannot speak to the specifics of this patent. We were not aware that this was a topic for today's hearing. But I will say generally we submit patent applications for many, many different things. Often they are fairly speculative. We probably do, I do not know, hundreds of patent applications a year, certainly scores. And it would not be surprising at all that in this area that is so important we would be looking for innovative ways to provide location-based services. But it was certainly—as we have said publicly, it was a mistake, and we certainly never intended to collect payload information.

Senator BLUMENTHAL. Well, in fact, the payload information would be extremely valuable in constructing this wireless network map, would it not?

Mr. DAVIDSON. I am not sure that we would say that. I think that what is most important is basically having the identification of a hotspot and a location, which is what we were collecting, and that is what we have used to create this kind of data base, as others have. And it is not obvious that small snippets of a few seconds of whatever happens to be broadcast in the clear from somebody's home at any given precise second when you are passing by with a car would necessarily be that valuable. And I think we certainly never intended to collect it.

Senator BLUMENTHAL. Would it be valuable, in your opinion, Mr. Tribble, to have that kind of payload data in constructing a wireless network map?

Mr. TRIBBLE. I am actually not sure how valuable——

Senator FRANKEN. Turn your microphone on.

Mr. TRIBBLE. Yes, Senator, I am actually not sure how valuable it would be. We do not collect that or use that in our mechanisms for geolocating, and, in fact, I checked with the engineering group, and they said it would be—they are not sure how you would do that. But they probably have not seen the patent, so I cannot really, I guess, specifically answer your question.

Senator BLUMENTHAL. Let me ask Mr. Brookman and Mr. Soltani whether you have an opinion as to whether payload data would be useful in strengthening the location network or map.

Mr. BROOKMAN. I am not a technologist so I will mostly defer to Mr. Soltani. My instinct is that I do not think that it would be. The primarily interesting fact is that here is a wireless access point. They may need to sense that it is sending information out technologically, but I do not believe that the content of that communication would be valuable at all.

Mr. SOLTANI. I would concur with Justin. I think the small differentiation is—what you are referring to is whether the header information, which is not necessarily—there is a question of whether that is payload data. So Google collects the information about the hot spot, which includes the header information about the MAC address or the identifier for that hotspot, and I think that is the question, whether that is payload data.

I would feel like it is also not payload data, but that remains to be determined by others.

Senator BLUMENTHAL. Let me turn back then to Mr. Davidson. What are the plans that Google has to use or dispose of the information that has been downloaded and collected?

Mr. DAVIDSON. We are in active conversation with many regulators, including your former office in the State of Connecticut, but regulators around the world. Some of them have asked us to destroy the data, and we have done so. Some of them are continuing their investigations.

Our intent is to answer all the questions of any regulator who has got an interest in this fully. We do not intend to ever use this data. We intend to dispose of it in whatever form regulators tell us we should.

Senator BLUMENTHAL. And would you agree that collection of this data violates privacy rights and that it may, in fact, be illegal?

Mr. DAVIDSON. I think our position was that it was not illegal, but it was not our intent, either, and it was not how we expect to operate our services.

Senator BLUMENTHAL. If it was not illegal, do you not agree it should be?

Mr. DAVIDSON. I think this raises a really complicated question about what happens to things that get broadcast in the clear and what the obligations are about people hearing them. And I think it is a complicated question. It is an important question. But I think we have to be careful about it. I think the law appropriately says—regulates—I believe it regulates the use of that information. And as I have said before, we have no intention to use it.

Senator BLUMENTHAL. I will have additional questions, Mr. Chairman. My time has expired and I appreciate your indulgence. In the meantime, I would like these patents to be made a part of the record.

Senator FRANKEN. Absolutely.

[The patents appears as a submission for the record.]

Senator FRANKEN. The Ranking Member.

Senator COBURN. Thank you, Mr. Chairman.

This is for both Apple and Google. You both have requirements for the people that supply apps for your systems. How do you enforce the requirements that you place on them? Specifically, how do you know that they are keeping their word? How do you know they are not using data different than what they have agreed to? How do you know they are not tracking?

Mr. TRIBBLE. Yes, Senator, so Apple curates the apps that are in our store. The way people get apps on their phone is that they are in the Apple apps store.

As I mentioned, we have requirements for the app developers. What we do is we examine apps, look at them. We do not look at their source code, but we run them, we try them out, we examine them before we even put them into the app store. If they do not meet our requirements, that——

Senator COBURN. I understand that. But once they are in your app store——

Mr. TRIBBLE. Once they are in the app store, we do random audits on applications. Now, we have 350,000 apps. We do not audit every single one, just like the Federal Government does not audit every single tax return. But we do random audits and do things like examine the network traffic produced by that application to see if it is properly respecting the privacy of our customers.

If we find an issue through that means or through public information, a blog, or a very active community of app users, we will investigate. And if we find a violation of our terms, including privacy terms or specific location handling terms, we will contact—we will have contacted them during the investigation and hopefully gotten them to fix it. But if they do not, we will notify them that their app will be removed from the store within 24 hours, and we will do that.

Now, in fact, the overwhelmingly common case is that the app developers are highly incentivized to stay in the apps store. So dur-

ing the investigation or if we warn them, typically they correct, and often that correction involves making sure they pop up a notice panel telling the customers what they are doing.

Senator COBURN. Mr. Davidson.

Mr. DAVIDSON. So we have taken a slightly different approach at Google. We have strived to make sure that our platform is as open as possible, and we have chosen not to try to be a gatekeeper in terms of what applications people get access to. That is striking a balance, but we have tried to maximize openness, and we have taken a different approach to try to protect consumer privacy, which is to use the power of the device itself to make sure that people know what information is being shared. And so the device itself will tell you, when you want to install an application, what that application wants to have access to. And that we believe is a very powerful form of policing for users. But we do not then generally go back and try to make sure that every application does what it says it is going to do because we have, as I say, a large number, but we are also really trying to maximize the ability of small app developers to get online.

Senator COBURN. Is that notification when you download that app in plain English where it is easily understood? Or is it a 10-page deal that everybody scrolls down to and says, "I accept"?

Mr. DAVIDSON. It is a terrific question. We have tried really hard to avoid that, so we do not show that ten-page thing that the lawyers write that says all the different things that may happen. It is plain language. It is rarely more than a screen. Sometimes you have to scroll down a little bit. And it says very specifically what pieces of information—not just location information, but all types of information that might be coming from the phone that that application has sought access to.

And I will tell you personally I have seen applications that I have rejected, and I think hopefully a lot of people do this, when you say, well, why does my solitaire program need my contact data base? It does not and I should reject it.

Senator COBURN. What is the motivation for the app producer—and, Mr. Zuck, you can comment on this, too—to have that information? Is it so they can re-use it and sell it?

Mr. DAVIDSON. I am sure that it is going to be a combination of things, and I am sure that in many cases they will be providing valuable services, so, you know, Foursquare or other location services that let you know if your friends are nearby. Twitter lets you look at tweets that are near your location. There are really valuable services out there that are going to be provided. Sometimes people might be using data to serve ads better or to build a data base of their own, and that is the kind of thing I think consumers need to decide whether they want to make that trade.

Senator COBURN. Mr. Tribble, do you want to comment on that?

Mr. TRIBBLE. I think that there are a variety of reasons why third-party apps would want that kind of information and a variety of things that they would do with it. Again, what we require the apps to do is to tell the users before they do that. We let them have a way of choosing not to do it or to change their mind later. So it is an area where there is a lot of innovation. I am sure Mr. Zuck

can tell you about that. And it is an important area in terms of privacy and rapidly evolving.

Senator COBURN. Mr. Zuck.

Mr. ZUCK. Thank you, Senator. It is a very good question, and it is exciting here at the kids' table to be heard and not just seen, I suppose.

Most of the privacy policies of these small businesses reflect the fact that most of these businesses are not collecting personal information, and those that are, very often their privacy policies extend from their other online presences or websites, et cetera.

As to your question about the use and why they do it, most of the time it is some overt process where someone is actively checking in or doing something very specific where they know they are sharing information in order to get information. But the other use of the information is to allow for partnerships and revenue streams from ad networks. And so data is not stored by these small businesses in most cases, but actually transferred back to the likes of Google and Apple that are the ones that are actually accumulating the large data bases of data about these users.

The one thing that is worth noting, though, is that this is another bite at the apple that these folks have with application developers and that there are terms of services for those ad networks as well. So that in sharing the information back to Apple or Google, there are restrictions on the kind of policies we have to have in place in order to share that information back with that ad network and to make use of that service.

Senator COBURN. All right. Thank you very much. I will have additional questions for the record for Mr. Brookman and Mr. Soltani.

Senator COBURN. Senator Whitehouse.

Senator WHITEHOUSE. Thank you very much.

It strikes me that we are in a very new area in trying to think about what our take-off point should be. What existing models are a good analogy for where we are right now and where we should go is an interesting discussion to have, and I encourage each of you to take that as a question for the record, if you could for me, and get back to me in writing because that is a longer discussion than we have time for. But, you know, if you want to sell pharmaceuticals in this country, you can do so, but you have to disclose their side effects. If you want to operate on somebody in this country, you can do so, but you have to get their consent and list the things that could go wrong in the surgery. If you want to sell a consumer product in this country, you have to put appropriate warnings on, and if the product is dangerous, you have got to pull it back off the market. If you want to sell stock in this country, you have got to file a proper SEC filing so people know what the financial information behind the stock offering is and they can make an intelligent decision.

In all of those different ways that we regulate conduct, we are trying to make, to your statement, Mr. Davidson, as open as possible a market, but not at the expense of people who are trying to take advantage of people.

And so it worries me that the principle—we hear it from you in terms of "as open as possible." We also hear it from the ISPs in terms of, "Do not blame us for what comes across the pipes," even

if it is crawling with malware and is really putting even potentially our National security at risk. "We are just providing a service. We just want anything to go through." And that is not an argument that we allow to stand in pharmaceuticals, in consumer products, in surgery—really anywhere. We build an arena in which the market can work, but we make sure that the boundaries of the arena are the boundaries of safety. And I think we really need to be working on those boundaries, and I think that "as open as possible" is simply not an adequate standard to this task—as open as possible, yes, but within what controls. And I think that is the question that we have to be focusing on, and it is complicated by the fact that some of these things you want and you are choosing them; some of it rides along with that. I do not know how effective your program that allows you to check in and out, tell you what things it has access to, is in terms of the real-life consumer. What does a 14-year-old loading an app know about all these choices? How informed is that choice? So I am not sure that is a boundary that I am perfectly comfortable with.

Mr. Tribble mentioned that you could change your mind later in the Apple system if you saw that something was going wrong. I am not sure, can you change your mind in yours? Or——

Mr. DAVIDSON. Absolutely. As I mentioned in my written and oral——

Senator WHITEHOUSE. How do you get prompted to——

Mr. DAVIDSON [continuing]. You can easily go back and change——

Senator WHITEHOUSE. How do you get prompted to once you have loaded the app?

Mr. DAVIDSON. Well, you can remove the application very, very easily. You can also change your settings in terms of, for example, the use of the location services that Google provides.

Senator WHITEHOUSE. But you have to be aware of it.

Mr. DAVIDSON. Absolutely. There is——

Senator WHITEHOUSE. So if you are not aware that somebody is selling your location information to somebody you are not interested in having it, you do not really get a second bite at that apple.

Mr. DAVIDSON. Well, and I think this is a tremendously important area, about the need to educate our consumers and users better because we believe you are right, that a lot of users do not understand all this. We have tried to make it very simple, and we have tried to strike the right balance. I do not think we—we do not say openness at all costs. What we have said is we are trying to maximize—I do not know if "maximize" is the right word, but we are trying to increase openness. We tried to create a very open platform, and it is a different approach. It is not no holds barred. We take certain—we do have a content policy for our market. But I think the question is what is the appropriate way—who are the appropriate actors to go after? We do not go after trucking companies because they happen to carry faulty goods. We go after the manufacturers of those goods. And I would just say we are trying to strike the right balance, and we also need to really educate consumers. That is why a hearing like this is honestly so important because it does shed a lot of light, even as we try to give people information.

Senator WHITEHOUSE. You do go after the trucking company if the company knew what it was carrying.

Mr. DAVIDSON. And I think this is——

Senator WHITEHOUSE. And Google is in a better position to know what is being carried as a professional company that specializes and has vast resources than a 17-year-old who has been told by his friend that this is a cool app to load. So I would not be satisfied—I do not think that is a comfortable analogy either for you to rely on.

The other thing, if somebody wants to take control of your computer and slave it to their botnet, they will try a lot of different ways to do it, and many of the ways in which they try this stuff will involve broadcast to thousands of people, and most people are careful enough to know better than to open the attachment or whatever. They are getting more sophisticated, and they are starting to add more personal data, so it is getting harder and harder to sort that out. But ordinarily you could have a success rate of only 1 in 1,000 and still be a pretty successful propagator of a botnet.

And so it seems to me that there are some things for which even a very high failure rate is still not good. So even if 999 of 1,000 of your customers said, "Oh, I do not want them to do that," if somebody is putting these apps up not for the facial purpose, for the stated purpose, but because they have loaded a bunch of other stuff behind it that they want to use for an ulterior motive, what I called earlier a Trojan horse, you take it for one reason but that is not really why they are doing business with you. That is just their way to get in the door and into your computer and being able to take economic advantage of your information.

It seems to me that there is some line that we want to draw that is an absolute line that says, even if you are—you know, you really should not be in a position where you are agreeing to this with as little information as you have, in the same way that you try to protect people from having their computers slaved to botnets by spam emails.

So, again, I think we need to consider a little bit more sort of what our model is going to be here and then work off of that, and all I can say is that I have not yet heard a model here today that is convincing to me that it adequately protects both the Internet itself and the privacy interests. We have talked a lot about privacy, but, frankly, it is not just privacy that is at issue here. Once somebody is in your computer with an application, there are a lot of other ways they can cause mischief, and it could be all the way to outright malware rather than just some—it could be something that is ultimately illegal, not just something that is immediately unwelcome.

So, anyway, I want to just thank Chairman Franken for having this hearing. I think it has been very interesting, very significant, and I think it is an issue where we have got a lot of work to do ahead of us, and I want to appreciate the participation of all of you. We all bring different perspectives to this. I do not think anybody's perspective is yet ideal. But together and working hard on this, I think that we can get something accomplished that will make the Internet safer and make people less vulnerable as consumers to

abuse and make sure that it is clearer that you are getting what you pay for or what you load up when you choose to take on these applications.

Much appreciation to the Chairman for his leadership on this.

Senator FRANKEN. Thank you, Senator Whitehouse.

By the way, I apologize to the witnesses. I had to step out for a meeting on Minnesota flooding.

Senator Schumer has stepped in, and I recognize you.

Senator SCHUMER. Thank you. First let me thank you, Mr. Chairman, for having this very important hearing, and there are so many different types of issues and questions that have come up because we are in this brave new world where information is available much more freely and that creates new privacy concerns, and creating the balance is one of the most important things we can do at the beginning of this century. So I look forward to your leadership and the leadership of Senator Coburn as we try to balance the important benefits, and I am so glad you have stepped into this place.

I always tell people that the Senate has so many different vacuums that, you know, somebody who is interested can sort of step into, and this is a classic example. So thanks for your leadership, Al.

I am glad that the representatives—I have a particular area that I know some of you know I care about. There are a lot of these areas I care about, but I am going to talk on a couple today. Apple and Google have come here, and I thank you both for that. I want to ask about a slightly different aspect of balancing technology with public safety, and that is the smartphone applications that enable drunk driving.

As you know, several weeks ago a number of my colleagues and I—Senators Udall, Lautenberg, Reed, and I—wrote letters to your companies calling your attention to the dangerous apps that were being sold in your app stores and asking you to take immediate—to immediately remove them. The apps we were talking about endangered public safety by allowing drunk drivers to avoid police checkpoints. I do not have to go into how bad drunk driving is in our country, and I just read those newspaper articles, particular at prom time and Christmastime, of parents just looking so forlorn because they have lost a kid to drunk driving.

Anyway, the DUIs that were popping up in stores were terrifying because they undermined drunk-driving checkpoints. The apps, they have names like Buzz and Fuzz Alert, and they are intended to notify drivers in real time when they approach police drunk-driving checkpoints. There is only one purpose to these. We know what that is, and that is, to allow drivers to avoid the checkpoints and avoid detection. People often think twice about drunk driving, driving while drinking, because they know they could get stopped, with all the consequences, and these apps enable them not to.

We brought these to the attention of RIM. They pulled the app down. I was disappointed that Google and Apple have not done the same, and I would like to ask you how you can justify to sell apps that put the public at serious risk. I know you agree with me that drunk driving is a terrible hazard, right? And I know each of your companies has different reasons for not removing these apps, so I

would like to discuss them with you separately. First, Mr. Davidson, tell me your reasoning why Google has not removed this kind of application.

Mr. DAVIDSON. I will start by saying we do take this issue very seriously——

Senator SCHUMER. I know. I do not doubt that.

Mr. DAVIDSON [continuing]. And we appreciate you raising it. As I actually just discussed with Senator Whitehouse, we have a policy on our application store, our application market and on our platform where we do try to maintain openness of applications and maximize it, and we do have a set of content policies regarding our Android marketplace. And although we evaluate each application separately, applications that share information about sobriety checkpoints are not a violation of our content policy.

Senator SCHUMER. Let me ask you this: Would you allow an app that provided specific directions on how to cook methamphetamines? That does not explicitly violate the terms of your service explicitly but generates a public safety hazard.

Mr. DAVIDSON. I think it would be—it would be fairly fact specific. We do look at these things specifically. I think applications that are unlawful or that, you know, directly related to unlawful activity, I think we do take those down.

Senator SCHUMER. So let me ask——

Mr. DAVIDSON. Malware we do take down. You are right. But we do have a fairly open policy about what we allow.

Senator SCHUMER. Well, no one is disputing fairly open, and that is the motto of Google, and, you know, you are a company that has paid the price in a certain sense for those beliefs. So everyone respects the company. But my view is even under your present terms of prohibiting illegal behavior, this app would fit. By why wouldn't you then change the app to include at least this specifically so it does not—you know, I know if you had to draft generalized language, it might be trouble. But why wouldn't you do that?

Mr. DAVIDSON. Again, I think we have a set of content policies. We try to keep them broad, and I will just say you have raised what we think is an extremely important question. It is a question that we are actively discussing internally, and I will take this back and your concern back to our most senior leadership.

Senator SCHUMER. So you will look at—if you do not believe under your current rules that this would be prohibited, you would look at specifically, at least narrowly trying to eliminate this app.

Mr. DAVIDSON. Yes.

Senator SCHUMER. You agree it is a terrible thing; it is a bad thing.

Mr. DAVIDSON. We agree it is a bad thing. I agree it is a bad thing, Senator.

Senator SCHUMER. And it probably causes death.

Mr. DAVIDSON. Senator, I think this is an extremely important issue.

Senator SCHUMER. All right. Let us go to Mr. Tribble. Tell me why you have not. Different reasoning. That is why I am doing it separately.

Mr. TRIBBLE. Well, Senator, I share your abhorrence of drunk driving. As a physician who has worked in an emergency room, I

have seen firsthand the tragedy that can come about due to drunk driving, so we are in complete and utter agreement on that. And, you know, Apple in this case is carefully examining this situation. One of the things we found is that some of these applications are actually publishing data on when and where the checkpoints are that are published by the police departments.

Senator SCHUMER. No, not in the same time sequence.

Mr. TRIBBLE. In some cases the police department actually publishes when and where they are going to have a checkpoint. Now, not all of them do that, and there are variances to—there are theories on why they——

Senator SCHUMER. How many police departments do that?

Mr. TRIBBLE. I have seen a map, for example, San Francisco, Ninth and Geary, we are going to be having a checkpoint tomorrow night. On the Web.

Senator SCHUMER. Do they publish all of them?

Mr. TRIBBLE. I do not know. So we are looking into this. We think it is a very serious issue.

Senator SCHUMER. It is sort of a weak read, I think.

Mr. TRIBBLE. Well——

Senator SCHUMER. I would bet to you that I do not know of a police department that in real time would publish where all these checkpoints would be. It would make no sense. And they publish it on their Web site?

Mr. TRIBBLE. As you know, they often publish in general that they are doing it. It was surprising——

Senator SCHUMER. But what does that——

Mr. TRIBBLE. That means that they believe that these checkpoints provide a deterrent effect and that wider publicity——

Senator SCHUMER. But that is a different type of checkpoint.

Mr. TRIBBLE. I agree. I am just saying we are in the process of looking into it. We think it is very serious. We definitely have a policy that we will not allow—encourage illegal activity. And——

Senator SCHUMER. Apple has pulled bad apps before.

Mr. TRIBBLE. Absolutely.

Senator SCHUMER. OK. You pulled one even about tasteless jokes. Well, this is worse than that, wouldn't you say?

Mr. TRIBBLE. Well, I would say that in some cases it is difficult to decide what the intent of these apps are. But if they intend to encourage people to break the law, then our policy is to pull them off the store.

Senator SCHUMER. Then I would suggest that you look at—just keeping that policy as is, it is a little different situation than Mr. Davidson. You would find that the intent of these apps is to encourage people to break the law.

Mr. TRIBBLE. And I will take that back, and we will——

Senator SCHUMER. And it is different. I know my time is up. I apologize. And I would encourage you to make a distinction between a police department that says, "Well, we usually have a checkpoint at Ninth and Geary," and an app that just talks about where the new checkpoints are and in real time. And you say they publish it.

Mr. TRIBBLE. Yes.

Senator SCHUMER. They publish it two days later.

Mr. TRIBBLE. No, I understand that distinction, and I agree that is different.

Senator SCHUMER. So you, too, Apple will take a serious look at this.

Mr. TRIBBLE. Yes, we will.

Senator SCHUMER. I would like if you folks, both of you, could get me an answer, say two weeks from now, as to what your—is that too soon?

Mr. DAVIDSON. We could certainly give you a progress report.

Mr. TRIBBLE. Yes.

Senator SCHUMER. How about a month from now as to what your internal examination has come up with, OK?

[The information referred to appears as a submission for the record.]

Senator SCHUMER. I thank you and I thank my colleague for indulging me in an extra two minutes. Thanks.

Senator FRANKEN. I was actually saying that we were going to go to a second round, not that you were two minutes over. I would never do that to the distinguished Senator from New York.

I am going to indulge my prerogative as the Chair and go to a second round.

Mr. Tribble, when you download an app on Android or an Android machine, it tells you if that app will access your location, your calendar, your contact list, and you get a chance to opt out of those. But an iPhone only asks you if you want to share your location with an app, nothing else. Don't you think it would be helpful for Apple to inform consumers if an app will be able to get information from their calendars or address books? What more can Apple do to inform consumers of the information that an app can access, do you think?

Mr. TRIBBLE. Well, in the case of those things that—you know, the app, we encourage, as I mentioned, and even require the app provider themselves to give notice and get consent from the consumer before they do that. Different from Google in those cases, we do not provide or attempt to provide technical means in all cases to prevent the app from getting at any and all information. In fact, we think that would be very difficult.

However, specifically in the case of location, we do make sure that every single time an application—or for the first time an application asks to get access to that user's location, it pops up that dialog box that says, "This app would like to use your location, yes or no." So I would say two things there. One of our priorities in this case has been on the especially sensitive nature of location and to provide technical measures or attempt to on the phone to provide that notice every single time when the app first asks.

In the case of other information which may also be personal information, but maybe not, you know, to the same extent as where am I right now, we require the app to give notice and to get consent from the user, but we do not have a technical means to require that. And if we—it is not that we would not want to. We think that is difficult, and it is especially difficult because when you start to do that for every little piece of information, the screen that the user is confronted with in terms of yes/no, yes/no, yes/no potentially becomes very long and complex.

Senator FRANKEN. Google has a screen that contains a number of those, and it seems to work for you guys, right?

Mr. DAVIDSON. It works for us guys, yes.

Senator FRANKEN. OK. Mr. Tribble, the Ranking Member asked you how your companies enforce your own rules for apps. When you were in my office yesterday—and thank you for coming—I actually asked you this question. How many apps have you removed from your App Store because they shared information with third parties without users' consent?

Mr. TRIBBLE. As I mentioned to Senator Coburn, of course, our first defense is to not put them there in the first place, but if we find an app, we investigate, we work with the developer to get them to give proper notice, and we tell them at some point, if we find them violating, "you are going to be off in 24 hours." In fact, I think all of the applications to date or the application vendors to date have fixed their applications rather than get yanked from the apps store in those cases.

Senator FRANKEN. So the answer to my question is zero?

Mr. TRIBBLE. Is zero.

Senator FRANKEN. OK. Thank you.

Mr. Soltani, let me ask you a different question. Of all the things that you have seen, what is the most serious privacy threat that mobile devices pose today?

Mr. SOLTANI. Senator, thank you for your question. I think the biggest take-away from this is that consumers are repeatedly surprised by the information that apps and platforms are accessing. Consumers are entrusting their computers and phones and other devices with a great deal of personal information, and to the degree that these platforms are not taking adequate steps to make this clear to consumers that others in the pipeline have access to this information, I think that is a problem. We have talked about the apps where, you know, a certain app might need access to—I think the example was it needed access to your location information and you said no. I do not think consumers would know whether apps would need access to certain types of information or not or could make those definitions clearer.

Kind of stemming from that, we see the—it sounds like the providers of these platforms are actually surprised as well that they are collecting information. In the case of Street View, they were surprised that they were collecting the WiFi information, and in the case of the recent Apple episode, they were surprised—even a year ago they responded to this issue—that they were collecting information for a year.

And so I think, you know, we need improved transparency on this stuff, and in order to do that, we need clear definitions of what things like "opt in" mean. For example, the check box being checked by default and you have to uncheck that, is that really kind of opt in or is that opt out? Clear definitions——

Senator FRANKEN. It sounds like opt out to me.

Mr. SOLTANI. Right. Clear definitions of what location is, you know, if it gets you within 20 feet, is that your location? And then most importantly, clear definitions of what "third parties" and "first parties" mean in this context.

Senator FRANKEN. Well, could you describe the results of the *Wall Street Journal's* investigation into mobile apps? Specifically, can you describe the information that apps are getting from users and sharing with third parties? And can you tell us—you said they are surprised—if the average user has any idea that this is happening?

Mr. SOLTANI. Right. So I do not think most consumers would know that apps would access things like your location information or information stored on your device.

Senator FRANKEN. So your address book or——

Mr. SOLTANI. Your address book, your contacts list. And then there was a case where Facebook, you would install the Facebook app, and it would synchronize your entire address book up to Facebook server. I think people were kind of surprised by that functionality. I do not think people realized what is the data that is held on the phone versus the data that is transmitted to websites, and then, even more, transmitted to downstream ad companies and other entities that are not even the website that builds the app.

I think ultimately this might be an issue with regard to kind of the incentives are mixed. So in this context, we have Apple and Google as platform providers, but they are also advertisers, and they also make apps. And so in the example earlier where it was the truck driving and making problematic products, I think in this case we have the same companies that are the truck and the product, and it is really weird to figure out what the incentives should be for them to kind of do the right thing and make intelligent defaults. I think we have seen the defaults fall in favor of what is in their best interest—obviously so. They are companies, right? They are commercial entities.

Senator FRANKEN. Thank you, Mr. Soltani, and thank you all.

Senator Blumenthal.

Senator BLUMENTHAL. Thank you, Mr. Chairman.

I want to thank all of you again for being here and for your very, very useful contribution to this hearing.

Just by way of brief footnote to your conversation, Mr. Tribble, Dr. Tribble, earlier with Senator Schumer, you may or may not be aware, but sometimes police departments actually publicize checkpoints so that drunk drivers will go to alternative routes where they do not publicize the checkpoints. So there may be more strategy than you may be aware in some of the law enforcement practices that are involved here. But I welcome both your and Mr. Davidson's willingness to come back to Senator Schumer with your response. I think that is very welcome and commendable.

I also want to welcome and commend Google's response on the notice issue in case of breaches, which I think is a very important source of support for notice legislation, and would ask, Dr. Tribble, I do not think I saw in your testimony—I may have overlooked it—any reference to the requirement for notice in case of breaches of confidentiality. Would Apple likewise support that kind of legislation?

Mr. TRIBBLE. I am actually not the policy person at Apple, but what I will say is that, in general, we think it is extremely important that information kept on our servers stays secure, and we do

a lot to make sure that that is the case. And we think that if—I personally think if customers are at risk from important information that is leaked from servers, I, for example, as a consumer would like to know.

Fortunately, Apple has not—you know, what we are discussing is not that here, but if that were to happen, I think that would be something that consumers would want to know about.

Senator BLUMENTHAL. Well, would it be Apple's practice to notify consumers in case of a breach as soon as possible?

Mr. TRIBBLE. Yes, I think we are—I believe we are subject to at least various State laws along those lines, breach notification, and although it is not my area of the company, I certainly believe that—I know we would comply with that and notify in case of a breach.

Senator BLUMENTHAL. And, again, I will be submitting questions that I am hoping that all the witnesses will respond to, and we are late into this hearing, but I would be very interested in knowing, and would welcome your response here if you can do it briefly, what additional measures you would suggest. As you may have heard earlier, we asked the panel before yours about requiring security measures, privacy by design so to speak, as well as remedies such as credit freezes, credit monitoring, insurance, in case of breaches and to prevent such breaches and would welcome any comments from the panel—or not. Whichever you would prefer.

Mr. BROOKMAN. Fortunately, I actually testified on this issue last week, so I have done a little bit of thinking about it.

From a consumer perspective, there is actually already a pretty strong legal regime in place to require reasonable security practices. The FTC has brought 30-some-odd cases where companies failed to adequately secure data. And for data breach notification, 46 or 47 States have versions in place. So the legal regime right now already has pretty strong protections in place. The things we would probably look for are, one, more authority to the FTC, maybe greater capacity to bring more cases. I think the 35 they brought are great, but obviously more would be better. And penalty authority especially as well. The FTC does not have the ability to get civil penalties for violations of the FTC Act. I think if there were a strong sword, a little stick, I think you would see better practices.

Also, I think we would like to see other of the fair information practices put into law. So one idea that we keep bringing up is this idea of data minimization. If you have data sitting on your servers and you do not need it anymore, get rid of it. In both the Sony and the Epsilon case, data breach cases, it seemed they were holding old data they did not need anymore. Sony had a 2007 data base with credit card numbers that they were not even using. Epsilon was keeping email addresses of people who had previously opted out. I had personally got email from companies I had opted out from years ago saying, "Oh, by the way, your data was breached here."

So I think putting into law protections for data minimization and stronger FTC authority would be valuable things here.

Senator BLUMENTHAL. Mr. Brookman, did Sony have in place adequate safeguards?

Mr. BROOKMAN. As I said, I am not a technologist. There have been a lot of press reports indicating that there are things they should have done better. Their servers were not patched to the latest security software. They were holding old data, and their password verification system probably should have been stronger.

I am probably not the best person to testify to that. It is easy for me to sit back and say now that it seemed inadequate, but there are definitely strong security minds in this space who have criticized what they have done.

Senator BLUMENTHAL. Well, in fact, they acknowledged that much better, stronger safeguards should be in place going forward. Whether that is an implicit acknowledgment as to the inadequacy previously, we cannot ask them because they are not here today. But certainly they are going to upgrade or at least have promised to upgrade their safeguards.

Mr. BROOKMAN. Yes, they have said that they are going to put better protections in place, and so if there were maybe a greater consequences to data security breaches such as FTC penalty authority, then hopefully companies would think about it more in advance than trying to append security and privacy after the fact.

Senator BLUMENTHAL. I have a bunch of other questions which I will ask the witnesses and will not detain you to as now, but thank you very much, Mr. Chairman.

Senator FRANKEN. Thank you, Senator Blumenthal.

The hearing record will be held open for a week. In closing, I want to thank my friend, the Ranking Member. I want to thank all of you who testified today. Thank you all.

As I said at the beginning of this hearing, I think the people have a right to know who is getting their information and the right to decide how that information is shared and used. After having heard today's testimony, I still have serious doubts that those rights are being respected in law or in practice. We need to think seriously about how to address this problem, and we need to address this problem now. Mobile devices are only going to become more and more popular. They will soon be the predominant way that people access the Internet, so this is an urgent issue that we will be dealing with.

We will hold the record, as I said, open for a week for submission of questions, and this hearing is now adjourned.

[Whereupon, at 12:39 p.m., the Subcommittee was adjourned.]

[Questions and answers and submissions for the record follow.]

APPENDIX

Additional Material Submitted for the Record

Witness List

Witness List

Hearing before the
Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law

On

"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

Tuesday, May 10, 2011
Dirksen Senate Office Building, Room 226
10:00 a.m.

Panel I

Jessica Rich
Deputy Director
Bureau of Consumer Protection
Federal Trade Commission
Washington, DC

Jason Weinstein
Deputy Assistant Attorney General
Criminal Division
U.S. Department of Justice
Washington, DC

Panel II

Justin Brookman
Director, Project on Consumer Privacy
Center for Democracy and Technology
Washington, DC

Alan Davidson
Director of Public Policy, Americas
Google Inc.
Washington, DC

Ashkan Soltani
Independent Researcher and Consultant
Washington, DC

Guy L. "Bud" Tribble
Vice President of Software Technology
Apple Inc.
Cupertino, CA

Jonathan Zuck
President
Association for Competitive Technology
Washington, DC

PREPARED STATEMENT OF HON. PATRICK J. LEAHY

Statement Of Senator Patrick Leahy (D-Vt.),
Chairman, Senate Judiciary Committee,
On the Subcommittee On Privacy, Technology And The Law
Hearing On "Protecting Mobile Privacy:
Your Smartphones, Tablets, Cell Phones and Your Privacy."

May 10, 2011

Today, the Subcommittee on Privacy, Technology and the Law holds a very important hearing on the privacy implications of Smartphones and other mobile applications. I commend the Subcommittee's Chairman, Senator Franken, for holding this timely hearing -- the first for this new subcommittee -- and I thank him for his dedicated leadership on consumer privacy issues.

Throughout my three decades in the Senate, I have worked to safeguard the privacy rights of all Americans. Ensuring that our Federal privacy laws accomplish this essential goal -- while addressing the needs of law enforcement and America's vital technology industry -- has been one of my highest priorities as the Chairman of the Senate Judiciary Committee. That is why I decided to establish this new privacy subcommittee, and why I am working to update the Electronic Communications Privacy Act (ECPA). I hope to introduce legislation soon to address some of these needed reforms.

In the digital age, American consumers and businesses face threats to privacy like no time before. With the explosion of new technologies, such as social networking sites, smartphones and other mobile applications, there are many new benefits to consumers. But, there are also many new risks to their privacy.

Like many Americans, I am deeply concerned about the recent reports that the Apple iPhone, Google Android Phone and other mobile applications may be collecting, storing, and tracking user location data without the user's consent. I am also concerned about reports that this sensitive location information may be maintained in an unencrypted format, making the information vulnerable to cyber thieves and other criminals. A recent survey commissioned by the privacy firm TRUSTe found that 38 percent of American smartphone users surveyed identified privacy as their number one concern with using mobile applications.

They have good reason to be concerned. The collection, use and storage of location and other sensitive personal information has serious implications regarding the privacy rights and personal safety of American consumers. As this Committee considers important updates to the ECPA and other Federal privacy laws, it is essential that we have full and accurate information about the privacy impact of these new technologies on American consumers and businesses.

This hearing provides a timely opportunity for us to obtain this information and to examine these pressing privacy issues. I am pleased that representatives from the Department of Justice and Federal Trade Commission are here to discuss the administration's views on the privacy implications of mobile applications. I am also pleased that representatives from Google and Apple will address the privacy implications of their smartphones, tablets and other mobile applications.

Safeguarding the privacy rights of American consumers and businesses is one of the most important and challenging issues facing the nation. The many threats to privacy in the digital age impact all Americans and should concern all Members, regardless of party or ideology. I welcome the bipartisan support on the Committee for examining consumer privacy issues and I look forward to a productive discussion.

#####

PREPARED STATEMENTS OF WITNESSES

PREPARED STATEMENT OF

THE FEDERAL TRADE COMMISSION

on

PROTECTING MOBILE PRIVACY: YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY

Before the

UNITED STATES SENATE

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE FOR PRIVACY, TECHNOLOGY AND THE LAW

Washington, D.C.

May 10, 2011

Chairman Franken, Ranking Member Coburn, and members of the Subcommittee, my name is Jessica Rich and I am the Deputy Director of the Bureau of Consumer Protection at the Federal Trade Commission ("FTC" or "Commission").[1] I appreciate this opportunity to appear before you today to discuss the Commission's efforts to protect consumers' privacy in the mobile arena.

This testimony first broadly surveys the growth of the mobile marketplace and the Commission's response to this developing industry. Second, it highlights four of the Commission's recent law enforcement actions in the mobile arena, one involving statements that a public relations agency made in the iTunes mobile application store, another involving unsolicited commercial texts, and two recent privacy enforcement actions involving Google and Twitter, major companies in the mobile arena. Finally, it describes the Commission's efforts to address the privacy challenges of these new, and often very personal technologies, including a discussion of how mobile technology is addressed in the privacy framework recently proposed by FTC staff.

I. The Mobile Marketplace

Mobile technology is exploding with a range of new products and services for consumers. According to the wireless telecommunications trade association, CTIA, the wireless penetration rate reached 96 percent in the United States by the end of last year.[2] Also by that

---

[1] While the views expressed in this statement represent the views of the Commission, my oral presentation and responses to questions are my own and do not necessarily reflect the views of the Commission or any individual Commissioner.

[2] *See* CTIA Wireless Quick Facts, *available at* www.ctia.org/advocacy/research/index.cfm/aid/10323.

same time, 27 percent of U.S. mobile subscribers owned a smartphone,[3] which is a wireless phone with more powerful computing abilities and connectivity than a simple cell phone. Such mobile devices are essentially handheld computers that can not only make telephone calls, but also offer web browsing, e-mail, and a broad range of data services. These new popular mobile devices allow consumers to handle a multitude of tasks in the palm of their hands and offer Internet access virtually anywhere.

Companies are increasingly using this new mobile medium to provide enhanced benefits to consumers, whether to provide online services or content or to market other goods or services.[4] Consumers can search mobile web sites to get detailed information about products, or compare prices on products they are about to purchase while standing in the check-out line. Consumers can join texting programs that provide instantaneous product information and mobile coupons at the point of purchase. Consumers can download mobile software applications ("apps") that can perform a range of consumer services such as locating the nearest retail stores, managing shopping lists, tracking family budgets, or calculating tips or debts. Apps also allow consumers to read news articles, play interactive games and connect with family and friends via social media applications. Any of these services can contain advertising, including targeted

---

[3] ComScore, The 2010 Mobile Year in Review Report (Feb. 14. 2011), *available at* www.comscore.com/Press_Events/Presentations_Whitepapers/2011/2010_Mobile_Year_in_Review.

[4] Indeed, a recent industry survey found that 62 percent of marketers used some form of mobile marketing for their brands in 2010 and an additional 26 percent reported their intention to begin doing so in 2011. *See Vast Majority of Marketers Will Utilize Mobile Marketing and Increase Spending on Mobile Platforms in 2011,* ANA Press Release describing the results of a survey conducted by the Association of National Advertisers in partnership with the Mobile Marketing Association, dated January 31, 2011, *available at* www.ana.net/content/show/id/20953.

advertising.

II. FTC's Response to Consumer Protection Issues Involving Mobile Technology

New technology can bring tremendous benefits to consumers, but it also can present new concerns and provide a platform for old frauds to resurface. Mobile technology is no different. Although there are no special laws applicable to mobile marketing that the FTC enforces, the FTCs core consumer protection law – Section 5 of the FTC Act – prohibits unfair or deceptive practices in the mobile arena.[5] This law applies to marketing in all media, whether traditional print, telephone, television, desktop computer, or mobile device.

For more than a decade, the Commission has explored mobile and wireless issues, starting in 2000 when the agency hosted a two-day workshop studying emerging wireless Internet and data technologies and the privacy, security, and consumer protection issues they raise.[6] In addition, in November 2006, the Commission held a three-day technology forum that prominently featured mobile issues.[7] Shortly thereafter, the Commission hosted two Town Hall meetings to explore the use of radio frequency identification (RFID) technology, and its integration into mobile devices as a contactless payment system.[8] And in 2008, the Commission

---

[5] 15 U.S.C. § 45(a).

[6] FTC Workshop, *The Mobile Wireless Web, Data Services and Beyond: Emerging Technologies and Consumer Issues, available at* www.ftc.gov/bcp/workshops/wireless/index.shtml.

[7] FTC Workshop, *Protecting Consumers in the Next Tech-ade, available at* www.ftc.gov/bcp/workshops/techade. The Staff Report is available at www.ftc.gov/os/2008/03/P064101tech.pdf.

[8] FTC Workshop, *Pay on the Go: Consumers and Contactless Payment, available at* www.ftc.gov/bcp/workshops/payonthego/index.shtml; FTC Workshop, *Transatlantic RFID Workshop on Consumer Privacy and Data Security, available at* www.ftc.gov/bcp/workshops/transatlantic/index.shtml.

held a two-day forum examining consumer protection issues in the mobile sphere, including issues relating to ringtones, games, chat services, mobile coupons, and location-based services.[9]

More recently, the agency has invested in new technologies to provide its investigators and attorneys with the necessary tools to monitor and respond to the growth of the mobile marketplace. For example, the Commission has established a mobile technology laboratory, akin to the Commission's longstanding Internet investigative laboratory, containing a variety of smartphones utilizing different platforms and carriers, as well as software and equipment that permit FTC investigators to collect and preserve evidence and conduct research into a wide range of mobile issues, including those related to consumer privacy.

III. Applying the FTC Act to the Mobile Arena

Law enforcement is the Commission's most visible and effective tool for fighting online threats, including those in the mobile marketplace. As described below, the FTC has brought four recent cases that illustrate how Section 5 applies to the mobile arena, including unsolicited text messages and the privacy and security of data collected on mobile devices.

In August 2010, the Commission charged Reverb Communications, Inc., a public relations agency hired to promote video games, with deceptively endorsing mobile gaming applications in the iTunes store.[10] The company allegedly posted positive reviews of gaming apps using account names that gave the impression the reviews had been submitted by disinterested consumers when they were, in actuality, posted by Reverb employees. In addition, the Commission charged that Reverb failed to disclose that it often received a percentage of the

---

[9] FTC Workshop, *Beyond Voice: Mapping the Mobile Marketplace, available at* www.ftc.gov/bcp/workshops/mobilemarket/index.shtml.

[10] *Reverb Commc'ns, Inc.*, FTC Docket No. C-4310 (Nov. 22, 2010) (consent order).

sales of each game. The Commission charged that the disguised reviews were deceptive under Section 5, because knowing the connection between the reviewers and the game developers would have been material to consumers reviewing the iTunes posts in deciding whether or not to purchase the games. In settling the allegations, the company agreed to an order prohibiting it from publishing reviews of any products or services unless it discloses a material connection, when one exists, between the company and the product. The *Reverb* settlement demonstrates that the FTC's well-settled truth-in-advertising principles apply to new forms of mobile marketing.

In February, the Commission filed its first law enforcement action against a sender of unsolicited text messages and obtained a temporary restraining order suspending the defendant's challenged operations. The FTC alleged that Philip Flora used 32 pre-paid cell phones to send over 5 million unsolicited text messages – almost a million a week – to the mobile phones of U.S. consumers.[11] Many consumers who received Flora's text messages – which typically advertised questionable mortgage loan modification or debt relief services – had to pay a per-message fee each time they received a message. Many others found that Flora's text messages caused them to exceed the number of messages included in their mobile service plans, thereby causing some consumers to incur additional charges on their monthly bill.[12] The Commission charged Flora with the unfair practice of sending unsolicited text messages and with deceptively claiming an affiliation with the federal government in connection with the loan modification

---

[11] *FTC v. Flora*, CV11-00299 (C.D. Cal.) (Compl, filed Feb. 22, 2011).

[12] While the financial injury suffered by any consumer may have been small, the aggregate injury was likely quite large. And, even for those consumers with unlimited messaging plans, Flora's unsolicited messages were harassing and annoying, coming at all hours of the day.

service advertised in the text messages.[13]

The FTC has also taken action against companies that fail to protect the privacy and security of consumer information. Two recent cases highlight the FTC's efforts to challenge deceptive claims that undermine consumers' privacy choices in the mobile marketplace.

First, the Commission's recent case against Google alleges that the company deceived consumers by using information collected from Gmail users to generate and populate a new social network, Google Buzz.[14] The Commission charged that Gmail users' associations with their frequent email contacts became public without the users' consent. As part of the Commission's proposed settlement order, Google must protect the privacy of all of its customers – including mobile users. For example, if Google changes a product or service in a way that makes consumer information more widely available, it must seek affirmative express consent to such a change. This provision applies to *any* data collected from or about consumers, including mobile data. In addition, the order requires Google to implement a comprehensive privacy program and conduct independent audits every other year for the next 20 years.

Second, in the Commission's case against social networking service Twitter, the FTC charged that serious lapses in the company's data security allowed hackers to obtain

---

[13] The complaint against Flora also alleges violations of the CAN-SPAM Act for sending unsolicited commercial email messages advertising his texting services that did not include a valid opt-out mechanism and failed to include a physical postal address. In these emails, Flora offered to send 100,000 text messages for only $300. *See* FTC Press Release, *FTC Asks Court to Shut Down Text Messaging Spammer* (Feb. 23, 2011), *available at* www.ftc.gov/opa/2011/02/loan.shtm.

[14] *Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (consent order accepted for public comment).

unauthorized administrative control of Twitter.[15] As a result, hackers had access to private "tweets" and non-public user information – including users' mobile phone numbers – and took over user accounts, among them, those of then-President-elect Obama and Rupert Murdoch. The Commission's order, which applies to Twitter's collection and use of consumer data, including through mobile devices or applications, prohibits misrepresentations about the extent to which Twitter protects the privacy of communications, requires Twitter to maintain reasonable security, and mandates independent, comprehensive audits of Twitter's security practices.

These are just two recent examples of cases involving mobile privacy issues, but the Commission's enforcement efforts are ongoing.[16] Staff has a number of active investigations into privacy issues associated with mobile devices, including children's privacy.

IV. Mobile Privacy Policy Initiatives

As noted, the rapid growth of mobile technologies has led to the development of many new business models involving mobile services. On the one hand, these innovations provide valuable benefits to both businesses and consumers. On the other hand, they facilitate unprecedented levels of data collection, which are often invisible to consumers.

The Commission recognizes that mobile technology presents unique and heightened privacy and security concerns. In the complicated mobile ecosystem, a single mobile device can facilitate data collection and sharing among many entities, including wireless providers, mobile operating system providers, handset manufacturers, application developers, analytics companies,

---

[15] *Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order).

[16] *See also FTC v. Accusearch, Inc.,* 2007 WL 4356786 (D. Wyo. Sept. 28, 2007) (operation of a website that illegally obtained telephone records, including cell phone records, through pretexting was an unfair act) *,aff'd,* 570 F.3d 1187 (10th Cir. 2009).

and advertisers. And, unlike other types of technology, mobile devices are typically personal to the user, almost always carried by the user and switched-on.[17] From capturing consumers' precise location to their interactions with email, social networks, and apps, companies can use a mobile device to collect data over time and "reveal[] the habits and patterns that mark the distinction between a day in the life and a way of life."[18] Further, the rush of on-the-go use, coupled with the small screens of most mobile devices, makes it even more unlikely that consumers will read detailed privacy disclosures.

In recent months, news reports have highlighted the virtually ubiquitous data collection by smartphones and their apps. Researchers announced that Apple has been collecting geolocation data through its mobile devices over time, and storing unencrypted data files containing this information on consumers' computers and mobile devices.[19] The *Wall Street Journal* has documented numerous companies gaining access to detailed information – such as age, gender, precise location, and the unique identifiers associated with a particular mobile

---

[17] *See, e.g.*, Pew Internet & American Life Project, *Adults, Cell Phones and Texting* at 10 (Sept. 2, 2010), *available at* www.pewinternet.org/Reports/2010/Cell-Phones-and-American-Adults/Overview.aspx ("65% of adults with cell phones say they have ever slept with their cell phone on or right next to their bed"); *Teens and Mobile Phones* at 73 (Apr. 20, 2010), *available at* www.pewinternet.org/Reports/2010/Teens-and-Mobile-Phones/Chapter-3/Sleeping-with-the-phone-on-or-near-the-bed.aspx (86% of cell-owning teens ages 14 and older have slept with their phones next to them).

[18] *United States v. Maynard*, 615 F.3d 544, 562 (D.C. Cir. 2010).

[19] *See* Jennifer Valentino-Devries, *Study: iPhone Keeps Tracking Data*, WALL ST. J. (Apr. 21, 2011), *available at* http://online.wsj.com/article/SB10001424052748704570704576275323811369758.html.

device – that can then be used to track and predict consumers' every move.[20] Not surprisingly, recent surveys indicate that consumers are concerned. For example, a recent Nielsen study found that a majority of smartphone app users worry about their privacy when it comes to sharing their location through a mobile device.[21]

A. Privacy Roundtables

The Commission has been considering these and related issues in connection with its "Exploring Privacy" Roundtable series. In late 2009 and early 2010, the Commission held three roundtables to examine how changes in the marketplace have affected consumer privacy and whether current privacy laws and frameworks have kept pace with these changes.[22] During the second roundtable, one panel in particular focused on the privacy implications of mobile technology, addressing the complexity of data collection through mobile devices; the extent and nature of the data collection, particularly with respect to geolocation data; and the adequacy of

---

[20] *See, e.g.*, Robert Lee Hotz, *The Really Smart Phone*, WALL ST. J. (Apr. 23, 2011), *available at* http://online.wsj.com/article/SB10001424052748704547604576263261679848814.html?mod= (describing how researchers are using mobile data to predict consumers' actions); Scott Thurm & Yukari Iwatane Kane, *Your Apps are Watching You*, WALL ST. J. (Dec. 18, 2010), *available at* http://online.wsj.com/article/SB10001424052748704368004576027751867039730.html?mod= (documenting the data collection that occurs through many popular smartphone apps).

[21] NielsenWire, *Privacy Please! U.S. Smartphone App Users Concerned with Privacy When It Comes to Location* (Apr. 21, 2011), *available at* http://blog.nielsen.com/nielsenwire/online_mobile/privacy-please-u-s-smartphone-app-users-concerned-with-privacy-when-it-comes-to-location/; *see also* Ponemon Institute, *Smartphone Security: Survey of U.S. Consumers* at 7 (Mar. 2011), *available at* http://aa-download.avg.com/filedir/other/Smartphone.pdf (64% of consumers worry about being tracked when using their smartphones).

[22] *See* FTC, *Exploring Privacy: A Roundtable Series*, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml.

privacy disclosures on mobile devices.[23]

B. Preliminary Staff Privacy Report

Based on the information received through the roundtable process, staff drafted a preliminary report ("Staff Report") proposing a new privacy framework consisting of three main recommendations, each of which is applicable to mobile technology.[24] First, staff recommends that companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices, such as not collecting or retaining more data than they need to provide a requested service or transaction. Thus, for example, if an app is providing traffic and weather information to a consumer, it does not need to collect call logs or contact lists from the consumer's device. Further, although the app may need location information, the app developer should carefully consider how long the location information should be retained to provide the requested service.

Second, staff recommends that companies should provide simpler and more streamlined privacy choices to consumers. This means that all companies involved in data collection and sharing through mobile devices – carriers, handset manufacturers, operating system providers, app developers, and advertisers – should work together to provide these choices and to ensure that they are understandable and accessible on the small screen. As stated in the Staff Report,

---

[23] Transcript of Roundtable Record, *Exploring Privacy: A Roundtable Series* at 238 (Jan. 28, 2010) (Panel 4, "Privacy Implication of Mobile Computing), *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtable_Jan2010_Transcript.pdf.

[24] *See* FTC Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* http://ftc.gov/os/2010/12/101201privacyreport.pdf. Commissioners Kovacic and Rosch issued concurring statements available at http://ftc.gov/os/2010/12/101201 privacyreport.pdf at Appendix D and Appendix E, respectively.

companies should also obtain affirmative express consent before collecting or sharing sensitive information such as precise geolocation data.

Third, the Staff Report proposed a number of measures that companies should take to make their data practices more transparent to consumers, including improving disclosures to consumers about information practices. Again, because of the small size of the device, a key question staff posed in the report is how companies can create effective notices and present them on mobile devices.

After releasing the Staff Report, staff received 452 public comments on its proposed framework, a number of which implicate mobile privacy issues specifically.[25] FTC staff is analyzing the comments and will take them in consideration in preparing a final report for release later this year.[26]

V. CONCLUSION

The Commission is committed to protecting consumers' privacy in the mobile sphere by bringing enforcement where appropriate and by working with industry and consumer groups

---

[25] *See* Comment of CTIA (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00375-58002.pdf; Comment of Verizon and Verizon Wireless (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00428-58044.pdf; *see also, e.g.*, Comment of Center for Digital Democracy and U.S. PIRG at 10-11, 20-21, 33 (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00338-57839.pdf; Comment of Stanford Security Laboratory at 11-12 (Feb. 18, 2011), *available at* http://www.ftc.gov/os/comments/privacyreportframework/00467-57980.pdf.

[26] Another major initiative addressing the mobile marketplace is the Commission's review of the Children's Online Privacy Protection Rule, issued pursuant to the Children's Online Privacy Protection Act ("COPPA"). Initiated in April 2010, this review sought public comment on whether technological changes to the online environment warrant any changes to the Rule or to the statute. In June 2010, the Commission also held a public roundtable to discuss the implications for COPPA enforcement raised by new technologies, including the rapid expansion of mobile communications. The Rule review is ongoing.

to develop workable solutions that protect consumers while allowing innovation in this growing marketplace.

Department of Justice

STATEMENT OF

JASON WEINSTEIN
DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE
SUBCOMMITTEE ON PRIVACY, TECHNOLOGY AND THE LAW

ENTITLED

"PROTECTING MOBILE PRIVACY:
YOUR SMARTPHONES, TABLETS, CELL PHONES AND YOUR PRIVACY"

PRESENTED

May 10, 2011

Good afternoon, Chairman Franken, Ranking Member Coburn, and Members of the Committee. Thank you for this opportunity to testify on behalf of the Department of Justice regarding privacy and mobile devices.

Over the last decade, we have witnessed an explosion of mobile computing technology. From laptops and cell phones to tablets and smart phones, Americans are using more mobile computing devices, more extensively, than ever before. We can bank, shop, conduct business, and socialize remotely with our friends and loved ones instantly, almost anywhere. These devices drive new waves of innovation, personal convenience, and professional resources. They also present increasingly tempting targets for identity thieves, cyberstalkers and other criminals.

Last month, one study concluded that 64% of American cell phone users were using smart phones.[1] The speed and scale of that growth makes the topic of this hearing particularly timely. As mobile devices penetrate our daily lives, it is appropriate to evaluate the effect that these new devices have on our safety and privacy. We must also ensure that the law provides sufficient resources to investigators and prosecutors who investigate and prevent crimes against Americans who increasingly conduct their lives using this new medium. I thank the committee for giving me the opportunity to address these issues.

Prosecuting cybercriminals and identity thieves

One of the Department of Justice's core missions is protecting the privacy of Americans and prosecuting criminals who violate that privacy. Americans today face a wide range of threats to their privacy, including risks from using mobile devices. Foreign and domestic actors of all types, including cyber criminals, routinely and unlawfully access data that most people would regard as highly personal and private. Unlike the government – which must comply with the Constitution and laws of the United States and is accountable to Congress, courts, and ultimately the people – malicious cyber actors do not respect our laws or our privacy. The government has an obligation to prevent, disrupt, and deter such intrusions.

---

1 *March Mobile Mix Report*, Millennial Media, available at http://www.millennialmedia.com/research/mobilemix/.

Every day, criminals hunt for our personal and financial data so that they can use it to commit fraud or sell it to other criminals. The technology revolution has facilitated these activities, making available a wide array of new methods that identity thieves can use to access and exploit the personal information of others. Skilled hackers have perpetrated large-scale data breaches that left hundreds of thousands—and in many cases, tens of millions—of individuals at risk of identity theft. Today's criminals can remotely access the computer systems of government agencies, universities, merchants, financial institutions, credit card companies, and data processors to steal large volumes of personal information—including personal financial information. As Americans accomplish more and more of their day-to-day tasks using smart phones and other mobile devices, criminals will increasingly target these platforms.

The most significant threats are continuing to evolve, and now increasingly include threats to corporate data. A report just released by McAfee and Science Applications International Corporation confirms this trend in cyber crime. According to this report, which was based on a survey of more than 1,000 senior IT decision makers in several countries, "high-end" cyber criminals have shifted from targeting credit cards and other personal data to the intellectual capital of large corporations. This includes extremely valuable trade secrets and product planning documents. These threats come both from outside hackers as well as insiders who gain access to critical information from within companies and government agencies. As entities make their key proprietary information available via mobile platforms, so that users can access it wherever and whenever it is most relevant, criminals and other actors will attack those devices as well.

The kinds of criminals we are up against are organized, international, and profit-driven. For example, in October 2009, nearly 100 people were charged in the U.S. and Egypt as part of an operation known as Phish Phry—one of the largest cyber fraud cases to date and the first joint cyber investigation between Egypt and the United States. Phish Phry was the latest action in what FBI Director Mueller described as a "cyber arms race" where law enforcement must coordinate and collaborate in order to keep up with its cyber adversaries. The defendants in

Operation Phish Phry targeted U.S. banks and victimized hundreds of account holders by stealing their financial information and using it to transfer about $1.5 million to bogus accounts they controlled. More than 50 individuals in California, Nevada, and North Carolina and nearly 50 Egyptian citizens have been charged with crimes including computer fraud, conspiracy to commit bank fraud, money laundering, and aggravated identity theft. Led by the FBI and the United States Attorney's Office for the Central District of California, this investigation required close coordination with state and local law enforcement, the Secret Service, and our Egyptian counterparts. In late March, five more people were convicted of federal charges for their roles in this phishing operation, bringing the total number of convictions to date to 46.

One increasingly common form of online crime involves the surreptitious infection of a computer with code that makes it part of a "botnet" – a collection of compromised computers under the remote command and control of a criminal or foreign adversary. Criminals and other malicious actors can extensively monitor these computers, capturing every keystroke, mouse click, password, credit card number, and e-mail. Unfortunately, because many Americans are using such infected computers, they are suffering from an extensive, pervasive invasion of privacy at the hands of these actors.

Just last month, the Department announced the successful disruption of the Coreflood botnet, an international botnet made up of hundreds of thousands of computers that had been infected by malicious software (often referred to as "malware"). The Coreflood malware allowed criminals to remotely control the infected computers in order to steal private personal and financial information from unsuspecting computer users, including users on corporate computer networks. Through a combination of civil and criminal authorities, including a temporary restraining order, the FBI seized the servers that the criminals used to control the botnet and set up a substitute "command and control" server. The Coreflood malware was programmed to automatically contact the Coreflood command and control servers for instructions on a routine basis; after FBI intervention, those requests were instead routed to the FBI's substitute server. The FBI then replied to bot queries with an "exit" command that put the bots to sleep and stopped them from collecting further private data and causing more harm to hundreds of

thousands of unsuspecting users of infected computers in the United States. As I'll discuss later in my testimony, the Department is concerned that as mobile devices become increasingly capable, they will be integrated into such botnets, or used to control them.

The Department's Organizational Response

The Department has organized itself to aggressively investigate and prosecute cyber crime wherever it occurs, including in the context of mobile devices and smart phones. Investigating and disrupting cyber crimes and cyber threats is a priority for the United States Attorney community, and the Attorney General's Advisory Committee has a subcommittee dedicated to cybercrime and intellectual property enforcement issues. A nationwide network of 230 Computer Hacking and Intellectual Property (CHIP) Assistant United States Attorneys in our USAOs focuses on these crimes, in coordination with the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS). CCIPS provides core expertise on these issues, prosecutes cutting edge cases and provides litigation assistance to United States Attorneys' Offices. CCIPS also provides resources such as manuals, and trains prosecutors across the country, often in conjunction with Assistant United States Attorneys. Department prosecutors also work closely with our law enforcement partners.

In FY 2008 through FY 2010, United States Attorneys' Offices brought approximately 4,000 identity fraud cases. In addition, many of the large scale fraud cases prosecuted by the Fraud Section of the Department's Criminal Division also included identity fraud conduct.

The Office of International Affairs (OIA) enhances international cooperation efforts by expediting the sharing of critical electronic evidence with foreign law enforcement partners and by marshaling efforts to secure the extradition of international fugitives. The Office of Enforcement Operations guides investigative policy in numerous areas, including approvals for wiretaps and policy relating to use of tracking devices. It is a combination of these resources both in Main Justice and in the United States Attorneys' Offices that enables prosecutors across the country to tackle these complex and demanding cases.

The FBI Cyber Division is addressing the cybercrime threat from mobile devices through the Financial Threat Focus Cell (FTFC) and the Telecommunications Initiative. Through the FTFC the FBI Cyber Division is working with the largest U.S. based Financial Institutions (FIs) to determine the types, dates and level of mobile banking that those FIs are implementing. The FTFC is also working with FI organizations such as the FS-ISAC, BITS Financial Services Roundtable - Remote Channel Fraud Subgroup and the National Cyber-Forensics & Training Alliance's (NCFTA) Telecommunications Initiative. These organizations provide insight to the FBI so that law enforcement is more cognizant of current and future trends in terms of mobile banking product releases, new business alliances (e.g. AT&T, Verizon and Discover Card's recent product) and new mobile banking vendor companies.

In addition to the FI aspect to the mobile banking threat, the FTFC is working with the telecommunications sector through the Telecommunications Initiative (TI). As a part of the TI, the FBI is working with telecommunication organizations such as the Communication Fraud Control Association (CFCA) and the CTIA – The Wireless Association to address mobile banking and other telecommunications fraud matters. Through the relationship between both the FIs and the TIs the FBI has been able to develop fraud matters such as remote call forwarding, phishing fraud matters and telephonic denial of service (TDOS) attacks against high net worth FI customers. The FBI has ongoing relationships with a number of FI and TI partners to help organize the proactive sharing of fraud information to help mitigate or prevent economic loss. Furthermore, the FBI is beginning to share real-time intelligence with its international law enforcement (LE) partners in regards to global mobile threats. Finally, the FBI is proactively working with several anti-virus companies to stay on the forefront of mobile virus attacks and vulnerabilities.

The Department's work, and the work of our law enforcement partners, has helped to deter national and transnational cyber crime. The Verizon 2011 Data Breach Investigations Report, which is a joint study produced by Verizon, the U.S. Secret Service and the Dutch High Tech Crime Unit, found that more cyber crime investigations were conducted in 2010 than in any previous year, and concluded that the successful prosecution of identity thieves and other

cybercriminals was having a significant impact. The report's leading hypothesis, in fact, was that "the successful identification, prosecution, and incarceration of the perpetrators of many of the largest breaches in recent history is having a positive effect."

Cyber crime in the mobile context

As mobile devices become more prevalent, identity thieves and other cybercriminals will begin to target the users of these devices. In fact, this may already be happening. In March, it was widely reported by technology researchers and journalists in the Washington Post, the New York Times, and elsewhere, that more than 50 apps for the Android mobile operating system had been modified to invade user privacy. According to the reports, these modified apps, infected by malware dubbed "Droid Dream," secretly installed malicious code on the device in addition to their apparent functions. This secret malware enabled the apps to steal sensitive information from the device, receive instructions from the criminals who had made the initial modifications, and even update their malicious capabilities. This activity is an example of the migration of criminal malware attacks that have targeted personal computers for years to targeting smart phones and mobile devices. As cell phones functionality expands, the line between mobile devices and personal computers becomes thinner. For criminals, this raises the prospect of millions of new sources of valuable personal and financial data, and millions of new devices to infect with malware and transform into "bots."

For acts that are particularly egregious – such as blatant theft of financial information or the malicious installation of malware I just described – criminal liability seems both appropriate and warranted. The Department of Justice has extensive experience with investigating and successfully prosecuting criminals who distribute malware and profit from their operation. It is the policy of the Department not to comment on ongoing criminal investigations, but criminal prosecution may be the most appropriate response to deter acts of this type and severity.

When deciding whether to bring an indictment under the Computer Fraud and Abuse Act (18 U.S.C. § 1030) ("CFAA"), Department prosecutors consider a wide range of factors, including the particular facts of the case, the law of the applicable circuit, the severity of the conduct, and the needs of justice. As mobile devices and services offered to mobile device users continue to expand, it will be important to distinguish between those cases that warrant criminal prosecution and those that may be best resolved through regulatory action. For certain less egregious actions, civil enforcement by the Federal Trade Commission might be more appropriate than criminal prosecution.

In addition to collection, it is also important to consider communications providers' ability to disclose the data that they collect from their customers. In this regard, it is important to note that under current law, communications providers may voluntarily disclose or sell any non-content data – such as information about a user's location – for any reason without restriction to anyone other than state, local, and federal government agencies. The Electronic Communications Privacy Act (ECPA) provides a broad exception for covered providers to disclose appropriately collected customer information to "any person other than a governmental entity." 18 U.S.C. § 2702(c)(6). This exception was included in ECPA at a time when there was great concern over ensuring the flexible development of the then-nascent Internet industry. As the commercial landscape changes, it will be important to ensure that our laws strike the appropriate balance and adequately protect consumers' privacy.

Cyberstalking

One important consequence of the proliferation of mobile devices and services that collect location and other personal information about their users is the risk that stalkers, abusive spouses, and others intent on victimizing the user could use information from their mobile device to determine their whereabouts and activities. Stalking is not a new crime, and it is one that the Department of Justice takes very seriously. The increase in the use of mobile devices, however, raises new challenges that must be confronted.

The Department's Office on Violence Against Women (OVW) funds a number of projects that target the intersection of technology and the crimes of stalking, sexual assault, domestic violence, and dating violence. The Office recognizes that stalkers are increasingly misusing a variety of telephone, surveillance, and computer technologies to harass, terrify, intimidate, and monitor their victims, including former and current intimate partners. Perpetrators are also misusing technology to stalk before, during, and after perpetrating sexual violence. For young victims in particular, new technologies bring the risk of digital abuses such as unwanted and repeated texts, breaking into personal email accounts, and pressure for private pictures. Three OVW-funded projects, in particular, focus on "high-tech" stalking and the dangers that new technologies pose for victims.

First, for over ten years, OVW has funded the Stalking Resource Center, a program of the National Center for Victims of Crime, to provide training and technical assistance to OVW grantees and others on developing an effective response to the crime of stalking. The Stalking Resource Center has trained over 40,000 multi-disciplinary professionals nationwide, with an emphasis on the use of technology to stalk. Among other projects, the Resource Center has co-hosted nine national conferences that specifically focused on the use of technology in intimate partner stalking cases. In addition, with funding from the Department's Office for Victims of Crime, the Stalking Resource Center is currently developing two new training tools designed to help law enforcement officers, victim advocates, and allied professionals understand the most common forms of technology used by stalkers.

Second, since 2007, OVW has supported the National Network to End Domestic Violence's Safety Net Project, which works to identify best practices for using technology to assist victims. It is also concerned with training victim service providers to understand how stalkers may misuse technology and what strategies victims can use to increase their safety. In the past three years, the Safety Net Project has trained over 10,000 professionals and provided over 2,200 technical assistance consultations to OVW grantees and others.

Third, OVW funds the Family Violence Prevention Fund's "That's Not Cool" campaign to assist teens in understanding, recognizing and responding to teen dating violence. A critical part of this project is to help teens define their "digital line" as it relates to relationship and dating abuse. The website www.thatsnotcool.com was launched in January 2009 to help teens identify digital dating abuse and to encourage them to define for themselves what is and is not appropriate. So far the campaign has produced strong results, including over 900,000 website visits and 47,400 Facebook fans.

The Department has also strongly responded to the cyberstalking challenge through the prosecution of violations of the federal cyberstalking prohibition, 18 U.S.C. § 2261A. This statute allows for the prosecution of individuals who stalk using "the mail, any interactive computer service, or any facility of interstate or foreign commerce." This encompasses the use of the Internet through computers, smart phones and other mobile devices. Cases have been prosecuted under this statute based on conduct involving MySpace, Facebook and other social networking sites.

In one example of an egregious case charged under this statute, a defendant, posing as the victim, and using the victim's real name and address, posted photographs of the victim's children on a pornographic web site. Many men responded to this invitation.

The federal prohibition, however, is limited by the statutory requirement that the stalker and the victim be in different states, a requirement not found in other threatening statutes. This additional requirement may prevent prosecutors from charging cases, even where the conduct includes the most egregious acts. If an abusive spouse uses his spouse's phone to determine when she visits law enforcement for assistance, or to find where she is when she takes refuge with a friend, this may not violate 18 U.S.C. § 2261A as currently drafted because the two live in the same state. Similarly, a stalker from a victim's home town could potentially use location data from her phone to track her without violating the cyberstalking prohibition for the same reason. In fact, the case described in the previous paragraph was chargeable under 18 U.S.C. § 2261A only because the stalker and the victim, who met on the Internet, lived in different states. The

Department is considering ways to address this limitation and looks forward to working with Congress on this issue. I hope that this Committee and Congress will take the necessary steps to ensure that law enforcement can continue to protect victims of cyberstalking, and deter their tormenters.

Investigative resources for prosecuting computer crimes

Investigating and prosecuting multi-actor, multi-national crimes is extremely resource intensive. It is expensive to train and equip investigators and prosecutors to address the threat of cyber crime. As the proliferation of mobile devices provides criminals with new targets, the task of law enforcement will only get more demanding. Ensuring that law enforcement has the resources it needs to prosecute these crimes is a vital component to ensuring the safety and privacy of Americans.

For more specific details of the Department of Justice's needs for the coming year, I would direct you to the President's 2012 proposed budget, which outlines our detailed requests. In particular, the budget includes a request for funding for the Department to establish six Department of Justice Attaché positions that would emphasize the investigation and prosecution of laws prohibiting international computer hacking and protecting intellectual property rights at embassies around the world. Because computer crime is so often transnational in nature, it is vital that the Department have strong overseas representation to ensure that we can work more quickly and effectively with our international partners when investigating and prosecuting international computer crimes that target American citizens. The program would establish Department representatives at hotspots for computer and intellectual property crime around the world, and would help ensure that we can continue to protect American citizens' privacy, both at home and abroad. I hope that Congress will provide the resources that we need to establish this program and expand our resources to fight international computer crime.

Enhancing Criminal Investigations and Prosecutions

In addition to the resource demands of combating cyber crime, law enforcement must have the authority to collect electronic evidence to investigate privacy invasions and protect public safety. One key statute that addresses this need, while also ensuring a fundamental balance between privacy and public safety, is the Electronic Communications Privacy Act. ECPA empowers law enforcement to collect the evidence it needs to prosecute a wide range of crimes. Department of Justice attorneys regularly use ECPA to obtain crucial evidence from mobile devices for all manner of investigations, including terrorism, drug trafficking, violent crime, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. But it is important to understand that it plays a central role in the investigation of criminal invasions of privacy as well. When considering how best to protect the privacy of American citizens, I would ask that the Committee remember the important role that law enforcement plays in protecting Americans from privacy threats, and how ECPA is critical to our ability to continue to pursue that role.

One particular area of concern for the Department in collecting digital evidence – and one which bears directly on this hearing's topic – is ensuring that law enforcement can successfully track criminals who use their smart phones to aid the commission of crimes. When connecting to the Internet, smart phones, like computers, are assigned Internet Protocol (IP) addresses. When a criminal uses a computer to commit crimes, law enforcement may be able, through lawful legal process, to identify the computer or subscriber account based on its IP address. This information is essential to identifying offenders, locating fugitives, thwarting cyber intrusions, protecting children from sexual exploitation and neutralizing terrorist threats – but only if the data is still in existence by the time law enforcement gets there.

In my recent testimony in January before the House Judiciary Subcommittee on Crime, Terrorism, and Homeland Security, I outlined some of the serious challenges faced by law enforcement in this area in the more traditional computer context. ISPs may choose not to store IP records, may adopt a network architecture that frustrates their ability to track IP assignments and network transactions back to a specific account or device, or may store records for only a

very short period of time. In many cases, these records are the only evidence that allows us to investigate and assign culpability for crimes committed on the Internet. In 2006, forty-nine Attorneys General wrote to Congress to express "grave concern" about "the problem of insufficient data retention policies by Internet Service Providers." They wrote that child exploitation investigations "often tragically dead-end at the door of Internet Serviee Providers (ISPs) that have deleted information critical to determining a suspect's name and physical location."

In one heart-wrenching example of the harm that a lack of data retention can cause, an undercover investigation that discovered a movie depicting the rape of a two-year-old child that was being traded on the internet was stymied because the ISP that had first transmitted the video had not retained information concerning the transmitter. Despite considerable effort, the child was not rescued and the criminals involved were not apprehended.

These challenges are equally serious in the context of smart phones and mobile devices. As the capabilities of smart phones expand, law enforcement increasingly encounters suspects who use their smart phones as they would a computer. For example, criminals use them to communicate with confederates and take other actions that would ordinarily provide pivotal evidence for criminal investigations. Just as some ISPs may not maintain IP address records, many wireless providers do not retain records that would enable law enforcement to identify a suspect's smart phone based on the IP addresses collected by websites that the suspect visited. When this information is not stored, it may be impossible for law enforcement to collect essential evidence.

In addition to collecting electronic evidence, it is vital to the success of the Department's mission that the scope and definition of criminal offenses is broad enough to allow us to prosecute the wide range of cybercrimes that are developing in today's increasingly networked society. This is particularly the case in the mobile context, where rapidly developing technology and services continue to provide opportunities for criminal acts. Some of the most egregious acts of privacy invasion that may be perpetrated on the users of mobile devices certainly rise to the

level of criminal action under the CFAA. These include the installation of malware, theft of financial and personal information, and similarly severe acts, some examples of which I mentioned earlier. The Department takes these crimes very seriously, and, where criminal prosecution is warranted, is committed to vigorously prosecuting offenders. To date, we have not experienced shortcomings in the CFAA vis-à-vis mobile devices. We are continuing to review these authorities but do not have any particular proposals at this time.

* * *

I appreciate the opportunity to share with you information about some of the challenges the Department sees on the horizon as Americans' use of smart phones and tablets continues to grow, and how the Department works to protect the privacy of users of mobile devices. We look forward to continuing to work with Congress as it considers these important issues.

This concludes my remarks. I would be pleased to answer your questions.

KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

Statement of Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Before the Senate Judiciary Committee
Subcommittee on Privacy, Technology, and the Law

Hearing on
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy"

May 10, 2011

Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Chairman's leadership in examining the privacy issues presented by location-enabled mobile devices and appreciate the opportunity to address the lack of legal protection facing of what is one of the fastest growing areas of technological innovation.

CDT is a non-profit, public interest organization dedicated to preserving and promoting openness, innovation, and freedom on the decentralized Internet. I will briefly note the particular privacy issues presented by mobile services, and then describe the inadequacy of existing law to protect consumers. CDT strongly believes that legislation based on the full range of Fair Information Practice Principles (FIPPs) should be enacted to address the privacy challenges faced in the mobile space.

1. The Promise and Peril of Location-Enabled Mobile Devices

Mobile phones and tablets have exploded in popularity in recent years, and all evidence indicates that this trend will continue. Smartphone sales are expected to eclipse those of desktop and laptop computers combined in the next two years.[1] However, mobile devices store and transmit a particularly personal set of data. These devices typically allow third parties to access personal information such as contact lists, pictures, browsing history, and identifying information more readily than in traditional internet web browsing. The devices also use and transmit information consumer's precise geolocation information as consumers travel from place to place.

---

[1] Cecilia Kang, *Smartphone sales to pass computers in 2012: Morgan Stanley analyst Meeker*, THE WASHINGTON POST, November 11, 2010, http://voices.washingtonpost.com/posttech/2010/11/smartphone_sales_to_pass_compu.html.

At the same time, consumers have less control over their information on mobile devices than through traditional web browsing. While third parties, like ad networks, usually must use "cookies" to track users on the web, they often get access to unique — and unchangeable — unique device identifiers in the mobile space. While cookies can be deleted by savvy users, device identifiers are permanent, meaning data shared about your device can always be correlated with that device. As is the case with most consumer data, information generated by mobile devices is for the most part not protected by current law and may be collected and shared without users' knowledge or consent.

Consumers interact with their mobile devices by running applications, or "apps" (i.e., programs designed to run on mobile devices). The mobile apps ecosystem is robust and offers an ever-increasing range of functionality from games, music, maps, instant messaging, email, metro schedules, and more. Mobile apps may be preinstalled on the device by the manufacturer or distributor, or users can download and install the programs themselves from their operating system's "apps store" (like iTunes or the Android Market), or a third-party store (like Amazon). App developers range from large, multinational corporations to individuals coding in their parents' basements. Generally speaking, we have seen a vibrant and creative app market develop for mobile devices. Unfortunately, it can be hard to know what information these apps have access to and with whom they are sharing it.

Recent studies of this flourishing apps data ecosystem have unearthed troubling findings. A recent survey indicated that of the top 340 free apps, only 19% contained a privacy policy *at all*.[2] Last December, the Wall Street Journal investigated the behavior of the 101 most popular mobile apps, finding that more than half transmitted the user's unique device ID to third parties without the user's consent. [3] Forty-seven apps transmitted the phone's location.[4] One popular music app, Pandora, sent users' age, gender, location and phone identifier to various ad networks.[5] In sum, a small phone can leak a big amount of data.

Once an app has access to a user's data, there are usually no rules governing its disclosure, and no controls available to consumers to regain control of it. For the most part, once data leaves the phone, it is effectively "in the wild." It may be retained long after the moment of collection, and often long after the original service has been provided. App developers, advertisers, ad networks and platforms, analytics companies, and any number of other downstream players can share, sell, or unpredictably use data far into the future. Even insurance companies are eying data mined from online services for new predictive models.[6] In short, today's mobile environment provides a gateway into an opaque and largely unregulated market for personal data.

Location data is of particular concern. In recent years, the accuracy of location data has improved while the expense of calculating and obtaining it has declined. As a result, location-

---

[2] Mark Hachman, *Most Mobile Apps Lack Privacy Policies: Study*, PC MAGAZINE, April 27, 2011, http://www.pcmag.com/article2/0,2817,2384363,00.asp.

[3] Scott Thurm and Yukari Iwatani Kane, *Your Apps are Watching You*, THE WALL STREET JOURNAL, December 17, 2010, http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html

[4] *Id.*

[5] *Id.*

[6] Leslie Scism and Mark Maremont, *Insurers Test Data Profiles to Identify Risky Clients*, THE WALL STREET JOURNAL, November 19, 2010, http://online.wsj.com/article/SB10001424052748704648604575620750998072986.html.

based services are an integral part of users' experiences and an increasingly important market for U.S. companies. Consumers like the convenience and relevance of location based services. Location data can be used guide you to the closest coffee shop or help you navigate an unfamiliar neighborhood. Your location can be leveraged to connect you with coupons or deals in your immediate vicinity. And new, innovative, and useful services are introduced daily.

People generally carry their mobile devices wherever they go, making it possible for location data be collected everywhere, at any time, and potentially without prompting. Understandably, many find the use of location data without clear transparency and control troubling. Research shows that people value their location privacy and are less comfortable sharing their location with strangers than with acquaintances, and want granular control over their location information.[7] Indeed, location data is especially sensitive information that can be used to decipher revealing facts or put people at physical risk. Location information could disclose visits to sensitive destinations, like medical clinics, courts and political rallies. Access to location can also be used in stalking and domestic violence.[8] Finally, as an increasing number of minors carry location-capable cell phones and devices, location privacy may become a child safety matter as well.

There are also questions and concerns about the collection, usage, and storage of data by mobile platform providers such as Apple and Google. Because in many instances, these companies are the ones actually calculating your location (based on comparing the WiFi access points in range of your device with known databases), they may receive extremely detailed information about consumer activity, considerably more so than traditional computer operating systems. Although these companies typically assert that data they receive from consumers is anonymized and used merely to build out their databases of access points, these limitations are self-imposed. Furthermore, these platforms may store detailed location and other customer information on the phone itself, which could then be accessed by government officials, potentially without a warrant, malicious hackers, or merely the person who finds your lost phone at Starbucks.[9]

Mobile devices and the services they enable provide consumers with great benefit. But it is imperative that Congress provide a clear policy framework to protect users' privacy and trust. CDT strongly supports privacy legislation that implements the full range of Fair Information Practice Principles (FIPPs) across all consumer data and provides enhanced protections for sensitive information, such as precise geolocation, including enhanced, affirmative opt-in consent.

Unfortunately, today's legal protections fall far short.

---

[7] *See, e.g.*, Janice Y. Tsai, Patrick Kelley, Paul Drielsma, Lorrie Cranor, Jason Hong, Norman Sadeh, *Who's viewed you?: the impact of feedback in a mobile location-sharing application*, Conference on Human Factors in Computing Systems: Proceedings of the 27th international conference on human factors in computing systems (2009), http://www.cs.cmu.edu/~sadeh/Publications/Privacy/CHI2009.pdf; Sunny Consolvo, Ian E. Smith, Tara Matthews, Anthony LaMarca, Jason Tabert, and Pauline Powledge, Location Disclosure to Social Relations: Why, When, & What People Want to Share, CHI '05: Proceedings of the SIGCHI conference on human factors in computing systems (2005), www.placelab.org/publications/pubs/chi05- locDisSocRel-proceedings.pdf.

[8] *See, e.g.*, Rob Stafford, *Tracing a Stalker*, Dateline NBC, June 16, 2007, http://www.msnbc.msn.com/id/19253352/.

[9] *See* Alexis Madrigal, *What Does Your Phone Know About You? More Than You Think*, THE ATLANTIC, April 25, 2011, http://www.theatlantic.com/technology/archive/2011/04/what-does-your-phone-know-about-you-more-than-you-think/237786/.

2. Existing Legal Protections for Mobile Device Information are Outdated, Inapplicable, or Unclear

A number of laws aim to protect electronic communications, including location information. Unfortunately, technology has far outpaced these statutory protections in both the commercial and government contexts. An update is long overdue.

Following is a summary of relevant laws and an analysis of their application to today's location-enabled mobile devices.

A. The Telecommunications Act of 1996 and Cable Communications Policy Act of 1984 (CPNI Rules)

Through the Telecommunications Act of 1996, with subsequent amendments, Congress has prohibited a telecommunications carrier from disclosing customer proprietary network information (CPNI), including "information that relates to the . . . location . . . [of] any customer of a telecommunications carrier . . . that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship" — except in emergency contexts or "as required by law or with the approval of the customer."[10] In short, Congress issued a minimal standard that prohibited carriers from releasing location and other customer information on a solely discretionary basis.

Fifteen years ago, these privacy rules were a groundbreaking development. At the time, telecommunications carriers served as the primary gatekeepers for location information. Data about a cell phone user's location was calculated within a *carrier's* network using signals sent by the phone to the *carrier's* service antennas. These traditional protections have been left behind as we move from voice (traditionally the purview of telecommunications carriers) to data (which is often not the prevue of telecommunications carriers).

In light of modern location technology, there are at least two major shortcomings of the CPNI statute and resulting Federal Communications Commission (FCC) rules:

1. The CPNI rules simply do not apply to new types of location technologies, applications, and services. More specifically, the CPNI rules do not cover methodologies that are independent of telecommunications carriers covered by the law (e.g., WiFi database lookups, cell tower database lookups, or unassisted GPS locations). Thus, when an iPhone or Android user installs a location-based application, the location data transmitted by the resulting service is very likely completely unregulated under the CPNI rules.

2. Even, when a telecommunications carrier is involved in providing a location based service, it may not be covered by the CPNI rules because the FCC has removed wireless broadband service from Title II of the Communications Act (to which the CPNI rules apply) and deregulated it. When the Commission issued its Wireless Broadband Order,[11] Commissioner Copps explained the fractured effect of the Order on the protection of location information under the CPNI rules.[12]

---

[10] 47 U.S.C. § 222.

[11] *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks,*

Thus, modern mobile devices leverage location services that are largely invisible to the telecommunications provider and thus very likely outside the scope of the law. Although Congress and then the FCC did extend CPNI rules to cover IP-enabled "interconnected" VoIP services,[13] that protection still only extends to voice service regulated under Title II. At best, the application of CPNI rules to carrier-provided location-based data services is a murky question; at worst, the CPNI rules provide no protection whatsoever.

Practically speaking, this creates some striking confusion. A consumer using a mobile phone today can be protected by the CPNI rules one moment and unprotected the next. For example, a user might place a phone call using the traditional Commercial Mobile Radio Service (CMRS). In this case, they could feel secure that the CPNI rules required their carrier to protection their information. After the call, they use an Internet-based app or location service that uses location data rendered apart from the telecommunications carrier. Here, the user is likely unprotected.

B. The Electronic Communications Privacy Act (ECPA)

The Electronic Communications Privacy Act was passed in 1986 primarily to address the issue of government access (about which, see below). However, it also contains important limitations on how companies may voluntarily share with other companies customer communications. Most notably, the law prohibits certain companies from sharing the content of customer communications or records without their consent.[14] In theory, this might prohibit mobile operating systems or applications from sharing consumer data without permission. Unfortunately, ECPA, while a very important and forward-looking statute at the time it was passed, was not written with the mobile apps ecosystem in mind. As applied to the current mobile environment, ECPA as a limitation on inter-business sharing of consumer data is, at best, vague and uneven.

When discussing the kinds of mobile applications and services at issue here today, it is not even clear which parties are currently covered by ECPA. ECPA's coverage of stored communications extends only to two categories of services — electronic communications services (ECSs) and remote computing services (RCSs). An ECS is a service that permits users to send or receive communications information (defined in part as "signs, signals, writing, images, sounds, data, or intelligence of any nature")[15] to a third party or parties, like an email service or a private bulletin board such as a restricted Facebook wall. Some apps and location-based services are ECSs, some are not, and some fall into a grey area. For example, a service that allows users to share their location with a specific group of friends or associates is likely an ECS, with the "data or intelligence" communicated to friends being the combination of the user's identity and her location data. However, an app that allows a user to share his location with a restaurant chain solely to allow it to return the location of the nearest restaurant is likely not an ECS, because it does not provide a way to communicate with third parties The statute ultimately requires highly fact-dependent analysis on the ECS question.

Declaratory Ruling, WT Docket No. 07-53, FCC 07-30, 2 (rel. Mar. 23, 2007).

[12] *Id* at ¶ 2 (carriers offering Title I services "appear[] to be entirely free, under our present rules, to sell off aspects of the customer[s'] call or location information to the highest bidder.").

[13] *See* 47 C.F.R. § 64.2001, *et seq.*

[14] 18 U.S.C. §§ 2702(a).

[15] 18 U.S.C. §§ 2510(12).

Remote computing services are, if anything, even more murky. An RCS includes any service that provides to the public computer storage or processing. The limited case law developed around this definition has not clarified its boundaries. Courts have held that websites enabling certain commercial transactions are not RCSs, but have suggested that remote processing of user-collected or -generated data is likely to be covered. Almost any app that collects user location or personal data and sends it to a remote server for further processing could, theoretically, fall under the ambit of this provision. However, it is important to note that mobile operating systems — the entities that often generate consumer location information in the first place — likely do not qualify as either ECSs or RCSs, and thus ECPA offers no protections at all as to those companies.

Of course, even if an app were to fall under the ECPA's ambit, there would still be open questions about whether customer data constituted the "content" of a communication subject to protection. If a consumer affirmatively sent a location request to an app maker to ask for a nearby bar or restaurant, ECPA could arguably restrict the transfer of that information to third parties because the consumer's location was the content of a customer-initiated communication. If on the other hand, the app accessed the user's location in the background merely in order to send to a third party to serve relevant advertising, such request probably would not be governed. Such a reading of the statute would however lead to the perverse result that a consumer's information is afforded greater protections when she affirmatively shares sensitive data, as opposed to when her data is shared without her knowledge or consent.

Though the issue is not the focus of the present hearing, it is important to note that legislation to clarify the standards for government access to that information should also remain a Congressional priority. While the Communications Assistance for Law Enforcement Act (CALEA) indicates what the standard for law enforcement access to location information *is not,* no statute indicates what the standard for law enforcement access *is.* CALEA provides that a pen register or trap and trace order[15] cannot be used to obtain location information, but that statute is silent on what the standard should be.[17] There is a federal statute on tracking devices, but it does not specify the standard that law enforcement must meet in order to place such a device.[18] Most importantly, the Electronic Communications Privacy Act (ECPA),[19] which sets up the sliding scale of authority for governmental access to information relating to communications (ranging from mere subpoena to warrant), does not specify what standard applies to location information.

This has resulted in a mish-mash of confused decisions while courts struggle to find and apply a legal standard. It has led to sometimes arbitrary distinctions based on whether location information is sought in real time or from storage, the degree of precision in the location information sought, the period(s) during which location information is sought, and the technology

[16] A pen register/trap and trace order permits law enforcement to obtain transactional, non-content information about wire and electronic communications in real time, including numbers dialed on a cellular telephone and telephone numbers of calls coming into a cell phone. *See* 18 U.S.C. §§ 3121-3127.

[17] 47 U.S.C. § 1002(a)(2).

[18] 18 U.S.C. § 3117.

[19] 18 U.S.C. §§ 2510 *et seq.*

used to generate the location information. Some courts[20] have adopted a "hybrid theory" advanced by the Department of Justice, holding that location information is accessible to government *in real time* if it meets the standard for *stored* transactional information in Section 2703(d) of the Stored Communications Act.[21] Other courts have required a higher level of proof – probable cause – for law enforcement access to this prospective location information.[22] As one federal magistrate judge recently testified in front of the House Judiciary Committee, there is no comprehensible standard for magistrate judges to apply when the government requests access to cell site location data – just an incoherent array of competing court decisions.[23]

As the first few circuit court decisions to address governmental requests for location information of all types have started to come down, it is becoming clear that the courts have constitutional concerns with these requests. In August, the D.C. Circuit held that putting a device in place to engage in extended GPS tracking without a warrant violates the Fourth Amendment.[24] In September, the Third Circuit held that magistrate judges faced with a request from the government for cell site location information have discretion under ECPA to insist upon a showing of probable cause, in part because of the potential sensitivity of the information.[25] Both the confusion in the lower courts and the consternation in the appeals courts demonstrate that Congressional attention to these statutes is sorely needed.

Congress enacted ECPA in 1986 to foster new communications technologies by giving users confidence that their privacy would be respected. ECPA helped further the growth of the Internet and proved monumentally important to the U.S. economy. Now, technology is again leaping ahead, but the law is not keeping up. CDT — through its Digital Due Process coalition — has convened technology and communications companies, privacy advocates and academics to create four principles for reforming ECPA for the next quarter-century. One of those principles is that location information should only be accessed through the use of a warrant[26] and we believe Congress should enact legislation that imposes a warrant requirement. Though the larger ECPA reform effort is and should remain independent of the issues being discussed here today, CDT believes setting easily-understood privacy-protective standards for government access to location data is a critical component of ensuring the privacy of American citizens and the success of American technology service providers.

---

[20] *See, e.g., In re Application of U.S. for an Order for Disclosure of Telecommunications Records and Authorizing the Use of a Pen Register and Trap and Trace*, 405 F. Supp. 2d 435 (S.D.N.Y. 2005).

[21] The SCA, part of the Electronic Communications Privacy Act, is codified at 18 U.S.C. §§ 2701 *et seq.*

[22] *See, e.g., In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority,* 396 F. Supp. 2d 747 (S.D.Tex. 2005).

[23] *See Electronic Communications Privacy Act Reform and the Revolution in Location Based Technologies and Services Before the H. Comm. on Judiciary Subcomm. on the Constitution, Civil Rights, and Civil Liberties,* 111th Cong. (June 24, 2010) (statement of Stephen Wm. Smith, United States Magistrate Judge).

[24] *U.S. v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010).

[25] *In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

[26] For more information on the Digital Due Process coalition and its principles, see Digital Due Process at http://www.digitaldueprocess.org.

C. The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act (CFAA) is a criminal statute that prohibits intentional trespass into and theft from protected computer systems.[27] It criminalizes, in relevant part, one who "intentionally accesses a computer without authorization or exceeds authorized access . . . information from any protected computer."[28] In short, it's a law to prosecute malicious hackers.

The CFAA is a law design to combat egregious computer crimes and cannot, and should not, be a primary tool in protecting consumers' mobile privacy from data sharing for marketing or related purposes. In the past, there have been failed attempts to stretch the CFAA to cover contractual terms of service.[29] CDT has warned that these attempts come with troubling encroachments on civil liberties and freedom of speech.[30] Criminal sanctions for certain computer crimes might well deter bad actors and provide appropriate tools in extreme circumstances. However, it is a blunt instrument not designed to address mobile privacy challenges arising from commercial activity.

The mobile market is nascent and innovating quickly. Many mobile app developers are individuals or small startup companies. They might be amateur programmers, working with various prefabricated pieces of code and advertising solutions. They may or may not have expertise in privacy or relevant law. Criminal sanctions, including jail time, would be heavy-handed and would likely chill the innovation we see today.

D. Federal Trade Commission Act and State Attorneys General

Absent any affirmative legal requirements provided by sectoral specific privacy laws (such as those governing health or financial data), the default privacy rule for most consumer data is set by the FTC Act's prohibition on unfair and deceptive trade practices.[31] Under this authority, the FTC has established some general precedents about what constitutes a deceptive or unfair privacy practice online, such as recent settlements against companies who offered deceptive and ineffective opt-out solutions, and against Google for sharing personal data with other Google customers in violation of previous representations as part of the Buzz product. While these cases are important, they also demonstrate that the FTC is generally limited under current law to bringing enforcement actions against companies that make affirmative misstatements about their own privacy practices. In the absence of a baseline federal privacy law that gives the FTC the tools it needs and establishes it as the lead law enforcement agency for privacy matters, consumer protections in the location privacy space will continue to fall short.

State Attorneys General also have consumer protection mandates that allow them to pursue service providers that engage in unfair or deceptive trade practices. To date, however, perhaps due to the inherent limitations in their authority, relatively little attention has been paid at the state level to consumer privacy concerns.

---

[27] 18 U.S.C. § 1030.

[28] 18 U.S.C. § 1030(a)(2)(C).

[29] *See generally*, US v. Drew, Electronic Frontier Foundation, *available at* https://www.eff.org/cases/united-states-v-drew (last visited May 6, 2011).

[30] *Id.*

[31] The FTC Act, 15 U.S.C. §§ 41 *et seq.*

3. The Need for Congressional Action

Given that the default rule for most consumer data — including sensitive location data — is merely that companies cannot make affirmative misstatements about the use of that data, CDT strongly supports the enactment of a uniform set of baseline rules for personal information collected both online and offline. Modern data flows often involve the collection and use of data derived and combined from both online and offline sources, and the rights of consumers and obligations of companies with respect to consumer data should apply to both as well. The mobile device space implicates many different kinds of data in a complicated ecosystem. Cramming more notices onto small screens is alone insufficient. We need a data privacy law that incentivizes and requires companies to provide clear and conspicuous notice to consumers about the use of their information and provides for meaningful control of that information. Moreover, companies should collect only as much personal information as necessary, be clear about with whom they're sharing information, and expunge information after it is no longer needed.

The Fair Information Practices (FIPPs) should be the foundation of any comprehensive privacy framework. FIPPs have been embodied to varying degrees in the Privacy Act, Fair Credit Reporting Act, and other sectoral federal privacy laws that govern commercial uses of information online and offline. The most recent formulation of the FIPPs by the Department of Homeland Security offers a robust set of modernized principles that should serve as the foundation for any discussion of consumer privacy legislation.[32] Those principles are:

- Transparency
- Purpose Specification
- Use Limitation
- Data Minimization
- Data Accuracy
- Individual Participation
- Security
- Accountability

For particularly sensitive data, such as health information, financial information, information about religion or sexuality, and — most relevant here — precise geolocation data, a legislative framework should provide for enhanced application of the Fair Information Practice Principles, including for affirmative opt-in consent for the collection and/or transfer of such information. Consumers understandably have greater concerns about the use and storage of such information, and the law should err against presuming a consumer's assent to share such information with others.

Furthermore, as noted above, the laws governing government access to consumer data should be modernized to require a warrant to access sensitive location information.

---

[32] U.S. Department of Homeland Security, Privacy Policy Guidance Memorandum, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security, December 2008, http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

4. Conclusion

CDT would like to thank the Subcommittee again for holding this important hearing. We believe that Congress has a critical role to play in ensuring the privacy of consumers in the growing market of mobile devices and services. CDT looks forward to working with the Members of the Subcommittee as they pursue these issues further.

For more information, contact Justin Brookman, justin@cdt.org, (202) 637-9800.

Testimony of Alan Davidson, Director of Public Policy, Google Inc.

Before the Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

May 10, 2011

Chairman Leahy, Chairman Franken, Ranking Member Coburn, and members of the Committee:

I am pleased to appear before you this morning to discuss mobile services, online privacy, and the ways that Google protects our users' personal information. My name is Alan Davidson, and I am a Google's Director of Public Policy for the Americas. In that capacity, I oversee our public policy operations in the United States, and work closely with our legal, product, and engineering teams to develop and communicate our approach to privacy and security, as well as other issues important to Google and our users.

Google is most well known for our search engine, which is available to Internet users throughout the world. We also make Android, an open operating system for mobile devices that in a few short years has grown from powering one device (introduced in the fall of 2008) to over 170 devices today, created by 27 manufacturers. We also offer dozens of other popular services, from YouTube to Gmail to Google Earth. Our products are generally offered for free for personal use, and one supported by revenue from advertising and sales to businesses.

Protecting privacy and security is essential for Internet commerce. Without the trust of our users, we simply would not be able to offer these services or platforms because on the Internet, competing services are only one click away. If we fail to offer clear, usable privacy controls, transparency in our privacy practices, and strong security, our users will simply switch to another provider. This is as true for our services that are available on mobile devices as it is for those that are available on desktop computers. For this reason, location sharing on Android devices is strictly opt-in for our users, with clear notice and control.

In my testimony today, I'll focus on three main points:

- Location-based services provide tremendous value to consumers;
- Google is committed to the highest standards of privacy protection in location-based services; and
- Congress has an important role in helping companies build trust and create appropriate government access standards.

I. Location based services provide tremendous value to consumers

Mobile services are creating enormous economic benefits for our society. A recent market report predicts that the mobile applications market will be worth $25 billion by 2015. At Google, we have seen an explosion in demand for location-based services.

People can use our services to find driving directions from their current location, identify a traffic jam and find an alternate route, and find the next movie time at a nearby theater. Location can even make search results more relevant: If a user searches for "coffee" from a mobile phone, she is more likely to be looking for a nearby café than for the website of a national coffee chain or the Wikipedia entry describing coffee's history. In the last year, a full 40% of Google Maps usage was from mobile devices. There are now 150 million active monthly Google Maps for Mobile users on Android, iPhone, BlackBerry, and other mobile platforms in more than 100 countries.

Many third party applications also use location services to provide helpful products. For example, the U.S. Postal Service offers an application to help users find nearby post offices and collection boxes, based on their location. And if you want a Five Guys burger, their application will find a location for you, and even lets you order and pay in advance. Twitter allows users to "geotag" their tweets from their application, which can give followers important context and perspective. On smartphones like iPhone, Palm, and Android devices, services such as Yelp and Urbanspoon use location to provide relevant local search results, while applications like Foursquare let users find nearby friends.

Mobile location data can even save lives. In the past, a parent's best hope of finding a missing child might have been a picture on a milk carton, but mobile location services may be changing that. Google works with the National Center for Missing and Exploited Children (NCMEC) in an ongoing partnership to develop technology solutions that help them achieve their mission. Today, modern tools and information can make NCMEC's AMBER alerts more effective and efficient by sending the alert to all users within one mile of an incident within seconds of the report through location-based targeting. Over time, the radius could be expanded, with speed and acceleration of distribution based directly on information received.

Existing emergency notifications like AMBER alerts can be improved using location data. In crisis situations, people are increasingly turning to the Internet on mobile or desktop devices to find information. Within a few hours of the Japan earthquake, for example, we saw a massive spike in search queries originating from Hawaii related to "tsunami." We placed a location-based alert on the Google homepage for tsunami alerts in the Pacific and ran similar promotions across News, Maps, and other services. In cases like the Japanese tsunami or the recent tornadoes in the U.S., a targeted mobile alert from a provider like Google or from a public enhanced 911 service may help increase citizens' chances of getting out of harm's way.

None of these services or public safety tools would be possible without the location information that our users share with us and other providers, and without the mobile platforms for businesses and governments to effectively reach the appropriate audience.

II. Google is committed to the highest standards of privacy protection in location-based services

Google would not be able to offer these services or platforms or help create the economic and social value generated from location data if we lost the trust of our users. Thus, at Google, privacy is something we think about every day across every level of our company. It is both good for our users and critical for our business.

Privacy at Google begins with five core principles, which are located and available to the public at www.google.com/corporate/privacy_principles.html:

- Use information to provide our users with valuable products and services.
- Develop products that reflect strong privacy standards and practices.
- Make the collection and use of personal information transparent.
- Give users meaningful choices to protect their privacy.
- Be a responsible steward of the information we hold.

As with every aspect of our products, we follow the axiom of "focus on the user and all else will follow." We are committed to using information only where we can provide value to our users. That's what we mean by our first principle.

For example, **we never sell our users' personally identifiable information**. This is simply not our business model.

To further guide us, under the second principle, we aim to build privacy and security into our products and practices from the ground up. From the design phase through launch, we consider a product's impact on our users' privacy. And we don't stop at launch; we continue to innovate and iterate as we learn more from users.

Our last three principles give substance to what we mean by privacy: We commit to *transparency*, *user control,* and *security*.

Internal process and controls

We also reflect these principles in our development process and employee training. As consumers become more reliant on services provided by third parties, consumer privacy relies increasingly on those parties' internal practices, process, and controls. As we recently explained, we have begun to implement even stronger privacy controls with a focus on people, training, and compliance.

We have developed a review process where all engineering projects leads are required to submit and maintain a Privacy Design Document detailing how their projects handle user data. These documents are reviewed by cross-functional working groups that can request code reviews and make

recommendations to the product teams. Completion of Privacy Design Documents will also be reviewed by managers and an independent internal audit team. We have also enhanced our core training for engineers and others to create a greater focus on responsible collection, use, and handling of data.

All this process is aimed at ensuring that products match our philosophy and avoid mistakes that fracture user trust — like the launch of Google Buzz — which fall short of our standards for transparency and user control. To help make sure we live up to this promise, we entered into a consent decree with the Federal Trade Commission this year, under which we'll receive an independent review of the privacy procedures we have outlined above once every two years. In addition, we'll ask users to give us affirmative consent before we change how we share their personal information.

How our products reflect our principles — Opt-in controls on Android

Moving to our specific products, I'll focus first on an important area in which we are putting our principles to work, and where we are innovating on the broader privacy issues faced in the online world: Simple, opt-in controls for collection and use of location information on Android.

While location-based services are already showing great value to users, Google recognizes the particular privacy concerns that come with the collection and storage of location information. That's why we don't collect any location information — any at all — through our location services on Android devices unless the user specifically chooses to share this information with Google. We also give users clear notice and control; the set-up process asks users if they would like to "allow Google's location service to collect anonymous location data."

And even after opting in, we give users a way to easily turn off location sharing with Google at any time they wish. The location services in our Android operating system embody the transparency and control principles that we use to guide our privacy process.

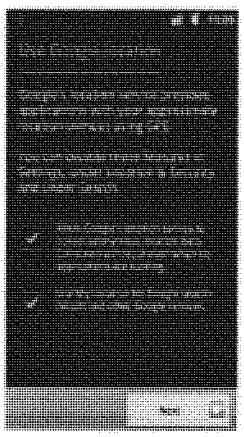
Google is also very careful about how we use and store the data that is generated by location-based services. The location information sent to Google servers when users opt in to location services on Android is anonymized and stored in the aggregate and is not tied or traceable to a specific user. The collected information is stored with a hashed version of an anonymous token, which is deleted after approximately one week. A small amount of location information regarding nearby Wi-Fi access points and cell towers is kept on the Android device to help the user continue to enjoy the service when no server connection is available and to improve speed and battery life. This information on the device is likewise not tied or traceable to a specific user.

Global Positioning System (GPS) enabled devices can provide a highly accurate location using information from GPS satellites. But GPS can be slow and drain battery life and can take 10 seconds (and sometimes much longer) to "fix" a location. Furthermore, many devices are not GPS enabled

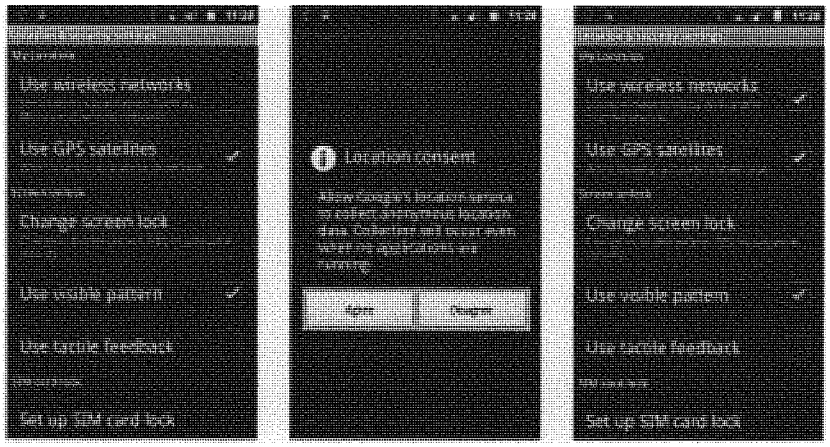
or are used in situations where obtaining a GPS signal might not even be possible (*e.g.*, indoors, where there is no line of sight between the device and the satellites).

In order to serve devices that may not have GPS capabilities, or simply to avoid the delay and battery drain from GPS services, various companies have worked out alternatives to GPS. These are generally based around the idea of detecting nearby, publicly available signals from Wi-Fi access points and cell towers and using this data to quickly approximate a rough position, usually with less accuracy than GPS. By treating Wi-Fi access points or cell towers as beacons, devices are able to fix their general location quickly in a power-efficient way, even while they may be working on a more precise GPS-based location. This can be done by using information that is publicly broadcast (for example, that list of Wi-Fi access points you see when you use the "join network" option on your computer). A database of known network locations is required to determine a user's estimated location from either Wi-Fi access point or cell tower information. Companies like Skyhook Wireless and Navizon compile such databases and license the data to many industry leaders.

Google has also created such location service called the Google Location Server — an Internet database on Google servers that uses Wi-Fi access points and cell towers to determine an estimated location and that uses GPS information to estimate road traffic. Device manufacturers can install the Google Network Location Provider application for Android (pursuant to a license with Google) on their devices. This application can determine a user's estimated location using the Google Location Server, to make location information available to users whether they are indoors and outdoors, more quickly, and using less battery power than GPS services. This Network Location Provider is turned off by default, and can be turned on by the user during the phone's initial setup or in the device settings.



The Network Location Provider is off by default. The user can opt-in and turn on location services during the initial setup flow.



The user can opt-in to turn on the Network Location Provider on their Android phone from within the device settings.

The Android operating system is built on the principle of openness, with the goal of encouraging developer innovation and a vibrant ecosystem for users. With this principle in mind, Google does not decide which applications can access location or other user information from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access during the application installation process. This permissions model is designed to empower users to make their own decision on whether or not to trust an application with the information requested. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation. An application can only access the device's GPS location or the device's network location if it displays a permission to the user at time of installation.

When Google creates an Android application, like the Google Maps for mobile application, Google is responsible for how the application collects and handles data and for the privacy disclosures made to users. Most Google-developed Android applications are subject to the Google Mobile Terms of Service and the Google Mobile Privacy Policy, unless Google has created a custom terms of service and privacy policy for the application. Google privacy policies are also clearly displayed to the user when the user first signs into the Android device.

When an Android application is not developed by Google, the application developer bears the responsibility for the design of the application, which includes responsibility for how the application collects and handles user data and the privacy disclosures made to users. If the user chooses to trust

an application with location information by proceeding with the installation after viewing the location-related permissions, then that application could potentially store this location information on the device or transmit the information off the device if the application also has the Internet access permission. Google does not control the behavior of third party applications or how they handle location information and other user information that the third party application obtains from the device, even though Google strongly encourages application developers to use best practices as described in this Google blog post.

How our products reflect our principles — Encryption and two-step verification

Along with transparency and user control, strong security for users of Google's services to protect against hackers and data breach is vital. Nothing can erode trust faster than personal information falling into the hands of hackers. Google faces complex security challenges while providing services to millions of people every day, and we have world-class engineers working at Google to help secure information.

For example, Google is the first (and only) major webmail provider to offer session-wide secure socket layer (SSL) encryption *by default*. Usually recognized by a web address starting with "https" or by a "lock" icon, SSL encryption is regularly used for online banking or transactions. As our Gmail lead engineer wrote:

> In 2008, we rolled out the option to always use https — encrypting your mail as it travels between your web browser and our servers. Using https helps protect data from being snooped by third parties . . . . We initially left the choice of using it up to you because there's a downside: https can make your mail slower since encrypted data doesn't travel across the web as quickly as unencrypted data. Over the last few months, we've been researching the security/latency tradeoff and decided that turning https on for everyone was the right thing to do.

We hope other companies will soon join our lead.

We also hope to see our competitors adopt another security tool we offer our users: encryption for search queries. Users can simply type "https://encrypted.google.com" into their browsers to navigate to the version of Google Search that encrypts search queries and results. As we said in our blog post about encrypted search, "an encrypted connection is created between your browser and Google. This secured channel helps protect your search terms and your search results pages from being intercepted hy a third party on your network."

And in March of last year Google introduced a system to notify users about suspicious activities associated with their accounts. By automatically matching a user's IP address to broad geographical locations, Google can help detect anomalous behavior, such as a log-in appearing to come from one continent only a few hours after the same account holder logged in from a different continent. Thus, someone whose Gmail account may have been compromised will be notified and given the opportunity to change her password, protecting her own account and her Gmail contacts.

Finally, we recently released 2-step verification for consumer Gmail accounts, which allows users who are concerned about the security of their account to use a password plus a unique code generated by a mobile phone to sign in. It's an extra step, but it's one that significantly improves the security of a Google Account. Now, if someone steals or guesses a Gmail user's password, the potential hijacker still cannot sign in to the user's account because the hijacker does not have the user's phone. We are already hearing stories from our users about how this extra layer of security has protected them from phishing attacks or unauthorized access.

III. Congress should act to build trust and create appropriate government access standards

Congress has a vital role to play in encouraging responsible privacy and security practices, both by bringing attention to these issues and through appropriate legislation.

As a start, Google supports the development of comprehensive, baseline privacy framework that can ensure broad-based user trust and that will support continued innovation and serve the privacy interests of consumers. Some key considerations in this area include:

- **Even-handed application.** A pro-innovation privacy framework must apply even-handedly to all personal data regardless of source or means of collection. Thus, offline and online data collection and processing should, where reasonable, involve similar data protection obligations.

- **Recognition of benefits and costs.** As with any regulatory policy, it is appropriate to examine the benefits and costs of legislating in this area, including explicit attention to actual harm to users and compliance costs.

- **Consistency across jurisdictions**. Generally, Internet users neither expect nor want different baseline privacy rules based on the local jurisdiction in which they or the provider reside. Moreover, in many instances, strict compliance with differing state or national privacy protocols would actually diminish consumer privacy, since it would require Internet companies to know where consumers are located at any given time.

We also suggest two concrete areas where Congress can act immediately to strengthen Americans' privacy protections and provide consistency for providers:

We pride ourselves at Google for industry-leading security features, including the use of encryption for our search and Gmail services. But we need help from the government to help ensure that the bad acts of criminal hackers or inadequate security on the part of other companies does not

undermine consumer trust for all services. Moreover, the patchwork of state law in this area leads to confusion and unnecessary cost. Congress should therefore promote uniform, reasonable security principles, including data breach notification procedures.

Finally, the Electronic Communications Privacy Act, the U.S. law governing government access to stored communications, is outdated and out of step with what is reasonably expected by those who use cloud computing services. ECPA worked well for many years, and much of it remains vibrant and relevant. In significant places, however, a large gap has grown between the technological assumptions made in ECPA and the reality of how the Internet works today, leaving us in some circumstances with complex and baffling rules that are both difficult to explain to users and difficult to apply.

As part of the Digital Due Process coalition, we are working to address this issue. The Digital Due Process coalition includes members ranging from AT&T to Google to Americans for Tax Reform to the ACLU. It has put forward common sense principles that are designed to update ECPA, while ensuring that government has the legal tools needed to enforce the laws. Particularly relevant to today's hearing, the coalition seeks to:

- **Create a consistent process for data stored online.** Treat private communications and documents stored online the same as if they were stored at home and require a uniform process before compelling a service provider to access and disclose the information.

- **Create a consistent process for location information.** Create a clear, strong process with heightened standards for government access to information regarding the location of an individual's mobile device.

Advances in technology rely not just on the smart engineers who create the new services, but also on smart laws that provide the critical legal underpinning for continued innovation and adoption of the technology. We hope to work with this Committee and with Congress as a whole to strengthen these legal protections for individuals and businesses.

* * *

I look forward to answering any questions you might have about our efforts. And Google looks forward to working with members of the Committee and with Congress in the development of valuable online services and strong privacy and security protections for users.

Thank you.

Testimony of Ashkan Soltani[1]
Independent Privacy Researcher and Consultant

United States Senate, Judiciary Subcommittee on Privacy, Technology and the Law
Hearing on
Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy

May 10, 2011

Chairman Franken, Ranking Member Coburn, and the distinguished members of the Subcommittee, thank you for the opportunity to testify about mobile privacy and the state of location tracking.

My name is Ashkan Soltani. I am a technology researcher and consultant specializing in consumer privacy and security. I have more than 15 years of experience as a technical consultant to Internet companies and federal government agencies. I received my masters degree in Information Science from the University of California at Berkeley, where I conducted extensive research and published two major reports on the methods by which users are tracked online and to what extent. Last year, I served as a staff technologist in the Division of Privacy and Identity Protection at the Federal Trade Commission on investigations related to Internet technology and consumer privacy. I have also worked as the primary technical consultant on The Wall Street Journal's *What They Know* series investigating issues relating to privacy online.

Recent revelations about how mobile devices handle sensitive data—particularly location information—have surprised consumers. Their devices often play a large role in their everyday activities, and many consumers show significant concern about who has access to their information.[2] Whether consumers understand these privacy risks and whether they have meaningful control over information access are critical questions for this Subcommittee.

I have been invited to testify about the current state of mobile privacy and location tracking from a technical perspective. First, I will describe location-based services and how a mobile device can determine its location. Second, I will discuss three recent issues that demonstrate how location data and other personal information are collected and shared in the current mobile ecosystem. Finally, I will discuss three broad implications for consumer mobile privacy and provide some suggestions for improvement.

---

[1] My oral and written testimony here today to the Subcommittee represents my own personal views, and does not reflect the views of any of the organizations that I have consulted or worked for in the past.

[2] Tsai, Janice Y., Kelley, Patrick Gage, Cranor, Lorrie Faith, Sadeh, Norman. Location Sharing Technologies: Privacy Risks and Controls. (2009). From http://repository.cmu.edu/isr/85/

A. MOBILE DEVICES AND LOCATION-BASED SERVICES

Mobile devices today are powerful computing machines. Like desktop computers, many mobile devices run complex operating system platforms that allow third-party developers to create software applications to perform specialized tasks. Two of the most widely used mobile platforms, Apple iOS and Google Android, offer consumers hundreds of thousands of innovative applications to download and install onto their devices through the Apple App Store and Android Market. These include e-mail capabilities and productivity tools, mapping and navigation services, social media applications and games. However, unlike desktop computers, mobile devices are uniquely *mobile* which introduces unique privacy implications for their owners.

Consumers take their mobile phones and tablet computers with them nearly everywhere they go.[3] They often carry these devices in their pockets from their homes to their offices, while traveling by car or train, when on their way to daycare and to the grocery store. Mobile phones, in particular, are personal "always-on" devices; therefore, the location of these devices often closely mirrors that of their owners' locations and activities.

The location of a mobile device at any given moment may not be particularly sensitive; However, the historical trail of past locations can reveal much about its user's behavior. In some cases, a person who has access to historical location data can infer trends that uniquely identify an individual. For example, if a mobile device's location is the same each work day, then consistently at another location every evening, it might expose the location of the device owner's workplace and home, respectively. An individual or organization with access to this information could then correlate it with public databases that could then be linked to a particular individual.[4]

However, location-based services (LBS) are a major selling point for many mobile devices. These features quickly enable the discovery of nearby stores and restaurants, sharing of current location with friends and family by using "check-in" functionality within social networking applications, and easy directional navigation to desired destinations. In order to provide this functionality, the application or service provider needs to pinpoint and use the mobile device's location.

---

[3] Three in five mobile phone owners say they carry their phones at all times, even inside the home. See: Stanton, D. (2008, September 8). New Study Shows Mobile Phones Merging New, Established Roles. Knowledge Networks. From http://www.knowledgenetworks.com/news/releases/2008/091808_mobilephones.html

[4] Golle, Philippe and Kurt Partridge. On the Anonymity of Home/Work Location Pairs. From http://xenon.stanford.edu/~pgolle/papers/commute.pdf (Researchers demonstrate it may be possible to associate home/work location pairs to individuals' identity.)

Note: The icons in the margins below refer to the diagram in Appendix A and are used to direct attention to specific portions of the "Location Ecosystem."

There are four primary ways the location of a mobile device can be determined, depending on both its hardware and software capabilities.

1. Global positioning system (GPS) is a technology that allows a device to determine its location by triangulating GPS satellite signals, which are typically accurate to within a few meters. While nearly all smartphones manufactured today contain a built-in GPS chip, many mobile devices (*e.g.*, laptops) typically do not. While GPS allows for high accuracy of location, it is often unavailable indoors and its high consumption of battery life often compels users to turn off GPS until they require it.

2. Wireless carriers can help mobile devices determine location by using information about the signals of nearby cell phone towers. This is called cellular geolocation. Cellular phone towers act as known "landmarks" since they have fixed locations. This property enables wireless carriers to triangulate a device's location anytime the device is powered on. Mobile phones can send a query to the carrier to request the physical coordinates of towers within range and then calculate its position as best as possible. This technique is generally less accurate than GPS and varies widely depending on the density of cell towers in a given area.

LP

3. Location providers are services that allow devices to determine location via a variety of methods, which include cellular, Wi-Fi and Internet Protocol (IP) based methods. Companies such as Google, Apple, and Skyhook can act as location providers by compiling extensive databases that correlate Wi-Fi access points and cell phone towers with their physical locations. Mobile devices then query these databases with information about nearby "wireless landmarks" (*i.e.*, Wi-Fi access points and cell phone towers) in order to obtain their current location. As a result, the location provider is able to infer the current location of the mobile device as well as enhance its own location database with any additional "wireless landmarks" provided with the query.

4. Location aggregators are a separate class of location service providers that obtain location information via direct arrangements with wireless carriers. As such, device location is obtained directly from triangulation of nearby cellular tower data and does not rely on the handset to be "aware" of its present location. This enables features such as 'geofencing,' which is the ability to notify a third party whenever a device enters geographic area without requiring a specialized application on the phone. Location aggregators occupy a unique niche in this marketplace as they have a detailed "carrier view" vantage point across all of their participating partners, and they provide data to third party applications and websites directly.

B. HOW MOBILE DEVICE LOCATION IS COLLECTED AND SHARED

1. By Location Providers

The process by which Location Providers gather data raises significant privacy concerns. Much of the initial public concern focused on Google's reported collection of consumer information when it mapped wireless landmarks like cell towers and Wi-Fi access points by using employee-driven automobiles that were equipped with special sensors.[5]

More recently, location providers began distributing the work by using their customers' mobile devices as "scouts in the field" in order to compile their databases of the physical locations of wireless landmarks. This "crowdsourcing" of location data has introduced additional privacy concerns. By leveraging consumers' mobile devices as scouts, location providers consequently receive the location of the mobile device as they report their findings.[6] Consumers have the option to "opt-out" of this practice; however, background collection and transmission of location information is enabled by default for most location providers.[7]

Even the notice that is offered may also be inadequate for meaningful choice. Figure 1 below compares the Google Android platform's permission screen informing users of the background collection of location data to the comparable screen on the Apple iOS platform. A customer would have to read Apple's lengthy software license agreement to learn that disabling location services means disabling the background collection of location data.

In addition, a mobile device user's attempt to "opt-out" may be ineffective. In April 2011, The Wall Street Journal reported that Apple iPhone devices woud still collect and transmitting this information, even when users' had affirmatively set the location services to "off." That is, even when consumers elected to disable collection of their device location, their iPhones had continued to record and transmit location services information to Apple's servers.[8] Surprisingly, this scenario conflicts with a July 12, 2010 letter from Apple's General Counsel to Representatives Ed Markey and Joe Barton which stated that "Apple automatically collects this

---

[5] Stone, Brad. (2010, May 14). Google Says It Collected Private Data By Mistake. From http://www.nytimes.com/2010/05/15/business/15google.html

[6] Valentino-Devries, Jennifer. (2011, April 23). Google Defends Way It Gets Phone Data. From http://online.wsj.com/article/SB10001424052748703387904576279451001593760.html

[7] Google's default is enabled by means of a pre-selected check box during the initial product setup which a user has to actively 'uncheck'. See Figure 1. The FTC has raised concerns about "pre-checked" dialogues as a mechanism for affirmative consent in a recent settlement with Google and their Buzz social networking product. See http://www.ftc.gov/os/caselist/1023136/110330googlebuzzcmpt.pdf at page 4.

[8] Valentino-Devries, Jennifer. (2011, April 25). IPhone Stored Location in Test Even if Disabled. From http://online.wsj.com/article/SB10001424052748704123204576283580249161342.html and Apple. (2011, April 27). Apple Q&A On Location Data. From http://www.apple.com/pr/library/2011/04/27location_qa.html.

information only (1) if the device's location-based services capabilities are toggled to 'On' and (2) the customer uses an application requiring location-based information."[9]

Figure 1. Permission screens controlling location service on the Android and iPhone platforms. (Location Services and subsequent collection is ON by default on both platforms.)

2. In Local Cache Files on the Device

In order to improve the speed of location look-ups and to further reduce battery consumption, many mobile platform developers design their systems to keep a local copy - a "cache" - of location information from previous queries on the mobile device. This allows a mobile device to determine its location without having to re-query the location provider every time it's near a previously seen landmark.

Like any repository of sensitive information, this cache of location data poses potential privacy issues. As mentioned previously, a person who is able to gain access to this database might be able to determine the user's past whereabouts (subject to the historical length of the cache). In addition, last month, researchers identified a cache of location data that includes a full year's worth of location history stored on their Apple iPhone device.[10] This data had been recorded by

[9] Apple Inc's Response For Information Regarding Its Privacy Policy and Location-Based Services. (2010, July 12). From http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf at page 7.

[10] Allan, Alasdair and Pete Warden. (2011, April 20). Got An iPhone or 3G iPad? Apple Is Recording Your Moves. From http://radar.oreilly.com/2011/04/apple-location-tracking.html.

iPhones even when a user elected to disable location services. This effectively means that, in addition to there being no meaningful mechanism by which consumers can disable the background collection of location data by location providers, they also lack a meaningful mechanism to disable the collection of location data in a cache file. The researchers also found a copy of this same cache file stored insecurely on computers that had been used to synchronize or backup their iPhones, iPads, and other iOS devices.[11]

By analyzing the data stored in this cache, which is a record of nearby cellular towers and Wi-Fi access points the phone encountered, the researchers were able to re-create a map of their previous travels from Washington DC to New York, as shown below in Figure 2. They also publicly released a tool that consumers could use to easily access and visualize their own location histories.[12]

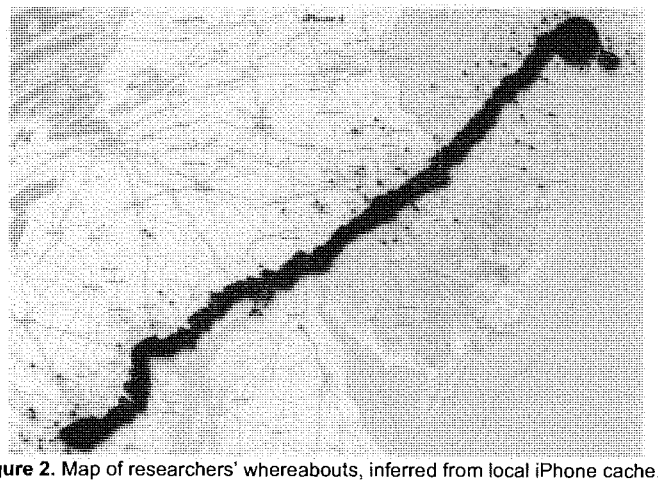


Figure 2. Map of researchers' whereabouts, inferred from local iPhone cache.[13]

[11] Apple announced a fix for this bug which reduces the size of the location database cache, stops transfer to iTunes when you connect your device to a computer, and deletes the cache entirely when you turn Location Services off. However, this fix doesnt apply to older 2G and 3G devices. Chen, Jacqui. (2011, May 05). iOS 4.3.3 is out with location tracking fixes for iPhone, iPad. From http://arstechnica.com/apple/news/2011/05/ios-433-is-out-with-location-tracking-fixes-for-iphone-ipad.ars

[12] Warden, Pete. (2011, April 20). iPhoneTracker. From http://petewarden.github.com/iPhoneTracker/

[13] Allan, Alasdair. (2011, April 20). Got an iPhone or 3G iPad? Apple Is Recording Your Moves. From http://radar.oreilly.com/2011/04/apple-location-tracking.html

Further research into competing platforms showed that Apple was not alone in this practice. Google and Microsoft smartphones also cache location histories, although the retention period for this information on these platforms appears to be shorter.[14]

It's worth noting here that while the recent "discovery" of local location caches has better informed the public about the issue, researchers and law enforcement have been aware of this practice for some time.[15] In addition to location history, researchers have repeatedly demonstrated that personal information such as email, text messages, browsing history, photos, and passwords can be recovered easily with physical access to the devices and, in some cases, remotely.[16] Surprisingly, this is even true for applications typically thought to be impervious to monitoring, such as the encrypted voice calling program Skype.[17]

3. By Smartphone Applications

In addition to storing location data locally and transmitting it to Location Providers, many users' smartphones will transmit their location and other sensitive data to numerous third parties via the use of third-party applications, such as games and other software programs. The specific parties and amount of information will vary depending on the specific "apps" used. However, the practice of transmitting potentially sensitive data off of the device is common for most applications.

---

[14] Gohring, Nancy. (2011, April 29). Microsoft Admits To More Windows Phone Update Problems. From http://www.pcworld.com/article/226733/microsoft_admits_to_more_windows_phone_update_problems.html and Foresman, Chris. Android Phone Keeps Location Cache Too, But It's Harder To Access. From http://arstechnica.com/gadgets/news/2011/04/android-phones-keep-location-cache-too-but-its-harder-to-access.ars

[15] Levinson presented his research on the iPhone cache file at a conference six months ago and subsequently published his findings in December 2010. Levinson, Alex. (2011, April 21). Three Major Issues with the Latest iPhone Tracking "Discovery." From https://alexlevinson.wordpress.com/2011/04/21/3-major-issues-with-the-latest-iphone-tracking-discovery/. Johnson, Bobbie. (2011, April 21). Researcher: iPhone Location Data Already Used By Cops. From http://gigaom.com/2011/04/21/researcher-iphone-location-data-already-used-by-cops/.

[16] Edwards, Sarah. Inside the App: All Your Data are Belong to Me. From http://www.shmoocon.org/speakers#insideapp

[17] A design vulnerability in the secure calling software Skype allows access to "full name, date of birth, city/state/country, home phone, office phone, cell phone and email addresses" of users because files on the device had insecure permissions and we stored in an unencrypted format. Case, Justin. (2011, April 15). (Updated) Exclusive Vulnerability In Skype For Android Is Exposing Your Name, Phone Number, Chat Logs, And A Lot More. From http://www.androidpolice.com/2011/04/14/exclusive-vulnerability-in-skype-for-android-is-exposing-your-name-phone-number-chat-logs-and-a-lot-more/

In a survey of the 101 popular iPhone and Android phone apps in December 2010, The Wall Street Journal found that 47 of them transmitted the phone's location and 56 also transmitted identifiers (such as hardware serial numbers) to a third parties.[18] Sometimes this information would go to the application developer's server, such as Yelp.com when using the Yelp "app." Other times, the location would be shared by the app further afield to its advertising partners without clear indication to the end-user. Fourty-five apps had no discernible privacy policies, and neither Apple nor Google requires apps to have privacy policies.

While user consent is typically required before applications are allowed to access location information, the purpose may not always be apparent to the user, and the user may have no indication that this information will subsequently be disclosed to third parties. For example, one iPhone app called Ninjump—a game—accesses and sends the a mobile device's location information to its mobile ad provider.[19] Most users would probably be befuddled about why an action game would ever need to access their location or disclose it to others, even if they consented to the initial collection of this information.

Data sharing isn't limited to location information. Applications can access and transmit data which includes text messages, emails, phone numbers, contacts stored, and even browser history stored on the device, as well as any information users knowingly enter in the process of using the app.[20] Some of this sharing may be expected, while other times it may be surprising. One example is where a popular social networking application had uploaded entire copies of users' address books to Facebook's servers.[21]

C. IMPLICATIONS FOR CONSUMER PRIVACY

These recent issues demonstrate key points of contention between consumers privacy and business interests.

1. Existing Notice and Choice Mechanisms Are Insufficient

Mobile apps and platforms do not provide consumers with sufficiently detailed notices about how their location and other sensitive information will be collected and used. Notice requirements vary from platform-to-platform. However, many disclosures related to privacy, such as data retention and sharing, frequently go unmentioned. The notices also rarely differentiate between first and third party data uses nor do they reveal business partners, like ad

---

[18] Thurm, Scott and Yutari Iwatani Kane. (2010, December 17). Your Apps Are Watching You. From http://online.wsj.com/article/SB10001424052748704694004576020083703574602.html
[19] WSJ Blogs. (2011, December 17). What They Know Mobile. Ninjump. From http://blogs.wsj.com/wtk-mobile/2010/12/17/ninjump/
[20] Seriot, Nicolas. (2010). iPhone Privacy. From http://seriot.ch/resources/talks_papers/iPhonePrivacy.pdf
[21] Moos, Kurt von. (2010, February 26). Privacy Fails: How Facebook Steals Your Friends Numbers. From http://kurtvonmoos.com/facebook_steals_contact_info/

networks, by name. As such, consumers are unable to make meaningful choices regarding their privacy risks when using mobile devices.

For example, with the exception of real-time location data, Apple's iOS platform for iPhones does not disclose to users what other location information may be accessed and shared by applications upon download. The iOS platform also does not inform users if an app will collect information from their address books, calendars, or other data from their iPhone.

Consumers are given a chance to "click through" to discover individual app privacy policies, but these are often long legal statements that are particularly difficult to read on a small mobile screen,[22] when they're even available. Comparatively, the Android platform allows more descriptive notices informing users of the data an app will collect. Although many of the terms used in these notice are still very technical in nature and can appear cryptic for a lay user to understand.

While mobile platforms today allow users to first review these disclosure notices before they install an app. But they also all adopt a "take it or leave it" approach to application permissions: the user can either allow access to all of the information the app requests, or deny all access (and thus not install the app). Granular permissions are not typically made available. That is, users are forced to give up their location information if they want to play the Ninjump game.

2. Collected Location Information Can Be Sensitive

Some industry players dismiss the recent concern about location privacy by saying that the information collected is not actually *device* location information. In Apple's Q&A on location data, they say that some of the collected information is about network equipment "some of which may be located more than one hundred miles away."[23]

While this may be true for cellular location in sparse rural areas, many urban environments yield device location measurements as accurate as 50 to 200 feet.[24] Since Wi-Fi is a short-range communication, knowing even one nearby Wi-Fi signal can typically pin the user within 100 feet.

---

[22] This matter became the underlying premise of a popular television show parodying "Apple's ridiculous 55-page iTunes terms and conditions." O'Grady. Jason. D (2011, April 28) South Park parodies iTunes terms and conditions. From http://www.zdnet.com/blog/apple/south-park-parodies-itunes-terms-and-conditions/10043.

[23] Apple. (2011, April 27). Apple Q&A On Location Data. From http://www.apple.com/pr/library/2011/04/27location_qa.html

[24] Steve Lee, product manager for Google Maps for Mobile and Google Latitude said in a May 2010 email that Google had 300 million Wi-Fi networks in its database which could pinpoint a device's location to within about 100 feet. Efrati, Amir. (2011, May 1). Google Calls Location Data 'Valuable.' From http://online.wsj.com/article/SB10001424052748703703304576297450030517830.html

As a quick demonstration, I recorded my device's location while sitting on a bench in the lobby of Hart Senate Office Building. Using GPS, my location was accurately reported to within 20 meters, as indicated by the small circle at the center of the left image in Figure 3 below. The right image shows nearly the exact same location found using Wi-Fi geolocation, which only uses a location database maintained by Google.

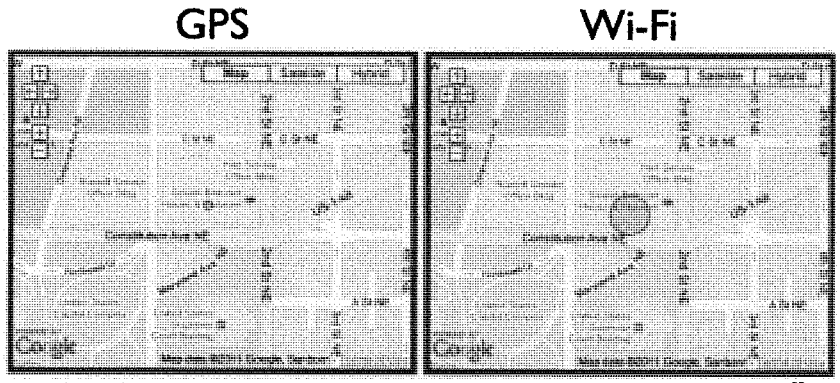


Figure 3. Comparing the accuracy of GPS and Wi-Fi based geolocation techniques.[25]

Quite a lot of information can be deduced from trails of historical location data. People are creatures of habit,[26] and it would often be easy to deduce where an individual works from her location on weekdays from 9am-5pm or, from the same nightly location, where she sleeps. These two pieces of information start to form a picture of who the device owner is.

3. Location Data Can Be Tied to Consumer Identities

Industry also argues that location data cannot be associated with consumers' real identities, and that this data if often simply "anonymous usage statistics."[27] However, to the degree that this data is also associated with unique identifiers—such as serial numbers or IP addresses that can

[25] The strongest Wi-Fi signal my device could detect was one of the "Odyssey" access points. Google's geolocation database reported the location of this access point (and thus my location) to within 120 meters as indicated by the circle in the right image.

[26] 93% of people return to the same locations: Song, C., Qu, Z., Blumm, N., and Barabási, A.L. Limits of predictability in human mobility. Science. 2010 Feb 19, 327(5968): 1018-21. From http://www.ncbi.nlm.nih.gov/pubmed/20167789

[27] "Google spokesman said it collects information anonymously." Kane, Yukari Iwatani, and Jennifer Valentino-DeVries. (2011, April 28). Jobs Tries to Calm iPhone Imbroglio. From http://online.wsj.com/article/SB10001424052748703367004576288790268529716.html

later be linked back to an individual device or person[28]—it becomes difficult to refer to it as "anonymous information."[29]

Identifiers enable further correlations with additional information generated via other channels, such as subscriber information (from a wireless carrier), login credentials (from phones that sync their e-mail or calendars), or even in some cases name, credit card or address information used in the app marketplace. For example, research recently demonstrated that "anonymous" device identifiers can easily be correlated to user's location and identity" in the form of pseudonyms and Facebook profiles with a reasonable degree of likelihood.[30]

Whether re-identification is possible depends on what other information is available, which itself hinges on the data retention and security practices of multiple participants in this ecosystem. It is rarely the case that information should be called "anonymous," since there is nearly always some small chance of re-identification.

Fortunately, at least some in industry share this view. When asked about the anonymity of location, the CEO of Location Provider Skyhook Jay Yarao stated:

> "I[f] you associate any history of a user at all it's very easy to, after the fact, figure out the name of that user. So when you hear companies like Microsoft and Google say, 'We're anonymizing the data,' it doesn't matter. If there's a location history, all I do is look at past 9 o'clock and there's a 95% chance that you went home. And I will look at that, and I will look up that address and I will know who you are. And as you start adding more and more data, I match that with where you work and now I know this is you."[31]

---

[28] While IP addresses can be dynamic, they can persist for days. IP addresses assigned to phones on the Verizon and Sprint do not change over a 2-day test period. See Balakrishnan, Mahesh, Iqbal Mohomed, and Venugopalan Ramusubramanian. (2009). Where's That Phone? Geolocating IP Addresses on 3G Networks. From http://research.microsoft.com/en-us/um/people/maheshba/papers/ephemera-imc09.pdf

[29]The Dutch Data Protection Authority argues that MAC addresses, in combination with the ability to identify the location of wireless hardware, may by itself qualify as personal information. Preuschat, Archibald. (2011, April 20). Google Faces New Demands In Netherlands Over Street View Data. From http://online.wsj.com/article/0,,SB10001424052748703922504576273151673266520,00.html

[30]Recently, a researcher demonstrated that device IDs can be linked to GPS location (30%), Weak Identities (20%), and Facebook profiles (10%) using public game service OpenFeint. See Cortesi, Aldo. (2011, May 4). De-Anonymizing Apple UDIDs with OpenFeint. From http://corte.si/posts/security/openfeint-udid-deanonymization/index.html

[31] Yarao, Jay. (2011, April 28). Everything You Need To Know About How Phones Are Stalking You Everywhere. From http://www.businessinsider.com/skyhook-ceo-2011-4

D. Conclusion

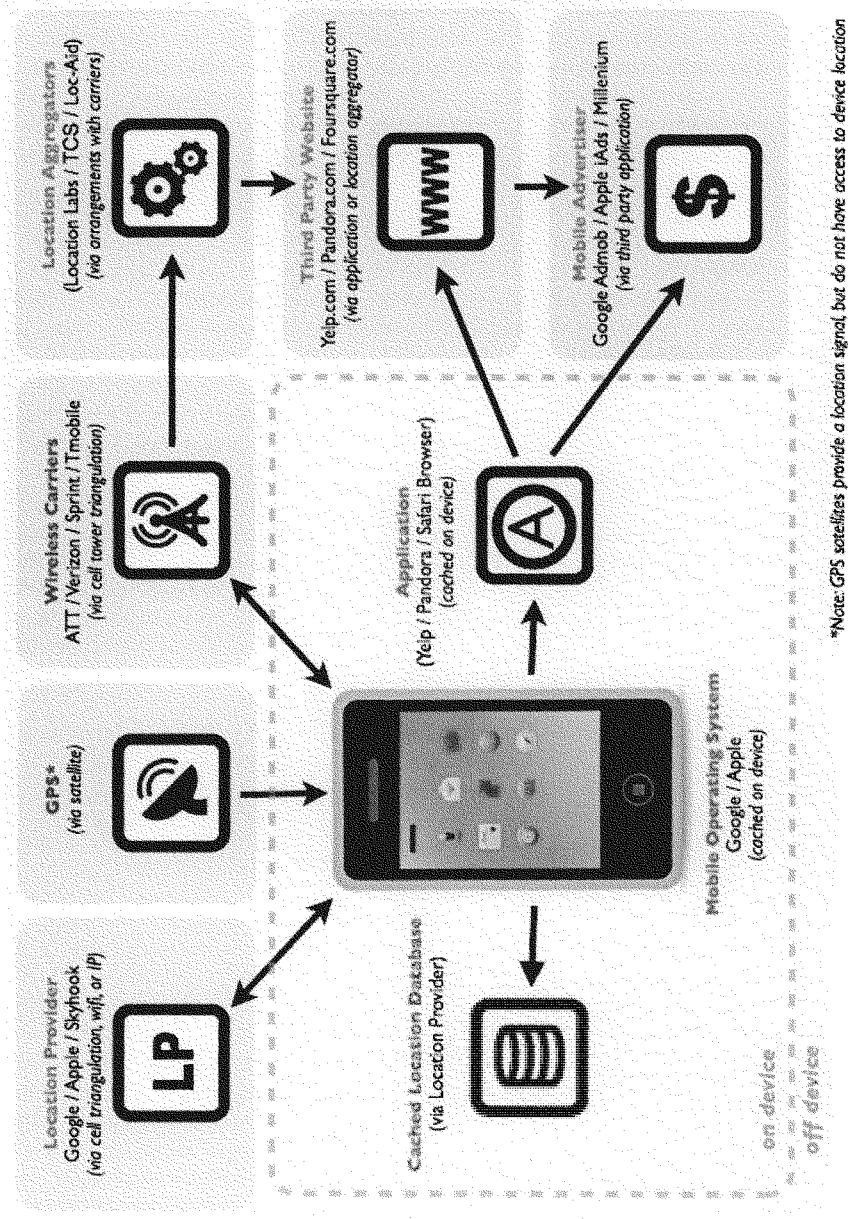
As mobile devices become more powerful—and more ingrained in the way consumers work and play—information about where a device is located becomes an ever more valuable input for commercial activity. But at the same time, consumers have expressed significant concern about how their devices expose sensitive information about them in ways they might not expect. Consumers need to be able to trust their devices in order to take full advantage of all the benefits mobile technology has to offer.

To better protect consumer privacy going forward, I offer four suggestions:

1. Mobile platform providers and application developers should work together to provide consumers with more transparency into exactly what data are collected, how they are stored, to whom they are transmitted, and how they are secured and used.
2. Certain disclosures should be mandatory, such as clearly differentiateing between first and third party uses of all potentially sensitive data, and also between active use and passive background activity. Precise definitions for "location" and "identity" should be provided.
3. Providers and developers should also work to ensure that the information consumers entrust with them are handled securely and in line with their expectations.
4. Providers and developers should also offer meaningful choice, such as granular permissions and working opt-outs, to consumers so they can make effective, privacy-concious decisions in the marketplace.

Thank you for the opportunity to testify here today. Mobile privacy is a very nuanced issue, even for us technologists, so I thank the subcommittee for their attention on this increasingly important problem. I will be happy to answer any further questions.

Appendix A: Flow of Location Data in Mobile Ecosystem



Testimony of Dr. Guy "Bud" Tribble
Vice President for Software Technology
Apple Inc.

On

Protecting Mobile Privacy:
Your Smartphones, Tablets, Cell Phones and Your Privacy

Before the

Subcommittee on Privacy, Technology and The Law
Committee on the Judiciary
United States Senate
Washington, DC

May 10, 2011

Good morning Chairman Franken, Ranking Member Coburn, and Members of the Subcommittee. My name is Bud Tribble, and I am Vice President for Software Technology for Apple Inc. On behalf of Apple, I thank you for the opportunity to address this important subject.

Apple's Commitment To Protecting Our Customers' Privacy

Apple is deeply committed to protecting the privacy of our customers who use Apple mobile devices, including iPhone, iPad and iPod touch. Apple has adopted a comprehensive privacy policy for all its products and implemented industry-leading privacy features in its products to protect our customers' personal data. We are also deeply committed to meeting our customers' demands for prompt and accurate location-based services. These services offer many benefits to our customers by enhancing convenience and safety for shopping, travel and other activities.

To meet these goals, Apple provides easy-to-use tools that allow our consumers to control the collection and use of location data on all our mobile devices. We do not share personally identifiable information with third parties for their marketing purposes without consent, and we require third-party application developers to agree to specific restrictions protecting our customers' privacy. Apple is constantly innovating new technology, features and designs to provide our customers with greater privacy protection and the best possible user experience.

Apple welcomes inquiries about how it protects its customers' privacy while providing reliable and fast location-based services. For instance, Apple provided on July 12, 2010 to Representatives Barton and Markey a detailed description of its collection and use of location-based information. I testified regarding the same topic before the Committee on Commerce, Science, and Transportation on July 27, 2010. And on April 27, 2011, Apple released a public response to recent questions regarding the collection and use of location information. A copy of that response is attached to this testimony as Exhibit A. The initial point made in that response should be emphasized: Apple does not track users' locations – Apple has never done so and has no plans to ever do so.

In my testimony today, I would like to address the following topics: (1) Apple's Privacy Policy; (2) Apple's collection, storage and use of location information on Apple mobile devices; and (3) the use of location information by third-party applications and the iAd Advertising Network.

I. Apple's Privacy Policy

Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store. The Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.[1]

The Policy includes the following provision regarding location-based information:

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.
>
> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

This provision incorporates similar language regarding location-based information that appears in Apple End User Software License Agreements ("SLAs") for products that provide location-based services. For example, the current iPhone SLA states:

> Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide and improve these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide and improve location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** (Emphasis exists in the SLA.) You may withdraw this consent at any time by going to the Location Services setting on your iPhone and either turning off the global Location Services setting or turning off the individual location settings of each location-aware application on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such

[1] The links take customers to http://www.apple.com/privacy, which customers may also access directly.

> third party's terms and privacy policy on use of location data by such third party applications or services.

The Policy includes the following provision regarding third-party products, such as iPhone apps:

> Apple websites, products, applications, and services may contain links to third-party websites, products, and services. Our products and services may also use or offer products or services from third parties – for example, a third-party iPhone app. Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties.

The Policy also includes the following language regarding mobile advertisements, such as those served through Apple's iAd service:

> Apple and its partners use cookies and other technologies in mobile advertising services to control the number of times you see a given ad, deliver ads that relate to your interests, and measure the effectiveness of ad campaigns. If you do not want to receive ads with this level of relevance on your mobile device, you can opt out by accessing the following link on your device: http://oo.apple.com. If you opt out, you will continue to receive the same number of mobile ads, but they may be less relevant because they will not be based on your interests. You may still see ads related to the content on a web page or in an application or based on other non-personal information. This opt-out applies only to Apple advertising services and does not affect interest-based advertising from other advertising networks.

The Policy identifies a dedicated page on Apple's website where customers may submit privacy-related inquiries and comments. Apple monitors these submissions and responds to appropriate inquiries in a timely manner. Customers may also address privacy concerns to TRUSTe, Apple's third-party privacy monitor. A link to TRUSTe is displayed within the Policy.

As noted above, customers may access the Policy from every page on Apple's website. The Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store.

Customers attempting to open a new iTunes Store account are directed to a webpage titled: "iTunes Store Terms & Conditions and Apple's Privacy Policy." They are asked to click the same unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy."

Apple updated the Policy on June 21, 2010.[2] The first time each existing iTunes Store customer logged on to the iTunes Store after that date, the iTunes Store displayed a message that prompted the customer to review the iTunes Store Terms and Conditions. The message stated:

---

[2] Note that on March 31, 2011, Apple made two non-material updates to its June 21, 2010 Privacy Policy. Specifically, Apple updated: (1) the URL where users can login to their accounts to view and modify their preferences and contact information and (2) the mechanism provided to users to ask questions about the Policy.

> iTunes Store Terms and Conditions have changed. Please read and agree to the terms and conditions below to continue using the iTunes Store.

Customers were asked to click an unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not agree to the Terms and Conditions and the Policy are not be able to use the iTunes Store (e.g., cannot make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

II. Location Information and Location-Based Services for Mobile Devices

Apple began providing location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location or finding nearby restaurants or stores.

Apple offers location-based services on a variety of mobile devices, including the iPhone 3G, iPhone 3GS, iPhone 4 CDMA and GSM models, iPad Wi-Fi + 3G, iPad 2 Wi-Fi and 3G and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, and iPod touch.

All of Apple's mobile devices run on Apple's proprietary mobile operating system, iOS. Apple released iOS 4.1 on September 8, 2010. Apple released the current versions, iOS 4.3.3 and 4.2.8 (for the iPhone 4 CDMA model), on May 4, 2011. Currently, iOS 4.3.3 may be run on iPhone 3GS, iPhone 4 GSM model, iPod touch 3rd and 4th generations, iPad, and iPad 2. My testimony focuses on iOS 4.1 and later versions, including the free iOS update Apple released on May 4, 2011.

A. Privacy Features

Apple has designed features that enable customers to exercise control over the use of location-based services.

First, Apple provides its customers with the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "Location Services" menu under "Settings." As described more fully below, when this toggle is switched "Off," (1) iOS will not provide any location information to any applications, including applications that may have previously received consent to use location information; (2) iOS will not collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; and (3) iOS will not upload any location information to Apple from the device.

Second, Apple requires express customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," iOS will not provide any location-based information to the application. This dialog box is mandatory—neither Apple's applications nor those of third parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even if Location Services is "On." The Location Services settings menu

provides an "On/Off" toggle switch for each application that has requested location-based information. When the switch for a particular application is "Off," no location-based information will be provided to that application.

Fourth, Customers can change their individual application settings at any time. An arrow icon ( ) alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the "On/Off" switch for any application that has used location-based information in the past twenty-four hours.

Finally, customers can use Restrictions, also known as Parental Controls, on a mobile device to prevent access to specific features, including Location Services. When a customer enables Restrictions, the customer must enter a passcode (this passcode is separate from the device passcode that the customer may set). If the customer turns Location Services off and selects "Don't Allow Changes," the user of the device cannot turn on Location Services without that passcode.

B. Location Information

1. Crowd-Sourced Database of Cell Tower Location and Wi-Fi Hotspot Information

Customers want and expect their mobile devices to be able to quickly and reliably determine their current locations in order to provide accurate location-based services. If the device contains a GPS chip, the device can determine its current location using GPS satellite data. But this process can take up to several minutes. Obviously, if the device does not have a GPS chip, no GPS location data will be available.

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer's request for current location information, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points – also referred to as Wi-Fi hotspots. As described in greater detail below, Apple collects from millions of Apple devices anonymous location information for cell towers and Wi-Fi hotspots.[3] From this anonymous information, Apple has been able, over time, to calculate the known locations of many millions of Wi-Fi hot spots and cell towers. Because the basis for this location information is the "crowd" of Apple devices, Apple refers to this as its "crowd-sourced" database.

The crowd-sourced database contains the following information:

> Cell Tower Information: Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a

[3] During this collection process, iOS does not transmit to Apple any data that is uniquely associated with the device or the customer.

mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.

Wi-Fi Access Point Information: Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

The crowd-sourced database does not reveal personal information about any customer. An Apple mobile device running Apple's mobile device operating system, iOS, can use the crowd-sourced database to (1) provide the customer with an approximate location while waiting for the more precise GPS location, (2) find GPS satellites much more quickly, significantly reducing the wait time for the GPS location, and (3) triangulate the device location when GPS is not available (such as indoors or in basements). The device performs all of these calculations in response to a request for location information from an application on the customer's device that has been explicitly approved by the user to obtain the current location, and the device requests from Apple the crowd-sourced database information needed for these calculations.[4]

The crowd-sourced database must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. In collecting and maintaining its crowd-sourced database, Apple always has taken great care to protect its customers' privacy.

2. Downloading Crowd-Sourced Data To A Mobile Device

To further improve the speed with which the device can calculate location, Apple downloads a subset of the crowd-sourced database content to a local cache on the device. This content describes the known locations of Wi-Fi hotspots[5] and cell towers that the device can "see" and/or that are nearby, as well as nearby cell location area codes,[6] some of which may be more than one hundred miles away. The presence of the local cache on the device enables

---

[4] For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) databases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own databases to provide location-based services and for diagnostic purposes.

[5] For each Wi-Fi hotspot, the location information includes that hotspot's MAC address, latitude/longitude coordinates, and associated horizontal accuracy number. For each cell tower, the location information includes the cell tower ID, latitude/longitude coordinates, and associated horizontal accuracy number.

[6] Cell base stations are grouped into "location areas" for network planning purposes, and each location area is assigned a unique "location area code." This "location area code" is broadcast by the cell base stations.

the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

The local cache does not include a log of each time the device was near a particular hotspot or cell tower, and the local cache has never included such a log. For each Wi-Fi hotspot and cell tower, the local cache stores only that hotspot's/cell tower's most recent location information, downloaded from Apple's constantly updated crowd-sourced database. After a customer installs the free iOS software update, iOS will purge records that are older than seven days , and the cache will be deleted entirely when Location Services is turned off.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Apple issued a free iOS software update on May 4, 2011. Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

When a customer runs certain applications, those applications request location information from iOS. Because of a bug that existed prior to the update, even when Location Services was off, the device would anonymously send the IDs of visible Wi-Fi hotspots and cell towers, without any GPS information, to Apple's servers, Apple's servers would send back the known, crowd-sourced location information for those hotspots and cell towers (and nearby hotspots and cell towers), and the device would cache that information in the consolidated.db file. None of this downloaded crowd-sourced location information – or any other location information – was provided to or disclosed to the application.

The iOS software update fixed the bug that caused crowd-sourced location information to be downloaded to the device while Location Services was off. iOS will now delete any existing local cache from consolidated.db and, if Location Services is off, (1) Apple will not download any crowd-sourced location information to the device, regardless of whether a specific application requests that information, and (2) iOS will delete any cache of this information stored in cache.db.

3. Collections and Transmissions from Apple Mobile Devices

Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of devices to develop and refine Apple's database of crowd-sourced location information. The mobile devices intermittently collect information about Wi-Fi hotspots and cell towers they can "see" and tag that information with the device's current GPS coordinates, i.e. the devices "geo-tag" hotspots and towers.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a separate table in the local cache; thereafter, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection every twelve hours (or later if the device does not have Wi-Fi access at that time). Apple's servers use this information to re-calculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced database. Apple cannot identify the source of this information, and Apple

collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced database. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one application's request to use location information.

4. Additional Location Information Collections

If Location Services is on, Apple collects location information from mobile devices under the following four additional circumstances.

First, as mentioned in Apple's April 27 response, Apple is collecting anonymous traffic data to build a crowd-sourced automobile traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years. This information is temporarily stored in the local cache on the device, anonymously uploaded to Apple, and then deleted from the device.

Second, Apple collects anonymous diagnostic information from randomly-selected devices to evaluate and improve the performance of its mobile hardware and operating system. For example, Apple may collect information about a dropped cell phone call, including the calculated location of the device when a call was dropped, to help identify and address any cell connection issues. Before any diagnostic information is collected, the customer must provide express consent to Apple. Apple cannot associate this information with a particular customer.

Third, Apple obtains information about the device's location (the latitude/longitude coordinates) when an ad request is made. The device securely transmits this information to the Apple iAd servers, the iAd servers immediately convert the latitude/longitude coordinates to a five-digit zip code, and the iAd servers then discard the coordinates. Apple does not record or store the latitude/longitude coordinates – Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Finally, if a customer has consented to an application's collection and/or use of location information, iOS will provide current location information in response to a request from that application. iOS will provide that customer-approved application with the location of the device only; iOS does not provide applications with direct access to the local cache.

III. Third-Party Applications And The iAd Network

A. Third Party Applications

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad and iPod touch. Currently the App Store includes more than 350,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

Any customer with an iTunes account may purchase and download applications from the App Store. Developers do not receive any personal information about customers from Apple when applications are purchased. Only Apple has access to that information.

Third-party application developers must register as an "Apple Developer" by paying a fee and signing the iPhone Developer Agreement (the "IDA") and the Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit ("SDK") and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application;
- Developers must provide information to their customers regarding the use and disclosure of location-based information (e.g., a description on the App Store or adding a link to the applicable privacy policy);
- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access;
- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information;
- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;
- If the customer denies or withdraws consent, applications may not collect, transmit, process or utilize the customer's location data; and
- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions.

Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code. Apple, however, does not monitor applications after they are listed in the App Store, unless issues or problems arise.

B. The iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network. The network can serve ads to iPhone, iPod touch, and iPad devices running iOS 4, and the network offers a dynamic way to incorporate and access advertising within applications. Customers can receive advertising that relates to their interests ("interest-based advertising") and/or their location

("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

As specified in the Policy and the relevant device SLAs, customers may opt out of interest-based advertising by visiting the following site from their mobile device: https://oo.apple.com. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."

For customers who do not toggle location-based service capabilities to "Off," Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Apple does not share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

In some cases, an advertiser may want to provide more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialog box will appear stating: "'Advertiser' would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad application with more specific location information—the information is not provided to the advertiser.

In closing, let me again affirm that Apple is strongly committed to protecting our customers' privacy. We give our customers clear notice of our privacy policies, and our mobile products enable our customers to exercise control over their personal information in a simple and elegant way. We share the Committee's concerns about the collection and potential misuse of all customer data, particularly personal information, and we appreciate this opportunity to explain our policies and procedures.

I will be happy to answer any questions you may have.

Exhibit A
April 27, 2011
Apple Q&A on Location Data

April 27, 2011

Apple Q&A on Location Data

Apple would like to respond to the questions we have recently received about the gathering and use of location information by our devices.

1. Why is Apple tracking the location of my iPhone?
Apple is not tracking the location of your iPhone. Apple has never done so and has no plans to ever do so.

2. Then why is everyone so concerned about this?
Providing mobile users with fast and accurate location information while preserving their security and privacy has raised some very complex technical issues which are hard to communicate in a soundbite. Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.

3. Why is my iPhone logging my location?
The iPhone is not logging your location. Rather, it's maintaining a database of Wi-Fi hotspots and cell towers around your current location, some of which may be located more than one hundred miles away from your iPhone, to help your iPhone rapidly and accurately calculate its location when requested. Calculating a phone's location using just GPS satellite data can take up to several minutes. iPhone can reduce this time to just a few seconds by using Wi-Fi hotspot and cell tower data to quickly find GPS satellites, and even triangulate its location using just Wi-Fi hotspot and cell tower data when GPS is not available (such as indoors or in basements). These calculations are performed live on the iPhone using a crowd-sourced database of Wi-Fi hotspot and cell tower data that is generated by tens of millions of iPhones sending the geo-tagged locations of nearby Wi-Fi hotspots and cell towers in an anonymous and encrypted form to Apple.

4. Is this crowd-sourced database stored on the iPhone?
The entire crowd-sourced database is too big to store on an iPhone, so we download an appropriate subset (cache) onto each iPhone. This cache is protected but not encrypted, and is backed up in iTunes whenever you back up your iPhone. The backup is encrypted or not, depending on the user settings in iTunes. The location data that researchers are seeing on the iPhone is not the past or present location of the iPhone, but rather the locations of Wi-Fi hotspots and cell towers surrounding the iPhone's location, which can be more than one hundred miles away from the iPhone. We plan to cease backing up this cache in a software update coming soon (see Software Update section below).

5. Can Apple locate me based on my geo-tagged Wi-Fi hotspot and cell tower data?
No. This data is sent to Apple in an anonymous and encrypted form. Apple cannot identify the source of this data.

6. People have identified up to a year's worth of location data being stored on the iPhone. Why does my iPhone need so much data in order to assist it in finding my location today?
This data is not the iPhone's location data—it is a subset (cache) of the crowd-sourced Wi-Fi hotspot and cell tower database which is downloaded from Apple into the iPhone to assist the iPhone in rapidly and accurately calculating location. The reason the iPhone stores so much data is a bug we uncovered and plan to fix shortly (see Software Update section below). We don't think the iPhone needs to store more than seven days of this data.

7. When I turn off Location Services, why does my iPhone sometimes continue updating its Wi-Fi and cell tower data from Apple's crowd-sourced database?
It shouldn't. This is a bug, which we plan to fix shortly (see Software Update section below).

8. What other location data is Apple collecting from the iPhone besides crowd-sourced Wi-Fi hotspot and cell tower data?
Apple is now collecting anonymous traffic data to build a crowd-sourced traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years.

9. Does Apple currently provide any data collected from iPhones to third parties?
We provide anonymous crash logs from users that have opted in to third-party developers to help them debug their apps. Our iAds advertising system can use location as a factor in targeting ads. Location is not shared with any third party or ad unless the user explicitly approves giving the current location to the current ad (for example, to request the ad locate the Target store nearest them).

10. Does Apple believe that personal information security and privacy are important?
Yes, we strongly do. For example, iPhone was the first to ask users to give their permission for each and every app that wanted to use location. Apple will continue to be one of the leaders in strengthening personal information security and privacy.

Software Update
Sometime in the next few weeks Apple will release a free iOS software update that:

- reduces the size of the crowd-sourced Wi-Fi hotspot and cell tower database cached on the iPhone,
- ceases backing up this cache, and
- deletes this cache entirely when Location Services is turned off.

In the next major iOS software release the cache will also be encrypted on the iPhone.

Press Contacts:
Natalie Harrison
Apple
harri@apple.com
(408) 862-0565

Natalie Kerris
Apple
nat@apple.com
(408) 974-6877

NOTE TO EDITORS: For additional information visit Apple's PR website, or call Apple's Media Helpline at (408) 974-2042.

Apple, the Apple logo, Mac, Mac OS, Macintosh, iPhone and iTunes are trademarks of Apple. Other company and product names may be trademarks of their respective owners.

Statement of Jonathan Zuck

President

The Association for Competitive Technology

Testimony before the Senate Committee on the Judiciary, Subcommittee on Privacy, Technology, and the Law

"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy"

May 10, 2011

Chairman Franken, Ranking Member Coburn, and distinguished members of the Committee: My name is Jonathan Zuck, and I would like to thank you for holding this important hearing on privacy and the growing mobile devices marketplace.

I am the president of the Association for Competitive Technology (ACT). ACT is an international advocacy and education organization for people who write software programs--referred to as application developers--and providers of information technology (IT) services. We represent over 3,000 small and mid-size IT firms throughout the world and advocate for public policies that help our members leverage their intellectual assets to raise capital, create jobs, and innovate.

Our community leaders are not political spokespersons—they are engineers; and I have drawn upon our membership's technical expertise and business concerns to inspire and inform these comments.

Prior to this hearing, several Senators and their staff asked for information about the size, scope, and impact of this new apps ecosystem; my testimony here strives to answer those questions as well as address concerns on privacy and security regarding mobile devices.

The new mobile apps world has sparked a renaissance in the software industry; small software companies are able to create innovative products and sell them directly to consumers. This is a radical departure from the era of up-front marketing costs, publisher delays, and piracy problems. The mobile app store has eliminated the longstanding barriers to entry that our industry battled for the past two decades.

My goal today is to help explain how small business is building this exciting new industry, how what we are doing is helping consumers, and how the very real concerns about privacy must be dealt with holistically, rather than from a technology-specific perspective.

Finally, for this renaissance to continue, government action must be careful to preserve the opportunities for small businesses to innovate, experiment, and compete with dominant market players.

The Smartphone Ecosystem is Creating Jobs and Opportunities in Tough Economy

The state of the U.S. economy is profoundly unsettled. Questions about job security, healthcare, and foreclosure have become dinner table conversation throughout this country.

In the face of all of this turmoil, there has been a bright spot in economic growth: Sales of smartphones and tablets, such as the iPhone, the HTC Thunderbolt (running Google Android), the Samsung Focus (running Microsoft WP7) , the iPad, Xoom, and now RIM's Playbook, continue to outpace all predictions and are providing a huge growth market in a slumping economy. In fact, nearly one hundred million smartphones were shipped in the first quarter of 2011[1] marking a 79% increase in an already fast growing market.

Vendor	1Q11 Shipments	1Q11 Market Share	1Q10 Shipments	1Q10 Market Share	1Q11/1Q10 Change
Nokia	24.2	24.3%	21.5	38.8%	12.6%
Apple	18.7	18.7%	8.7	15.7%	114.4%
Research In Motion	13.9	14.0%	10.6	19.1%	31.1%
Samsung	10.8	10.8%	2.4	4.3%	350.0%
HTC	8.9	8.9%	2.7	4.9%	229.6%
Others	23.2	23.2%	9.6	17.1%	143.7%
Total	**99.6**	**100.0%**	**55.4**	**100.0%**	**79.7%**

Source: IDC Worldwide Quarterly Mobile Phone Tracker, May 5, 2011

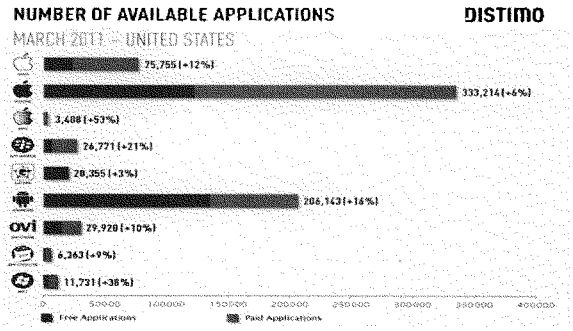
Note: Vendor shipments are branded shipments and exclude OEM sales for all vendors. 2

Smartphones that run third party applications are creating opportunities for handset manufacturers like HTC, Apple, and Motorola, communications firms like Verizon and AT&T, and most especially for application developers like our members.

In 2008, Apple launched an "apps store" to provide a place for developers to sell independently developed applications for the iPhone. Since then, over 300,000 new applications have gone on sale with billions of applications sold or downloaded. The Android platform has recently exceeded the growth rate seen in the iPhone, totaling more than 200,000 applications with 10,000 new programs available each month. In 2010 we saw the release of Windows Phone 7 with its own applications store and an entirely

[1] Mark Kurlyandchik, *IDC: Nokia Remains Top Smartphone Vendor Worldwide*, DailyTech, May 6, 2011.
[2] *Id.*

unique user interface. Total unique apps across all platforms are expected to exceed 500,000 by the end of 2011.[3]



Possibly the most important thing we have noticed about the new apps world is how it has revolutionized the software development industry. It is nothing less than a rebirth. Startup costs of the modern app developer are a fraction of what they used to be just 10 years ago. Gone now are the costs of printing discs, manuals, marketing materials, contracts with retailers, onerous contracts with publishers, and contracts with credit card providers all once necessary to sell a single product. Distribution is now all digital. Those costs savings in distribution are now used to hire more developers and artists, thus creating more jobs across the country. With mobile and Xbox 360 apps, we have seen the return of the small "garage," independent developer focused on products that can be created and shipped in a matter of months. The apps store model creates a direct bridge between the customer and the developer. Our members tell us that being a developer has not been this exciting since the origins of the personal computer and software industry in the 70s and 80s.

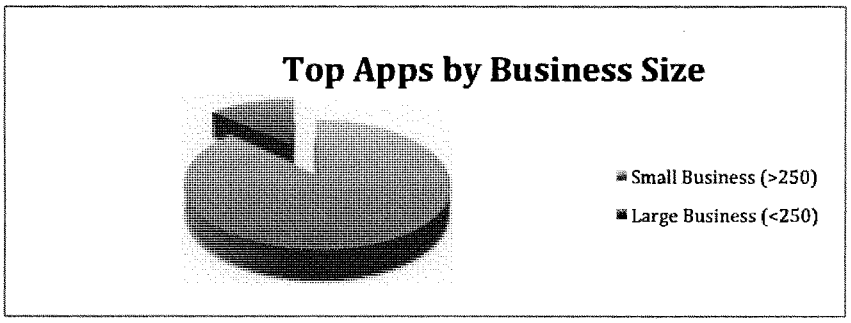
So who is this new generation developer? What does an apps creator look like? To find out, ACT conducted surveys and focus groups within our membership and also analyzed the top 500 selling apps.

First, we learned mobile apps are overwhelmingly created by developers in small businesses. A review of the top 500 best selling applications show that over 85% are

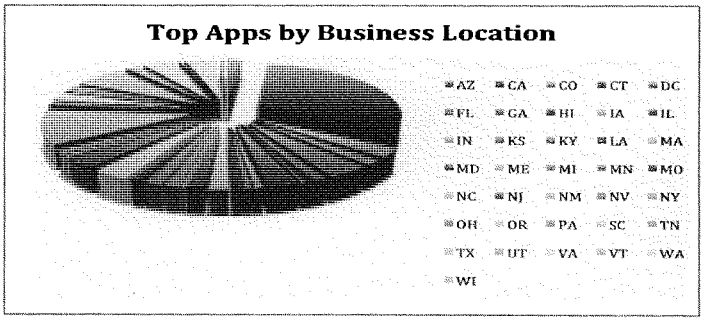
---

[3] *http://d2omthbq56rzfx.cloudfront.net/wp-content/uploads/2011/04/Distimo-survey-201103-app-stores-count.png*

written by small businesses[4]; in a majority of cases, micro businesses with less than 10 employees.



Second, app developers are not just in California. During the dotcom boom of the 1990s, the majority of growth occurred in Silicon Valley while the rest of the country did not reap all of the benefits of the economic boom. Conversely, the recent growth of the mobile apps industry has led to job creation all across the United States. While California continues to have a large representation of apps developers, nearly 70% of the businesses are located outside of the state of California. The independent nature of this burgeoning industry allows developers to live almost anywhere, including Moorhead, MN, and Tulsa, OK[5].



[4] *ACT analysis of top 500 selling apps, some discrepancies exist due to lack of verifiable employment data and apps created by a developer who has significant investment from a larger company. Some apps branded for a larger company are in fact developed by small firms subcontracted to build the application. Sample size of 408 applications, from "top apps" on March 25, 2011.*

[5] *ACT study of top selling apps as of March 25, 2011. ACT members Chalk LLC in Moorhead, MN, and Permafrost Software in Tulsa, OK.*

Third, app development companies have low initial costs, but also have the ability to become a highly successful and sustainable business. ACT's members reported development costs ranging from $1,000 to upwards of $1,000,000. Given the wide range of our findings and those of other reports[6], it is better to view the cost of mobile apps in tiers. In tier one, a simple app with no real back end server based functionality can run in the low thousands; this category makes up a significant percentage of all the apps in various mobile stores. They may be single feature programs, vanity apps, or just irreverent apps like iBeer.

The second tier are the apps that provide multiple levels of functionality. Often working with data stored in a remote server to provide information/user generated content or advanced capabilities like writing and saving specialized documents, this tier runs from $30,000 to $100,000.

The final tier runs from $100,000 on up. This category is for apps that may need to tie into sophisticated inventory management systems, require specialized licenses for content, interface with business critical databases not just to read, but also write information, and finally, games with immersive environments where art and music costs can be significant.

Understanding the Real Opportunity for Small Business

To get a sense of the size of the market and potential opportunity, we must first understand the various business models underlying the mobile app market. First, there are app developers who charge their customers to download their applications and/or charge them for purchases they make inside the app. For example, photography app Hipstamatic costs $1.99. If users want additional camera effects (Kodachrome or Holga, for instance) they can buy the add-ons in the application.

Second, some apps are supported either entirely or partly by advertising revenue. This is an increasingly important model especially as the Android platform grows in importance. Some applications charge for downloads and run advertisements inside the app itself.

---

[6] *http://appmuse.com/appmusing/how-much-does-it-cost-to-develop-a-mobile-app/*

Finally, many applications are given away free by larger companies in order to extend services to mobile devices or as marketing tools. From Citibank's online banking app to Pepsi's "Refresh Project" and Conde Nast's magazine apps, Fortune 1000 companies are increasingly offering mobile apps to their customers and potential customers. While large companies brand these apps, smaller companies with the expertise necessary to build world-class applications under tight deadlines usually build them.

Mobile App Stores

The exponential growth in app stores during the past few years is unprecedented. Apple launched the mobile app store arena with the iTunes App Store less than 4 years ago, soon followed by Nokia, Google, Microsoft, Amazon, and others. According to IHS, the worldwide market revenue of these app stores in 2010 was $2.15 billion, a 160% increase over 2009, and is expected to reach nearly $4 billion this year. Forrester Research estimates that the revenue created from customers buying and downloading apps to smartphones and tablets will reach $38 billion by 2015.

A growing percentage of revenues for app markets are coming from "in app purchases." According to Xyologic a company that indexes and analyzes app store data, 40 percent of game downloads are now free titles with in-app purchases. In March, it found there were more than 99.9 million downloads of free iPhone games from the App Store.

Yet revenues from app purchases and in-app purchases only represent a part of the overall opportunity for app developers. According to Xyologic, 80.8 percent of all app downloads in the month of March were free. While some of those apps relied on in-app purchasing for revenue, many others were supported by advertising or developed to support other brands and services.

Custom Mobile Development

The majority of the more than 600,000 free apps available across all app stores are not designed to be profitable on their own. They are designed as an extension to an existing service or a marketing program for an established or growing brand. Yet, the value of

these apps and the jobs they create are completely missed by the revenue numbers of app stores and advertising platforms.

This translates into an tremendous number of job-creating opportunities for smaller app development shops. Forrester Research predicts this market to reach $17 billion by 2015.

Mobile Advertising Revenues

In-app mobile advertising is growing more slowly than revenues from app downloads and in-app purchases, but it is a particularly important revenue model for apps with enormous scale, or "eyeballs," like the hugely successful Angry Birds. In the games category, which represents around half the app market, the total revenue from in-app advertising was $87 million according to Juniper Research. Juniper expects that to grow to around $900 million by 2015.

It is also worth noting that the business model of the platform makes a difference in how developers pursue revenue. As shown in an earlier chart, the iOS store has more than 333,000 applications and nearly 70% of those are paid for up front. Google/Android, a company whose entire revenue stream and dominant market position is dependent on advertising, tends to push developers towards the advertising model, with only 30% of the 206,000 apps relying on direct payment to the developer.

The Future for Mobile App Developers

Even more important are the opportunities that lay farther ahead. Members of Congress all have BlackBerries and many have iPhones, Androids, or Windows Mobile devices as well. Yet, according to a recent Morgan Stanley report[7], most people haven't yet invested in such technology. True "smartphones" have around 25% penetration in the U.S.; in Asia, it may be as low as 6%. This represents a pathway for growth leading far into the future.

To understand just how important international sales are to the mobile apps market, one only needs to look at a comparison between the total number of users possessed by a

[7] *http://www.morganstanley.com/institutional/techresearch/pdfs/2SETUP_12142009_R1.pdf*

combined AT&T / T-mobile (130 million wireless subscribers)[8] and China's number one wireless carrier, China mobile (584 million subscribers)[9]. Even if only 6% of China's mobile subscribers become smartphone users – and app purchasers – the market opportunity for U.S. software developers is huge.

How Location Based Information Helps Consumers

In the lead up to today's hearing, considerable attention has been directed at the type of information stored on smartphones. A misunderstood element in the public debate on this data collection is the essential role location information plays in the basic function of the device. People buy smartphones to have access to the Internet while they are mobile and a persistent connectivity is essential for this service.

When a smartphone tracks the location of its user, it is making a note to remind itself which access point or cell tower was used there to connect to the Internet. When a user returns to that area, the phone remembers this information. Each day most phone users travel the same route to work or to attend school and then return home to the same place. Keeping this data enables the smartphone to easily find an Internet connection providing efficient, constant online access. This is important for two reasons.

First is battery life. A phone uses a lot of power to search for a cell tower or wireless router. If it constantly needs to search for an Internet connection, it will deplete its battery many times more quickly than if it maintained a constant connection. Customers rate the importance of battery life very highly as a feature in the customer experience, so keeping a charge is a very important requirement of the phone. By maintaining a list of frequently visited locations, a smartphone avoids draining its battery in search of data connection points.

The other reason efficient connectivity matters is spectrum scarcity. The proliferation of smartphones has led to a crowded wireless spectrum, leading to potentially diminishing service quality. Wherever possible, wireless carriers are eager to connect users to wi-fi instead of their networks to provide faster connection speed and to lessen the burden on

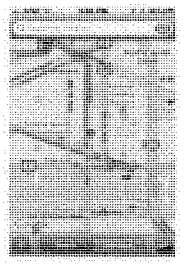
---

[8] *http://www.siouxcityjournal.com/business/local/article_f24b5818-ea11-5f04-b0b0-d7bbd02055b0.html*

[9] *http://www.wirelessweek.com/News/2011/01/Carriers-Subs-Reach-842M-China-Mobile/*

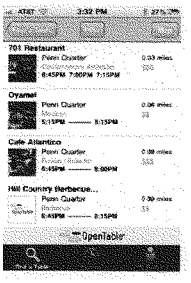
wireless networks. Carriers even provide their own wi-fi service for free to customers in densely populated areas to help alleviate the demand for wireless spectrum. By keeping track of the wi-fi and cell tower locations at frequently visited areas, the smartphone can allow users to automatically switch to wi-fi networks to provide constant, high quality Internet connectivity while diminishing the pressures on a crowded spectrum.

While location data is essential for phones to operate efficiently, consumers also love the smartphone services made possible using location-based technology. Many of the most successful apps or smartphone features have become popular based on knowing exactly where users are at any given time. And that's exactly how customers want it.



Map with Location and Traffic Data

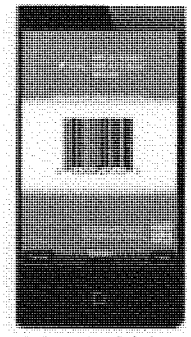
Anyone who has owned a smartphone has probably charted their location as a blue dot on their map app. Many also use those same programs to see where the traffic bottlenecks are before starting their evening commute. Some apps use location to help users find the nearest gas station, post office, parking garage, or coffee shop.



Open Table Reservations

The OpenTable app adds location technology to its existing services to allow diners to find open tables at nearby restaurants, read reviews, and make reservations with a simple tap of the button. Using location information, the app can also provide step-by-step directions to the establishment.

Location services on smartphones have also changed the way we interact socially, creating a market for check-in features to tell your friends and family where you are. Facebook has an app with this feature and, within the last decade, has achieved a market valuation approaching $100 billion. Foursquare, an app which exclusively provides check-in services, has been valued at nearly half a billion dollars.


Red Laser Bar Code Scan

There is clearly big business opportunity in this marketplace. But location-based services and advertising offer a unique opportunity for Main Street businesses as well. Some apps, like RedLaser, allow users to scan the UPC code of a product and, using the smartphone's location data, find several local retailers nearby where it can be purchased.

Meanwhile, a user searching for a particular product or service on their smartphone can receive an ad from a local small business based on their current location data. These ads have the benefit of reaching potential customers at the exact time of a purchasing decision and cost far less than the newspaper circulars or the TV ads that big box stores are able to afford.

Similarly, local small businesses can also level the playing field with the national chain stores and Internet retailers through shopping apps like Groupon. This app serves 38 million North American subscribers who receive daily discounts at local establishments based on their location data.

While improving the core performance of smartphones, location data is also the building block for apps that users find useful and provide small businesses with opportunities to reach new customers. This data also contains information about the user which they may want to keep private so appropriate safeguards must be in place to ensure it is used in a manner with which consumers are comfortable.

The Smartphone ID Conundrum

Recent news stories have focused on the existence of unique identifiers attached to each smartphone. Known as a UDID number for iPhone and Android ID for Android based products, this is a number that serves as a unique token for each device. The Wall Street Journal article "What They Know - Mobile"[10] made special effort to note the transmission of this number by nearly every single application in the market. While

[10] *http://blogs.wsj.com/wtk-mobile/*

highlighting the transmission of a "unique identifier" may make for good newsprint, the article unfortunately did not properly explain why developers transmit this number.

In order to help better explain the role this Smart Phone ID (SPID) number plays in the development and maintenance of mobile applications, ACT surveyed developers[11] to find out how they currently used the SPID number. Respondents highlighted three key uses:

- Allows developers to control access to parts of the program without locking the user out completely (i.e., locking achievement levels in games, viewing paid subscriber content);
- Prevents piracy of applications, allows verification of ownership for updates to apps; and
- Allows management of access control for software testing and customer service.

Additionally, developers reported on several benefits to their customers specifically and consumers in general. Most often cited were:

- Working in concert with other stored data, the SPID makes it possible to have applications remember your favorites even when you buy a new phone;
- Helps content providers know when your device is on a wi-fi network instead of 3G - allowing them to send you HD or other high bitrate content; and
- Makes it easier to receive updates without annoying verification procedures.

At first glance, it would seem to make perfect sense to only allow the SPID to be shared with the app maker itself, but not with third parties. However, in today's world, many different companies work together to provide services to customers. For instance, when shipping a product via FedEx, the sender shares considerable personal information about the recipient with the (third party) shipper including contact information and purchased items. Similarly, small businesses rely on cloud computing to give customers a complete service offering in a cost-effective way. For game developers, a company like OpenFeint offers an easy way to keep track of scores and allows game users to interact with each other, saving app makers thousands of dollars in development time and ongoing infrastructure cost. This service needs to be able to tell devices apart.

---

[11] *ACT April 28 questionnaire to members working on at least one mobile platform. Question: How do you currently use UDID/Android ID in your development process?*

Finally, developers felt that the usage restrictions and best practices for SPIDs were well documented, especially on Apple's iOS. As you can see from the documentation for the UIDevice.uniqueIdentifier[12], Apple gives plenty of advice to app makers on how to properly handle this information [emphasis added]:

> A device's unique identifier (sometimes abbreviated as UDID for Unique Device Identifier) **is a hash value composed from various hardware identifiers such as the device serial number**. It is guaranteed to be unique for each device. The UDID is independent of the device name. For devices that use a SIM (subscriber identity module) card, the UDID is independent of the SIM card.
>
> For user security and privacy, **you must not publicly associate** a device's unique identifier with a user account.
>
> You may use the UDID, in conjunction with an application-specific user ID, for identifying application-specific data on your server. For example, you could use a device-user combination ID to control access to registered products or when storing high scores for a game in a central server. However, if you are developing a game, you may want to instead use Game Center's player identifier key as explained in Game Kit Programming Guide.
>
> Important: **Never store user information based solely on the UDID**. Always use a combination of UDID and application-specific user ID. A combined ID ensures **that if a user passes a device on to another user, the new user will not have access to the original user's data**.

The key takeaway from this survey is that it is important, and often necessary, to keep devices separate and uniquely identified. Users may own many devices, multiple people may share devices (for example, family members), and others switch devices. Developers have different technical reasons to identify devices, but all come down to the same thing: enhancing the user experience. The developer's focus is in making the user's phone more convenient and useful.

While there may be some sinister ways in which the SPID can be illegally used, 99.9% of developers have the very best intentions. Specific instances of SPID abuse should be the focus of FTC action, not the very existence of such a valuable and valid tool.

---

[12] *http://developer.apple.com/library/ios/#documentation/uikit/reference/UIDevice_Class/Reference/UIDevice.html*

Understanding the Existing Laws and Regulations

Regardless of how data protection is approached, it is critical to understand the protections available under existing federal and state laws and regulations. Consumer protection laws with technology-neutral legal standards can address data-privacy and data-security concerns regardless of whether they arise from undisclosed hacking, phishing, lost laptops, website data-collection, inadvertent peer-to-peer "sharing" of sensitive personal files, unauthorized wi-fi-snooping, recklessly designed social-networking applications like Google Buzz, art contests seemingly designed to enable the reverse-engineering of children's social-security numbers, or mobile apps.

Currently, the FTC Act gives the FTC broad authority to act against those who misuse data, regardless of the technology used. Specifically, Section 5 of the FTC Act directs the FTC to take action against any business engaging in "deceptive" or "unfair" trade practices.[13]

The FTC's duty to halt deceptive trade practices authorizes the FTC to take law-enforcement action not only when a business violates explicit promises to consumers,[14] such as violations of stated privacy policies or terms of use, but also even when a business makes material omissions to consumers,[15] such as not telling consumers about the sharing of their collected information with third parties.

Similarly, the FTC's duty to halt unfair trade practices authorizes the FTC to take law-enforcement action when business practices cause injuries to consumers that are: substantial; not outweighed by countervailing benefits to consumers and competition; and could not have been reasonably avoided by consumers themselves.[16] For example, the FTC can take action against a business's failure to report a data breach.

Finally, it is critical to understand two points about consumer-protection laws. First, the FTC has real teeth if it finds that a company engaged in "unfair or deceptive practices,"

---

[13] 15 U.S.C. § 45
[14] *Id.*
[15] FTC, *Policy Statement on Deception (*Oct. 14, 1983) *available at* http://www.ftc.gov/bcp/policystmt/ad-decept.htm.
[16] 15 U.S.C. §45(n); *see also* FTC, *Policy Statement on Unfairness* (Dec. 17, 1980) *available at* http://www.ftc.gov/bcp/policystmt/ad-unfair.htm.

including assessing injunctive and civil penalties. Second, state consumer-protection acts grant state Attorneys General even broader substantive and remedial powers than those that federal law grants to the FTC. As a result, even were resource constraints or agency capture to preclude FTC action in a particular case, 50+ law-enforcement agencies would still have broad, technology-neutral authority to protect the privacy and security of consumers' data.

Consequently, the consumer-protection authority of the FTC and the State Attorneys General already authorizes and requires these law-enforcement agencies to patrol the Internet for companies that might violate their promises to consumers or cause them substantial harm. The FTC recently used such authority to protect consumer privacy by taking action against Google[17] and Chitika[18] for failing to properly handle consumers' information. Both companies now face twenty years of oversight and damage to their brands.

Existing consumer-protection laws thus already authorize both the FTC and state law enforcement agencies to police the entire range of products that connect to the Internet, including mobile devices, and to take action against the bad actors that ignore existing laws and will continue to ignore any future laws. This existing authority also ensures that good actors already have every incentive to behave reasonably and that bad actors have good reason to fear the existing legal consequences of their wrongdoing.

Given the existing authority of the FTC and the State Attorneys General, do we need additional regulation? ACT believes this is an open question, but one where consumer privacy protection should not be viewed through a limited, technology-specific lens. Instead, thoughtful, arduous, and considered discussion must take place on the role of personal data in the economy, the true interests of consumers, and the best interaction between citizens and the providers of products and services that use their data.

---

[17] *In the Matter of* Google Inc., a corporation, FTC File No. 102 3136.
[18] *In the Matter of* Chitika, Inc., a corporation, FTC File No. 1023087.

Avoiding the Patchwork Problem; Dealing with Data Holistically

In periods of great technological change, both new opportunities and new challenges are created. More often than not, however, the seemingly new challenges are merely old issues illuminated under a new light.

Like the dot-com boom before it, the emergence of smartphones and mobile apps has renewed interest in the way corporations and governments collect and share data, most importantly, personal data. Yet, in both cases, these new technologies are simply bringing new light to issues surrounding personal data collection and use that have existed for decades.

There are genuine questions to be asked and considered with respect to the collection and use of personal data. How and when should people be told the data is being collected or when it is being shared? How should they be told? Should people be able to modify data that is collected about themselves? Should people be able to delete data about themselves or otherwise control how it is used? Asking these questions only in the context of smartphones and mobile apps ignores the larger picture. The technology used to collect the data is much less significant than the important questions about the process and behavior of those collecting it.

First, the data collected by apps developers is an almost infinitesimal piece of the global collection of personal data. From credit card companies, to warranty cards, to loyalty programs, companies have been collecting data on their customers long before the Internet or smartphones came around. Not only do other companies collect the same data as smartphone apps, but they have exponentially larger collections of personal data already at their disposal. Information brokers like Epsilon and Google collect, retain, and share far more information than all mobile apps combined.

Even the collection of location data that has been singled out in recent press reports is not unique to smartphones and mobile apps. Standalone commercial GPS providers like TomTom or GPS-based safety services like OnStar collect this information on their users. Your EZ Pass technology for wireless payment of highway tolls also collects and stores location data. More recently, Google has been collecting personal information while

mapping home and business wireless networks. In nearly every instance, these companies may share that data with third parties.

All of this reminds us that isolating and regulating one specific technology is not the answer to the broader questions surrounding the collection and sharing of personal data. Given the enormity of existing data collections and the number of ways it is amassed, focusing exclusively on one technology – particularly the newest and least established – is a symbolic gesture that does not solve the underlying problem, but creates the false sense that the problem has been solved and the need for thoughtful debate and policy consideration is over. However, focusing instead on regulations of behavior and data usage, it then applies to everyone, regardless of means of collection and sharing.

Finally, perhaps the most dangerous problem is that when regulation focuses solely on new technology, it discriminates against small businesses. Whenever we are talking about new, disruptive technologies, we are most often talking about small businesses. Revenue models, customer expectations, and efficiency opportunities are all still emerging, and it is small businesses that perform that service. Lots of businesses start, a very small number survive, but in the end, we know what works, and then the large businesses get involved. To stunt the growth of a new, experimental market is to discriminate against the very small businesses on which we rely to lead innovation and growth in the American economy.

Conclusion

The future of the digital marketplace looks bright for small business, so long as the marketplace remains dynamic and competitive. This is a more than $10 billion opportunity for small business across the United States. Barriers to entry in the marketplace are currently low, and our members are very excited about the future – according to ACT's Board President, Mike Sax, "Programming is fun again!"

While there are important questions that need to be discussed on personal data collection, retention, and sharing, limiting this question solely to smartphones and mobile apps would be ineffectual and counterproductive.

The use of location information and smartphone ID's are providing immense value to consumers. Whether it's the ability to make dinner reservations or find directions to the nearest hardware store, our members put a value on creating a product that improves the lives of their customers.

Banning the collection of location data would essentially outlaw these beloved consumer apps while doing nothing to address the big questions about data collection and how that data is used. That is why ACT believes that Congress must take a holistic approach to privacy that does not single out any one technology, especially nascent ones. We need to outlaw bad behavior, not good technology. I hope that the committee will continue to focus the spotlight on the contribution small business makes to the future of the digital economy and the way government can do a better job to encourage that productive future. Thank you for your time and consideration on this important topic.

QUESTIONS FOR WITNESSES FROM HON. AL FRANKEN, HON. RICHARD BLUMENTHAL, AND HON. TOM COBURN

Questions from Senator Al Franken to Mr. Davidson

1. Will Google commit to requiring that all apps in the Android Market have a clear, understandable privacy policy?

2. If not, will Google at least commit to require that all location-aware apps in the Android market have a clear, understandable privacy policy?

3. Will Google commit to informing users through a clear, conspicuous method, i.e. a permission screen, that the apps they download have the technical ability to share or disclose the information they gather from the user to third parties?

4. Do you think that most users understand the terms used in your app permission screen? For example, if an app can have access to your "network connections", do you think the average user knows what that means? What can you do to make your permission screen more clear for average users without deep technical knowledge or sophistication?

5. Android OS devices transmit a unique identifier along with the location data that they transmit to Google servers. *See* Jennifer Valentino-Davies, "The Unique ID Android Uses in Collecting Location," *The Wall Street Journal*, April 26, 2011. Apple succeeds in collecting this information without such an identifier. Will Google refrain from using such identifier in future data collection?

6. Under what circumstances does Google consider location information obtained from a user's device to be non-content customer records data subject to the voluntary disclosure permission in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(c)(6)?

7. Since Google gets the vast majority of its revenue from advertising, it seems like your incentive to protect privacy might be in conflict with your incentive to collect your user's information. What relationship does AdMob have to the Android Operating System and applications in the Android App Market?

Questions from Senator Al Franken to Mr. Tribble

1. Will Apple commit to requiring that all apps in the Apple App Store have a clear, understandable privacy policy?

2. If not, will Apple at least commit to requiring that all location-aware apps in the Apple App Store have a clear, understandable privacy policy?

3. In your testimony you said that requiring apps to have privacy policies is not enough to protect user's privacy. I agree. What further steps can you take, in addition to requiring privacy policies, that will help users understand where their information is going and have greater control over it?

4. Will Apple commit to informing users though a clear, conspicuous method (i.e. a permission screen) of the non-location information (i.e. calendar information, address book information, etc.) that an app will access once it is downloaded onto an Apple mobile device?

5. Will Apple commit to informing users through a clear, conspicuous method (i.e. a permission screen) that the apps they download have the technical ability to share or disclose the information they gather from the user to third parties?

6. Apple appears to acknowledge that it has not done enough to educate users about how their location information is being used. *See* Apple Q&A on Location Data, April 27, 2011 ("Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.") Can you explain how Apple will improve its education of users about the way their location information is gathered, used and shared by Apple and others?

7. You have said that Apple audits the applications in the App Store and that if Apple finds an app is violating the Registered Apple Developer Agreement, it will remove it from the store. Yet when I asked you at the hearing how many apps had been kicked out of the store for violating these terms, you said "zero". Do you believe that there is not a single app that is currently violating your Developer Agreement?

8. In Apple's May 6, 2011 response to my letter of April 27, 2011, Apple wrote that when "using only the crowd-sourced locations of Wi-Fi hotspots and cell towers… the device location calculated by iOS will only be an approximation." Please give the mean, median, and mode of how accurately the device's location can be calculated using only the crowd-sourced database Apple maintains on mobile devices. Please use precise figures, e.g. 50m, 100m, etc.

9. In various statements, Apple has stressed that the hotspots and cell towers in the crowd-sourced database downloaded to users' mobile devices "could be more than one hundred miles away." Please give the mean, median, and mode of the distance these hotspots and cell towers are from users' devices. Please use precise figures, e.g. 50m, 100m, etc.

10. In an interview with All Things Digital, Apple founder Steve Jobs stated that the hotspots and cell tower data in the crowd-sourced database downloaded to users' mobile devices "are not telling you anything about your location." *See* Hayley Tsukayama, "Post Tech: Jobs explains mobile policies, says Apple will testify in hearing," *Washington Post*, April 27. Is it Apple's position that the WiFi hotspot and cell tower data in the crowd-sourced database downloaded to users' mobile devices do not in any way communicate anything about a user's location?

11. Apple has acknowledged that the crowd-sourced database cache stored on the iPhone should not have kept up to a year's worth of data. *See* Apple Q&A on Location Data, April 27, 2011 ("The reason the iPhone stores so much data is a bug we uncovered…"). On what date did Apple employees discover this "bug"?

12. On what date did Apple learn that the iPhone was submitting location information to Apple servers even when location services were turned off?

13. Under what circumstances does Apple consider location information obtained from a user's device to be non-content customer records data subject to the voluntary disclosure permission in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(c)(6)?

QFRs FOR JUSTIN BROOKMAN AND ASHKAN SOLTANI

1. In your view, is there anything the wireless access point location approximation scheme described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 78 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," that explicitly excludes the collection of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

2. These patent applications contemplate examining "data frames" to determine the location of wireless access points as contemplated in these patent applications, looking at "the data in the frame … itself" to determine the data rates of frames that might contain content data, and contemplate sending "raw data collected" back to "a central repository … for processing." If Google actually engaged in any of these practices, would it be accurate to describe Google's interception and/or storage of content data through its Street View program as unintentional? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

    a. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

    b. Indirectly valuable for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

    a. Legal or illegal under current federal law; or

    b. Legal or illegal under current state law.

Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.

FROM SENATOR RICHARD BLUMENTHAL

QFRs: FOR GOOGLE WITNESS

1. Please provide text and citations for any and all materials directly or indirectly associated with or related to the methods for intercepting wireless data transmissions traveling between third party computers and wireless access points described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

2. Please indicate where in the scheme described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" these patents explicitly exclude the interception of content data. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

3. Wireless signal interception as described in Paragraph 51 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 47 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" involves configuring a Google computer "to observe or capture data packets .. transmitted to or from" a wireless access point, with the Google computer "operat[ing] in a 'sniffer' or 'monitor' mode, thereby handling transmitted frames … without requiring" the Google computer "to be associated with" the wireless access point. This scheme appears to contemplate 'sniffing' (i.e., intercepting and decoding) all transmitted frames.

    a. Where does this patent distinguish between 'sniffing' or 'monitoring' frames containing content data and 'sniffing' or monitoring frames that did not contain content data? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

    b. Was there ever a version of Google's Street View programming designed to intercept and decode all of the information received from a wireless access point and then subsequently discard unwanted data?

    c. Was there ever a version of Google's Street View programming that distinguished between frames containing content data and frames that did not contain content data? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

    d. Was there ever a version of the software on Google's Street View cars that specifically deleted, blanked, or removed intercepted IP payload data?

e. Did the software addition that Google points to as responsible for collecting "payload data" affirmatively intercept and decode content, or did it remove a preexisting block on decoding content?

4. Does the term "data rate" as used in these patent applications consistently refer to information about the communication with the access point such as "data rate" as defined by 802.11 standards, or does it refer to a "measured" data rate?

5. Paragraphs 70-71 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraphs 66-67 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discuss 'evaluating different types of frames sent to (or received from) the device of interest" including "management frames, control frames, data frames, etc." as part of a scheme to estimate "the confidence of the location" of a wireless access point.

   a. Please explain what types of evaluations are contemplated for each of the three types of frames listed.

   b. How does evaluation of data frames contemplated in these paragraphs affect Google's estimate of the confidence of the location of a wireless access point?

6. Paragraphs 74-75 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraphs 70-71 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discuss determining "the confidence in the location" of a wireless access point, and note that "the types of frames that are used in the measurement, such as data frames, management frames, and/or control frames may affect the confidence."

   a. How do these patents contemplate evaluating these three types of frames in order to improve the confidence estimate for the location of the wireless access point?

   b. How does evaluation of data frames contemplated in these paragraphs affect Google's estimate of the confidence of the location of a wireless access point?

7. Paragraph 82 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 78 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discusses how "[T]he location of a given [wireless access point] may be based on a number of measurements taken by one or more client devices. <u>The raw data collected</u> by a client device may be processed locally <u>or sent to a central repository … for processing</u>" (emphasis added).

   a. Do these patent applications specifically exclude the collection of raw data that includes "content data" before sending it to a central repository for processing? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

b. Is there any relation between the scheme described in Paragraph 82 and the operation of the Google Street View cars during the period when those cars were used to identify the locations of wireless access points?

QFRs: FOR APPLE AND GOOGLE WITNESSES

1. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose? If so:

   A. Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.

   B. Please indicate any and all purpose(s) underlying any such signal interceptions.

   C. Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

   D. Please describe any and all methods initially contemplated and/or implemented for these purposes.

   E. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

   F. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

   G. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or

contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

H. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

1) If so, please explain how and why such content data is excluded from interception.

2) If not, please explain how and why such content data is not excluded from interception.

I. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

J. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.

K. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?

2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.

A. How many wireless access points exist, or have ever existed, in any database of wireless access point locations?

1) How many of these wireless access points were unencrypted when identified?

2) How many of these wireless access points were encrypted when identified?

3) How many of these wireless access points were "hidden" when identified?

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

B. Indirectly valuable to your company for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Legal or illegal under current federal law;

B. Legal or illegal under current state law; and

C. Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.

Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.

FROM SENATOR RICHARD BLUMENTHAL

QFRs: FOR APPLE WITNESS

1. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose? If so:

   A. Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.

   B. Please indicate any and all purpose(s) underlying any such signal interceptions.

   C. Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

   D. Please describe any and all methods initially contemplated and/or implemented for these purposes.

   E. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

   F. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

   G. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

   H. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies

from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

1) If so, please explain how and why such content data is excluded from interception.

2) If not, please explain how and why such content data is not excluded from interception.

I. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

J. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.

K. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?

2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.

A. How many wireless access points exist, or have ever existed, in any database of wireless access point locations?

1) How many of these wireless access points were unencrypted when identified?

2) How many of these wireless access points were encrypted when identified?

3) How many of these wireless access points were "hidden" when identified?

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

B. Indirectly valuable to your company for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Legal or illegal under current federal law;

B. Legal or illegal under current state law; and

C. Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.

Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.

Written Questions of Senator Tom Coburn, M.D.
Alan Davidson, Director of Public Policy, Americas, Google, Inc.
U.S. Senate Committee on the Judiciary
May 17, 2011

---

1. Google has stated it does not sell users' personally identifiable information to third parties. However, Google operates advertising services that are connected to mobile devices using its Android platform. Could you comment on how Google operates its ad services, particularly whether Google sends targeted ads to mobile device users, and if so, what user information Google collects in order to send targeted ads?

    a. Is advertising the largest source of revenue for Google? If not, what services or products contribute most to Google's bottom line?

    b. Are there any apps to which Google refuses to provide advertising services? If so, what are the primary reasons for refusing such services? If not, why?

    c. Are there any apps Google refuses to host on the Android app store? If so, what are the primary reasons for refusing to provide those apps, and how often, on average, does Google reject an app or later remove it from your store for questionable behavior?

    d. How many employees and/or automated services are dedicated to crawling your app store to weed out apps that inappropriately use consumers' personal information or violate your respective privacy policies?

    e. In other contexts, such as the sale of counterfeit pharmaceuticals online, there has been a recent push in the industry (with the suggestion of the Intellectual Property Enforcement Coordinator) to form a working group in order for the industry to take the lead on how to combat the dangerous use of these products online. Is there any such industry working group to address the unique issues surrounding mobile device products and/or location based services?

Written Questions of Senator Tom Coburn, M.D.
Dr. Guy "Bud" Tribble, Vice President for Software Technology
U.S. Senate Committee on the Judiciary
May 17, 2011

1. Mr. Tribble, in Mr. Soltani's testimony, he gave the committee an example whereby he seemed to imply that Apple had knowledge of his own iPhone's location within a few feet when he was sitting in the atrium of the Senate Hart Office Building using Wi-Fi. Your testimony states that Apple does not track users' locations. Can you clarify the seeming contradiction regarding the location data on Mr. Soltan"s iPhone in his example?

2. Apple states it does not sell users' personally identifiable information to third parties. However, Apple operates advertising services that are connected to mobile devices using its platform. Can you comment on how you operate your ad services, particularly whether you send targeted ads to mobile device users, and if so, what user information you collect in order to send targeted ads?

    a. Is advertising the largest source of revenue for Apple? If not, what services or products contribute most to your bottom line?

    b. Are there any apps to which Apple refuses to provide advertising services? If so, what are the primary reasons for refusing such services? If not, why?

    c. Are there any apps Apple refuses to host in its app stores? If so, what are the primary reasons for refusing to provide those apps, and how often, on average, do you reject an app or later remove it from your store for questionable behavior?

    d. How many employees and/or automated services are dedicated to crawling Apple's app store to weed out apps that inappropriately use consumers' personal information or violate its privacy policy?

    e. In other contexts, such as the sale of counterfeit pharmaceuticals online, there has been a recent push in the industry (with the suggestion of the Intellectual Property Enforcement Coordinator) to form a working group in order for the industry to take the lead on how to combat the dangerous use of these products online. Is there any such industry working group to address the unique issues surrounding mobile device products and/or location based services?

1634 Eye Street, NW
Suite 1100
Washington, DC 20006

June 1, 2011

United States Senate
Committee on the Judiciary
Chairman Patrick Leahy
ATTN: Julia Gagne
Hearing Clerk, Dirksen Office Building
Washington, DC 20510
Julia_Gagne@judiciary-dem.senate.gov

Re: Hearing on "Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones, and Your Privacy"

Dear Chairman Leahy:

I am writing to respond to the written Questions For the Record submitted by Senator Blumenthal regarding Google's interception of WiFi signals in order to build out its geolocation services database.

I appreciate the opportunity to respond to further questions arising from the hearing. Some of the Senator's questions go beyond my own personal level of technical knowledge, and I have obtained assistance from my more technical colleagues at CDT to develop my answers below. Before directly addressing the specific questions — which generally concern two patents obtained by Google regarding network-based location approximation — let me offer one caveat and one broad observation.

First, both from a legal and an engineering perspective, the task of interpreting the precise meaning of language in a patent is one best suited to those with specialized training in patent law, which neither I nor my colleagues at CDT have. We are sufficiently familiar with patent disputes, however, to know that many patents contain elements and assertions that are both expansive and defensive in nature, and may not in fact ever be included in an actual functioning implementation of the patented technology. We cannot speak to what elements of the patents at issue here have been implemented by Google or any other company.

Second, in considering the patents in question, it is important to recognize that from our analysis, the patents in question are focused almost exclusively at what are termed "layers 1 and 2" of the multi-layered technical architecture on which all Internet communications are based, while almost all true "user content"

P +1-202-637-9800 F +1-202-637-0968 E info@cdt.org

such as the content of e-mails or web-browsing sessions is transmitted at "layer 7" of the architecture. This can introduce significant confusion in that certain terms can refer to different things at different layers of the architecture, and the meaning of certain terms may depend heavily on the layer to which the term is referring.

To try to illustrate the overlapping nature of the layered architectural model, below is a simplified diagram that shows some (but not all) of the layers that might be implicated by the questions. What this diagram tries to illustrate is that in the layered model, the "payload" of some packets (which at layers 1 and 2 are sometimes called frames) will contain entire whole packets of information from a lower level protocol. Thus, as illustrated below, when sending an e-mail, the true "user content" of the e-mail (with the to/from routing information and the e-mail content) will be found in a layer 7 SMTP packet, which is entirely contained within a layer 3 "Internet Protocol" packet (which uses IP addresses for routing). And the IP packet is entirely contained in a layer 1 and 2 802.11 frame (which uses MAC addresses for routing):

<table>
<tr><td colspan="2">802.11 Frame (layers 1 and 2)</td></tr>
<tr><td>Routing and address info</td><td>MAC Address</td></tr>
<tr><td>Other fields</td><td>"Data rate," among others</td></tr>
<tr><td>Content payload</td><td>
<table>
<tr><td colspan="2">Internet Protocol Packet (layer 3)</td></tr>
<tr><td>Routing and address info</td><td>IP Address</td></tr>
<tr><td>Content payload</td><td>
<table>
<tr><td colspan="2">SMTP (e-mail) Packet (layer 7)</td></tr>
<tr><td>Routing and address info</td><td>joe@example.com</td></tr>
<tr><td>Content payload</td><td>E-mail content</td></tr>
</table>
</td></tr>
</table>
</td></tr>
</table>

This illustration may be helpful in understanding the patents at issue in the questions below and the ambiguity around the term "content" as regards the Google patents and WiFi interception issue.

QUESTIONS:

1. In your view, is there anything the wireless access point location approximation scheme described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 78 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," that <u>explicitly excludes</u> the

collection of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

We are interpreting the terms "content data" and "content of a user's internet communications over a wireless network" to refer to what I have called "user content" transmitted at layer 7 of the Internet architecture, meaning (in an e-mail example) the to/from e-mail addresses and e-mail text and attachments, or (in a web browsing example) the web address or URL and the web page content. With this understanding, our review of the patents at issue indicates that the patents are silent on the treatment or analysis of user content. The patents do not explicitly exclude the collection of user content, but at the same time the patents do not make any mention at all of user content (and the patents do not indicate any intention to analyze user content in order to determine location).

In the event that your definition of "content data" is intended to incorporate routing and addressing information that is contained in 802.11x frames (and higher layer routing and addressing information such as MAC addresses, SSIDs, and IP addresses), then the patents do seem to envision the collection and analysis of such routing information.

2. These patent applications contemplate examining "data frames" to determine the location of wireless access points as contemplated in these patent applications, looking at "the data in the frame … itself" to determine the data rates of frames that might contain content data, and contemplate sending "raw data collected" back to "a central repository … for processing." If Google actually engaged in any of these practices, would it be accurate to describe Google's interception and/or storage of content data through its Street View program as unintentional? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

We do not interpret the patents to contemplate "examining" any user content to make any determination of location, but instead to examine headers and data fields (such as the "data rate," which is a field found in some 802.11x frames) and use those non-content bits of information to calculate location. Our reading of the specific language quoted from paragraph 52 of the U.S. patent is that (a) it most likely refers to management or control frames, not data frames, but that (b) in any event, the information sought by looking at "data in the frame" would be found in lower-level header fields like "data rate" (and not in user content such as e-mails or web browsing sessions).

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

a. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

b. Indirectly valuable for any other purpose.

As noted more fully in response to Question 1, we interpret the terms "content data" and "contents of a user's internet communications over a wireless network" to refer to what I have called "user content" transmitted at layer 7 of the Internet architecture. With this understanding, then, we are unaware of any value, direct or indirect, that user content would have in efficiently locating wireless access points using commercially available methods. The user content of course has value to the end users (for example, the sender and recipient of an e-mail), but even if (for example) an e-mail contains a street address, a service provider seeking to locate access points would have no way of knowing whether the address related to the location of the access point in use.

In the event that the term "content data" is intended to incorporate routing and addressing information that is contained in both 802.11x frames and higher layers, such as MAC addresses, SSIDs, and IP addresses, then such routing and addressing information could be used to calculate approximate locations of access points, using methods suggested in the patents.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

   a. Legal or illegal under current federal law; or

   b. Legal or illegal under current state law.

   Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.

The legality under federal law of the reception by a device of wireless signals is a very complex technical and legal question turning on, among other things, the interpretation of provisions such as 18 U.S.C. § 2510(16), which define the category of radio communications which are "readily accessible to the general public," access to which is not a violation of federal law. This is one of the more confusing sections in the U.S. Code, and we are aware of no cases that apply these provisions to modern WiFi technologies.

Section 2510(16)(A) says that encrypted connections are not accessible to the public and thus protects encrypted wireless communications.
Section 2510(16)(C) protects public communication over certain types of subcarriers — signals carrying information as part of or associated with a larger signal. This provision may arguably protect certain WiFi technologies carried on subcarriers (802.11a, g, and n); on the other hand, because the subcarriers used

to transmit that information were not envisioned when the statute was written, they may be construed to fall outside the specific set covered by the statute as interpreted through FCC rulemaking. Section 2510(16)(E) also affords protections for public communications over certain frequencies, which seems to cover WiFi transmissions made on some common channels, but not others.

State law is more varied, and thus even more difficult to interpret with certainty.

Hopefully, this brief overview demonstrates that the status of the interception of personal wireless devices under the law is not at all clear, and the legality of a given interception can turn on specific technical questions regarding the choices made by the operators of individual WiFi hotspots, as well as the technical options in use by the WiFi equipment in question.

Separately, it is important note that for *any* wireless system to work, all devices seeking to communicate on a given frequency (whether or not those devices are the intended recipient of a communication) must in a sense "listen" to at least a portion of all communications on the frequency in order to determine whether the communication is intended for the particular device. Before interpreting certain kinds of routing and signaling information contained within a given communication, there is no way for a receiver to understand that a given packet is aimed elsewhere. Thus, to the extent that the term "content data" is intended to incorporate routing information that is contained in 802.11x frames (such as MAC addresses), devices must as a technical matter be permitted to receive such information in order for the wireless system to function.

The uncertainty of the law's application in this context is yet another illustration of why the Electronic Communications Privacy Act (ECPA) and other surveillance laws need to be updated to provide clear protection to electronic communications technologies and services that have evolved substantially in recent years. CDT is a member of the Digital Due Process coalition, which has offered a few narrow recommendations for updating ECPA.

* * *

We hope that our answers have been helpful. We appreciate the opportunity to further discuss the issues raised in the hearing, and we look forward to working with the Committee on these important issues.

Sincerely,

/s/

Justin Brookman
Director, Consumer Privacy
Center for Democracy & Technology

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

Questions for the record from Senator Blumenthal
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

Google appreciates the opportunity to respond to the Committee's further questions arising from Google's testimony concerning the steps it takes to protect mobile privacy with its Android operating system and in regard to the prior collection of publicly broadcast Wi-Fi information through Google's Street View cars. Before responding to the questions, one point of clarification is necessary. Each question includes as a predicate the "interception" of wireless data transmissions between third party computers and wireless access points. As the Committee knows, the term "intercept" has legal meaning under Sections 2510 and 2511 of Title 18. Accordingly, as a general response, the answer to all of the questions is that Google does not engage in the unauthorized interception of the content of communications. Nonetheless, we provide this response in a good faith effort to provide the Committee with useful information about Google's activities in regard to Wi-Fi.

1. **Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points <u>for any purpose</u>?**

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise.

To the extent Senator Blumenthal's questions follow up on the questions he raised at the hearing concerning the Wi-Fi payload data collected via Google's Street View cars, Google has publicly explained what happened, including what information was collected and how, on our blog (http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html and http://googlepublicpolicy.blogspot.com/2010/10/creating-stronger-privacy-controls.html).

Further, the Committee has also expressed interest in the collection of location data by devices running the Android operating system. While also not involving any unauthorized interception of data transmissions between third party computers and wireless access points, Google, like many other companies, has developed systems for identifying wireless access points to provide better location-based services. Although a substantial amount of the information relating to these systems is non-public and proprietary, we have described how these systems work in our testimony.

If so:

a. Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from the interception of wireless data transmissions described above.

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise, whether in the United States or abroad. To the extent that the Committee has interest in Google's other location-based services described in our testimony, Google operates location-based services in many countries around the world, including all states and territories of the United States.

b. Please indicate any and all purpose(s) underlying any such signal interceptions.

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise, whether in the United States or abroad, for any purpose. Like many other companies, Google does receive and collect information regarding wireless access points and other publicly broadcast geographic markers. The purpose of doing so is to offer location-based services.

c. Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. Location-based services have been an important part of Google's research and development for many years. We do not have a timeline for each product or service, but can say in regard to the collection of publicly broadcast Wi-Fi information via Street View, Google first began its collection of such information for purposes of providing location based services in 2008 and discontinued the activity in May 2010.

d. Please describe any and all methods <u>initially contemplated and/or implemented</u> for these purposes.

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. With regard to Google's collection of publicly broadcast Wi-Fi information via Street View vehicles, we direct you to the report prepared by independent technical services firm Stroz Friedberg LLC, which describes in detail the methods used and the type of information collected (the "Stroz Report"). See http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html. In regard to the

Android operating system, a substantial amount of the information relating to the system is non-public and proprietary, but we point the Committee to our testimony, which describes our practices and methods in that regard.

e. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

See our response to Question 1(d).

f. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. The question also implies that Wi-Fi signaling information is susceptible to "interception." Google understands the term interception to refer to the content of communications. Every Wi-Fi enabled radio publicly broadcasts, and every Wi-Fi enabled device receives, Wi-Fi frame transmissions in accordance with the 802.11 standard. Google's ability to provide location-based services, like any company providing location-based services, depends upon receiving publicly broadcast Wi-Fi data such as MAC addresses, SSID, signal strength, time stamps, etc. A number of Google products and services include Wi-Fi enabled features. Information collected and how it is used may be found in Google's Mobile Privacy Policy at http://www.google.com/mobile/privacy.html as well as product specific policies for Maps, Latitude, and our other location-based services.

g. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. Google has no patents, patent applications, published works or other publicly available materials that describe the unauthorized interception of wireless communications traveling between third party computers and wireless access points. While not involving the unauthorized interception of the content of communications, to the extent the Committee is interested in the specific patent discussed the the hearing, we point the Committee to our answers to the supplemental questions for the record below.

h. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data"

transmitted between third party users and wireless access points? If so, please explain how and why such content data is excluded from interception. If not, please explain how and why such content data is not excluded from interception. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See response to 1.D. As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. With regard to Google's collection of publicly broadcast Wi-Fi information via Street View vehicles, we direct you to the report prepared by independent technical services firm Stroz Friedberg LLC, which describes in detail the methods used and the type of information collected (the "Stroz Report"). See http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html.

i. **Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized.** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. As we have said before with respect the collection of publicly broadcast Wi-Fi information via Street View vehicles, Google did not use payload data in any product or service.

j. **Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.**

No.

k. **Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?**

No.

2. **Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.**

a. **How many wireless access points exist, or have ever existed, in any database of wireless access point locations?**

i. **How many of these wireless access points were unencrypted when identified?**

ii. **How many of these wireless access points were encrypted when identified?**

iii. **How many of these wireless access points were "hidden" when identified?**

Location-based services depend in part on the ability to identify Wi-Fi access points. Such information is publicly broadcast in accordance with the 802.11 standard, involves no interception of wireless data communications, and therefore Questions 1.a-h are inapplicable. The total numbers of access points used for our location-based services is non-public, proprietary information, and Google does not publish a directory of such information.

3. **Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:**

   a. **Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and**

   b. **Indirectly valuable to your company for any other purpose.**

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. To the extent the question contemplates the payload data collected by Google via its Street View vehicles, Google has not used the payload data collected by Street View vehicles in any product or service. That information has no use or value, directly or indirectly, to Google for any purpose, and never did.

4. **Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:**

   a. **Legal or illegal under current federal law;**

   b. **Legal or illegal under current state law; and**

   c. **Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

Google directs the Committee to Section 2511(2)(g) of Title 18, which states "[i]t shall not be unlawful . . . for any person (1) to intercept or access an electronic communication made

through an electronic communication system that is configured so that such electronic communication is readily accessible to the general public." Wi-Fi transmissions broadcast from unencrypted networks are readily accessible to the general public by definition.

Most states follow federal law and any inconsistent state law would yield to federal law under the Supremacy Clause of the U.S. Constitution. Many foreign jurisdictions follow the same principles or their laws have not addressed the situation.

Supplemental Questions for the Record to Alan Davidson, Google, Inc.

Google appreciates the opportunity to respond to the Committee's further requests and in particular to Senator Blumenthal's followup questions below. First, several of the questions include as a predicate that patents exist for the purpose of "interception" of wireless data transmissions. As the Committee knows, the term "intercept" has legal meaning under Section 2510 and 2511 of Title 18. Accordingly, as a general response, the answer to all of the questions is that Google does not engage in the unauthorized interception of content of communications, and Google has no patents or applications pending that describe the "interception" of wireless communications traveling between third party computers and wireless access points. Also, the questions could be read to require the disclosure of non-public proprietary information. Nonetheless, in a good faith effort to answer the Committee's questions, Google provides the following responses.

1. **Please provide text and citations for any and all materials <u>directly or indirectly associated with or related to</u> the methods for intercepting wireless data transmissions traveling between third party computers and wireless access points described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" (including foreign or domestic patents, patent applications, published works, or other publicly available materials).**

As noted above, the term "intercept" has legal meaning, and unequivocally, Google does not engage in the unauthorized interception of the content of communication transmitted over wireless networks or otherwise. It has no patents or applications pending that describe the "interception" of wireless communications traveling between third party computers and wireless access points. The patent application referenced in the Question describes a method for approximating the location of a wireless device. The patent application is concerned with measuring the data rates of publicly broadcast Wi-Fi frames. The measurement of data rates does not involve the use of the content of any communications.

2. **Please indicate where in the scheme described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" these patents <u>explicitly exclude</u> the interception of content data.** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See Response to Question 1, which is incorporated herein. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with

establishing confidence in the location of an access point, and therefore there is no reason to disclaim it.

3. **Wireless signal interception as described in Paragraph 51 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 47 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation" involves configuring a Google computer "to observe or capture data packets .. transmitted to or from" a wireless access point, with the Google computer "operat[ing] in a 'sniffer' or 'monitor' mode, thereby handling transmitted frames ... without requiring" the Google computer "to be associated with" the wireless access point. This scheme appears to contemplate 'sniffing' (i.e., intercepting and decoding) all transmitted frames.**

   a. **Where does this patent distinguish between 'sniffing' or 'monitoring' frames containing content data and 'sniffing' or monitoring frames that did not contain content data?** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

See Response to Questions 1 and 2. Every Wi-Fi enabled radio publicly broadcasts, and every Wi-Fi enabled device receives, Wi-Fi frame transmissions in accordance with the 802.11 standard. Google's ability to provide location-based services, like any company providing location-based services, depends upon receiving publicly broadcast Wi-Fi data such as MAC addresses, SSID, signal strength, time stamps, etc. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with establishing confidence in the location of an access point.

   b. **Was there ever a version of Google's Street View programming designed to intercept and decode all of the information received from a wireless access point and then subsequently discard unwanted data?**

No. We direct you to the report prepared by an independent technical services firm, Stroz Friedberg LLC, which describes in detail the describes in detail how the Wi-Fi equipment and software operated, the frequencies and protocols covered, and type of information collected ("the Stroz Friedberg Report"). See http://googleblog.blogspot.com/2010/05/wifi-data-collection-update.html. As noted in the Stroz Friedberg Report, the software was designed to recognize encrypted networks and never to store payload data from those networks.

   c. **Was there ever a version of Google's Street View programming that distinguished between frames containing content data and frames that did not contain content data?** *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

No.

   d. **Was there ever a version of the software on Google's Street View cars that specifically deleted, blanked, or removed intercepted IP payload data?**

No.

e. Did the software addition that Google points to as responsible for collecting "payload data" affirmatively intercept and decode content, or did it remove a preexisting block on decoding content?

No, the software did not decode content at all. See the Stroz Friedberg Report referenced above for information on how the software operated.

4. Does the term "data rate" as used in these patent applications consistently refer to information about the communication with the access point such as "data rate" as defined by 802.11 standards, or does it refer to a "measured" data rate?

The "data rate" is a property of the transmission, as defined by 802.11 standards.

5. Paragraphs 70-71 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraphs 66-67 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discuss 'evaluating different types of frames sent to (or received from) the device of interest" including "management frames, control frames, data frames, etc." as part of a scheme to estimate "the confidence of the location" of a wireless access point.

a. Please explain what types of evaluations are contemplated for each of the three types of frames listed.

Each of the frames types are sent at specific data rates. The receiving device driver obtains and appends the data rate to each frame that was sent to, or received from, an access point. The data rate is extracted from the various frames for evaluation by means of a mechanical, automated process.

b. How does evaluation of data frames contemplated in these paragraphs affect Google's estimate of the confidence of the location of a wireless access point?

As described in the patent application, it is assumed that data rate, like signal strength, can be used to estimate "distance." Thus, given the expected location of an access point and the GPS location of where a frame is captured plus the data rate, Google could determine how probable it is to receive a frame at the given data rate and at a given distance from the access point to the location where the frame was captured.

Data frames are sent at different data rates (unlike management/control frames which are sent at fixed data rates). For example, the higher the data rate, the shorter the distance at which it can be received. These assumptions could help build or reduce confidence in an access point's estimated location.

6. Paragraphs 74-75 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraphs 70-71 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discuss determining "the confidence in the location" of a wireless access point, and note that "the types of frames that are used in the

measurement, such as data frames, management frames, and/or control frames may affect the confidence."

a. How do these patents contemplate evaluating these three types of frames in order to improve the confidence estimate for the location of the wireless access point?

See Response to Question 5(b).

b. How does evaluation of data frames contemplated in these paragraphs affect Google's estimate of the confidence of the location of a wireless access point?

See Response to Question 5(b).

7. Paragraph 82 of U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 78 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," discusses how "[T]he location of a given [wireless access point] may be based on a number of measurements taken by one or more client devices. <u>The raw data collected</u> by a client device may be processed locally <u>or sent to a central repository ... for processing</u>" (emphasis added).

a. Do these patent applications specifically exclude the collection of raw data that includes "content data" before sending it to a central repository for processing? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

The sentence cited in the Question simply states the proposition that the publicly broadcast Wi-Fi frames received may be processed locally or in storage. The patent application is concerned with measuring the data rates of publicly broadcast Wi-Fi frames. Content data is irrelevant to the patent process described in the application and has nothing whatsoever to do with establishing confidence in the location of an access point. Thus, where the frames are processed is irrelevant as well.

b. Is there any relation between the scheme described in Paragraph 82 and the operation of the Google Street View cars during the period when those cars were used to identify the locations of wireless access points?

The quotation from Paragraph 82 referenced in the question simply states that data may be analyzed locally or later in a central data store. The same is true for any data collection and analysis. In the case of Wi-Fi data collected via Street View vehicles, the data was stored in Google's File Servers.

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

Questions for the record from Dr. Coburn
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

1. **Google has stated it does not sell users' personally identifiable information to third parties. However, Google operates advertising services that are connected to mobile devices using its Android platform. Could you comment on how Google operates its ad services, particularly whether Google sends targeted ads to mobile device users, and if so, what user information Google collects in order to send targeted ads?**

Advertisers may use Google's advertising services to run mobile advertising campaigns based on several factors. Those factors can include platform, device, geography, or demographic information.

To protect user privacy, Google adheres to the following principles when offering its advertising services and targeting options:

- **Transparency** – We provide detailed information about our advertising policies and practices (see our general Google privacy policy and the AdMob privacy policy).
- **Choice** – We offer innovative ways to view, manage and opt out of targeted advertising.
- **No personally identifying information** – We do not collect or serve ads based on personally identifying information without the user's permission.

Recently, we extended our online advertising transparency and choice approach to our mobile application ad networks. For these ad systems, we have created a user-friendly solution involving anonymization, user control, and user notice. First, Google performs a one-way, non-reversible cryptographic hash of a device identifier which we then associate with an anonymous ID specifically for ad serving. Second, for both Android and iPhone users we give consumers an easy way to opt out the use of their device identifier by Google's advertising services altogether. Third, we are notifying all users of how we customize ads and their opt-out controls with clear notice. Because the mobile application interfaces are more limited, we chose to show a full-size privacy notice that was rotated along with other advertisements, rather than use an icon, which is hard to see or click on the smaller mobile screen.

a. Is advertising the largest source of revenue for Google? If not, what services or products contribute most to Google's bottom line?

Yes.

b. Are there any apps to which Google refuses to provide advertising services? If so, what are the primary reasons for refusing such services? If not, why?

Developers of mobile applications that use Google's advertising service (known as AdMob or AdSense for Mobile Apps) must agree to either AdMob's Terms of Use (http://www.admob.com/home/terms) and Publisher Guidelines and Policies (http://helpcenter.admob.com/content/content-guidelines), or AdSense's Terms of Use (https://www.google.com/adsense/localized-terms) and Publisher Guidelines and Policies (https://www.google.com/adsense/support/bin/answer.py?answer=48182).

If Google determines that a developer is in violation of these terms or policies, Google may take enforcement action. Depending on the severity of the violation, the enforcement action may take the form of a warning, suspension, or permanent termination.

c. Are there any apps Google refuses to host on the Android app store? If so, what are the primary reasons for refusing to provide those apps, and how often, on average, does Google reject an app or later remove it from your store for questionable behavior?

Google may suspend an application from future availability on Android Market if Google discovers that an application violates the Android Market developer agreement (http://www.android.com/us/developer-distribution-agreement.html) or policies (http://www.android.com/us/developer-content-policy.html). In addition to suspending an application, Google may also permanently disable the account of a developer for repeated or egregious violations of the Android Market developer agreement or policies.

Android Market is built on the principle of openness, with the goal of encouraging innovation and user choice. With this principle in mind, Google does not pre-screen applications before they are made available by developers to users of Android Market. But we will remove applications when we are notified about or otherwise discover applications that violate our developer agreement or policies. As of May 31, 2011, Google is removing an average of 250-300 applications per day from Android Market due to violations of our developer agreement or policies.

d. How many employees and/or automated services are dedicated to crawling your app store to weed out apps that inappropriately use consumers' personal information or violate your respective privacy policies?

We have a team of employees dedicated to responding to complaints and information we receive about applications in the Android Market to determine if the applications comply with our developer agreement and policies, but not specifically related to inappropriate use

of personal information. The size of this team is growing and will be adjusted as needed. Separately, we have recently implemented tools that automatically examine the code of Android Market applications for signs of potential malware.

More broadly, Google does not control the behavior of third party applications or how they handle location information and other user information that the third party application obtains from the device. Instead, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access during the application installation process. This permissions model is designed to empower users to make their own decisions about whether or not to trust an application with the information requested. The user may choose to trust the application by completing the installation or the user may choose to cancel the installation.

The application developer bears the responsibility for the design of the application, which includes responsibility for how the application collects and handles user data and the privacy disclosures made to users. Even though the developer bears the responsibility, Google strongly encourages application developers to use best practices, as described in this Google blog post: http://android-developers.blogspot.com/2010/08/best-practices-for-handling-android.html.

Furthermore, developers that upload applications to Android Market must agree to the Android Market developer agreement (http://www.android.com/us/developer-distribution-agreement.html), pursuant to which developers agree to comply with applicable laws and to protect the privacy rights of users.

The specific relevant language is as follows:

> 4.2 You agree to use the Market only for purposes that are permitted by (a) this Agreement and (b) any applicable law, regulation or generally accepted practices or guidelines in the relevant jurisdictions (including any laws regarding the export of data or software to and from the United States or other relevant countries).
>
> 4.3 You agree that if you use the Market to distribute Products, you will protect the privacy and legal rights of users. If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users. Further, your Product may only use that information for the limited purposes for which the user has given you permission to do so. If your Product stores personal or sensitive information provided by users, it must do so securely and only for as long as it is needed. But if the user has opted into a separate agreement with you that allows you or your Product to store or use personal or sensitive information directly related to your Product (not including other products or applications) then the terms of that separate agreement will govern your use of such information. If the user provides your Product with Google Account information, your Product may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given you permission to do so.

e. In other contexts, such as the sale of counterfeit pharmaceuticals online, there has been a recent push in the industry (with the suggestion of the Intellectual Property Enforcement Coordinator) to form a working group in order for the industry to take the lead on how to combat the dangerous use of these products online. Is there any such industry working group to address the unique issues surrounding mobile device products and/or location based services?

There are numerous industry groups that address issues surrounding mobile device products and location based services. For example, CTIA - The Wireless Association publishes Best Practices and Guidelines for Location Based Services, available at: http://www.ctia.org/business_resources/wic/index.cfm/AID/11300. The Guidelines state that they are intended to promote and protect user privacy as new Location-Based Services ("LBS") are developed and deployed. As CTIA explains it, "Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.)." Google supported the development of these guidelines.

Google also is a member of the Mobile Marketing Association, which represents more than 700 member companies globally. Its mission is to provide education, measurement and guidance to the mobile marketing industry worldwide. MMA has a standing committee on privacy and data security.

The Digital Advertising Alliance, composed of the bulk of the online advertising and publishing industry, has issued guidelines for online behavioral advertising. They are working now to extend these guidelines into the mobile advertising area.

There are many other organizations and industry working groups that focus on particular aspects of the mobile industry and mobile devices.

Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"

Questions for the record from Senator Franken
Alan Davidson, Director of Public Policy, Google Inc.
June 8, 2011

1. **Will Google commit to requiring that all apps in the Android Market have a clear, understandable privacy policy?**

Google agrees that application developers that collect personal data from the users of their applications should offer clear notice of their practices, including via a privacy policy. Our Android Market developer agreement (http://www.android.com/us/developer-distribution-agreement.html) requires app developers to protect their users' privacy:

> 4.3 **You agree that if you use the Market to distribute Products, you will protect the privacy and legal rights of users.** If the users provide you with, or your Product accesses or uses, user names, passwords, or other login information or personal information, **you must make the users aware that the information will be available to your Product, and you must provide legally adequate privacy notice and protection for those users.** Further, your Product may only use that information for the limited purposes for which the user has given you permission to do so. If your Product stores personal or sensitive information provided by users, it must do so securely and only for as long as it is needed. . . .

(Emphasis added.)

Beyond privacy policies, we have also strongly encouraged developers to use best practices in the design of their applications as described in this Google blog post: http://android-developers.blogspot.com/2010/08/best-practices-for-handling-android.html.

Like the Federal Trade Commission and many others, we do not view privacy policies as the sole or even best way to provide clear notice of privacy practices. Unless a privacy policy is mandated by law, therefore, we have not *required* such a policy in order to satisfy the requirements of our developer agreement quoted above. We continue to evaluate this policy, and may revise it as needed to best protect the rights of Android users.

2. **If not, will Google at least commit to require that all location-aware apps in the Android market have a clear, understandable privacy policy?**

Please see the response to Question 1, above.

With respect to location information specifically, the Android operating system uses a permissions model in which the user is automatically informed of certain types of information an application will be able to access during the application installation process. The permissions model informs the user if an application will have access to the user's location information. An application can access the device's GPS location through a permission, which will display the permission message "Your location: fine (GPS) location" to the user during installation. An application can access the device's network location through a permission, which will display the permission message "Your location: coarse (network-based) location" to the user during installation.

3. **Will Google commit to informing users through a clear, conspicuous method, i.e. a permission screen, that the apps they download have the technical ability to share or disclose the information they gather from the user to third parties?**

As described above, we believe the permissions model provides clear, conspicuous notice to users about certain information that can be accessed by an application. An application can only send information off the device if it obtains Internet access. For an application to obtain Internet access, the user must grant a permission. Specifically, the user would see a permission message displayed saying: "Network communication: full Internet access" during installation.

The Android permissions model is designed to give users actionable information to help them decide whether to proceed with an application installation. The small size of a mobile device screen requires a delicate balance to determine the most useful quantity of information to present to the user. The downside of too little information is clear, but presenting too much information (especially if that additional information sounds like a legal disclaimer) could cause users to ignore the permission screen and defeat the goal of having better informed users.

One example of how we have recently adjusted this balance is demonstrated by our decision to show a longer permission description when a user installs an application from the web interface of Android Market (http://market.android.com) versus the on-device installation process. Users have the ability to browse applications on the large screen of their desktop or laptop computer through this website and push an installation of the application to their mobile device.

For example, the Android operating system will display a permission if an application wishes to access the device's GPS location. If the application installation is initiated from Android Market on the mobile device, the permission displayed on the phone says:

> Your location: fine (GPS) location

This is a concise description appropriate for the small mobile device screen. If the application installation is initiated from Android Market through the web interface, the permission displayed on the website says:

> YOUR LOCATION: FINE (GPS) LOCATION—Access fine location sources such as the Global Positioning System on the device, where available. Malicious applications can use this to determine where you are, and may consume additional battery power.

This is a more detailed description that takes advantage of the larger screen.

We will continue to consider ways to improve messaging to users, including with respect to this particular issue.

4. **Do you think that most users understand the terms used in your app permission screen? For example, if an app can have access to your "network connections", do you think the average user knows what that means? What can you do to make your permission screen more clear for average users without deep technical knowledge or sophistication?**

Please see our answer to Question #3 above. We have done our best to strike balances in our permissions model to make it understandable and useful in a way that benefits the maximum number users. We will continue to consider ways to improve the existing permission model.

5. **Android OS devices transmit a unique identifier along with the location data that they transmit to Google servers.** *See* **Jennifer Valentino-Davies, "The Unique ID Android Uses in Collecting Location,"** *The Wall Street Journal*, **April 26, 2011. Apple succeeds in collecting this information without such an identifier. Will Google refrain from using such identifier in future data collection?**

We believe this identifier (which we refer to as an "anonymous token") serves an important functional purpose, and have designed our systems in a way to protect user privacy.

The Google Network Location Provider application for Android (or NLP) is a proprietary Google application that may be installed on Android devices by a device manufacturer pursuant to a license with Google. NLP interacts with the Google Location Server (or GLS) to determine a user's estimated location using Wi-Fi access points and cell towers, providing location information in a way that works indoors and outdoors, responds faster, and uses less battery power than GPS services.

With the opt-in consent of the user, NLP transmits certain location information to Google servers in association with an anonymous token randomly generated by GLS. A new token will be generated by GLS if the user performs a factory reset of the device. This token is only used to tag communications between NLP and GLS, which enables Google to compute velocity for road traffic estimates and to identify invalid transmissions to GLS. Google wants only legitimate devices to provide information, because invalid transmissions have the potential to pollute the GLS database with inaccurate data and degrade the ability of GLS to provide reliable location information to future users.

The collected information is stored in temporary databases on Google servers for approximately one week in association with a hashed version of the anonymous token. The token is put through a one-way hash as soon as it arrives at the server. The token itself is never stored on a Google server, only a hash of the token is temporarily stored in which the hash key is rotated at least every seven days. After this approximately one week of temporary storage, the information related to the hashed token values is stripped from the data and measures are taken to obfuscate GPS route endpoints. The remaining data is transferred into aggregate and anonymous databases on Google servers for permanent

storage, consisting of a database of Wi-Fi access point and cell tower locations and a database of road traffic information.

The design choice to use this anonymous token (rather than some other identifier) helps ensure that the information cannot be traced back to a particular device or particular user. Additional practices such as only storing a hashed version of the anonymous token, rotating the hash key, stripping the hashed token values, and taking measures to obfuscate GPS route endpoints are additional security measures instituted to further anonymize this information. Access by Google employees to the temporary and permanent databases is subject to access restriction policies and processes.

6. **Under what circumstances does Google consider location information obtained from a user's device to be non-content customer records data subject to the voluntary disclosure permission in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(c)(6)?**

Without commenting on the specific legal question, we note that the location information sent to Google servers when users opt in to location services on Android devices is anonymized and stored in the aggregate and is not tied or traceable to a specific user. Therefore, Google cannot identify a particular user from the location information stored in our location servers and cannot produce information about a particular user.

7. **Since Google gets the vast majority of its revenue from advertising, it seems like your incentive to protect privacy might be in conflict with your incentive to collect your user's information. What relationship does AdMob have to the Android Operating System and applications in the Android App Market?**

The Android operating system and Android Market are part of one business unit, while AdMob is part of a separate unit. The AdMob product is not part of the Android operating system.

We note that offering free, advertising-supported services is not inherently in conflict with strong incentives to protect privacy. Many long-standing industries are advertising-supported, including broadcast television and newspapers, yet these businesses have little history of mistreatment of user privacy. Like providers of those services, our users are our lifeblood—without their trust and engagement, we would not have an audience to which to show ads.

Moreover, all businesses, regardless of their profit model, have an incentive to sell customer data—indeed, this path is followed by countless merchants, grocery chains, and even government agencies. Yet Google does not; we never sell our users' personally-identifiable information, or share it without their express consent.

Instead, we follow the axiom of "focus on the user and all else will follow." This applies to every aspect of our business, including our treatment of personal information. As our testimony explains, Google would simply go out of business if we lost the trust of our users. This is reflected foremost in our privacy principles, which are located and available to the public at www.google.com/corporate/privacy_principles.html. Our commitment to these principles is reflected in our industry-leading privacy practices and tools, including our Ads Preferences Manager (http://www.google.com/ads/preferences/).

SEN. BLUMENTHAL QFRs FOR ASHKAN SOLTANI

1. In your view, is there anything the wireless access point location approximation scheme described in U.S. Patent Application 2010/0020776, "Wireless Network-Based Location Approximation," and Paragraph 78 of WIPO Patent Application WO 2010/044872, "Wireless Network-Based Location Approximation," that explicitly excludes the collection of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

   On quick review, there is nothing explicitly excluding "content data" in this patent. In fact, the full data frame is received and processed in order to ascertain data speeds and signal quality.

2. These patent applications contemplate examining "data frames" to determine the location of wireless access points as contemplated in these patent applications, looking at "the data in the frame … itself" to determine the data rates of frames that might contain content data, and contemplate sending "raw data collected" back to "a central repository … for processing." If Google actually engaged in any of these practices, would it be accurate to describe Google's interception and/or storage of content data through its Street View program as unintentional? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

   Content data, as described above, would be present in the data frames. If full data frames are collected and sent back to a central repository, then it's possible that these would include content data. However, the patent doesn't specify exactly what is meant by "raw data".

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:
   a. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

   Content data, as described above, *may* contain information that reveals specifics as to the hardware and configuration settings of the Wireless Access Points that generate the WiFi signal. This information could conceivably be used to improve the ability to geo-locate clients although this isn't mentioned directly in the patent.

   b. Indirectly valuable for any other purpose.

   It's difficult to speculate on all of the ways content data could be useful. Presumabl wiretap would likely prohibit most of these valuable uses however.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:
    a. Legal or illegal under current federal law; or
    b. Legal or illegal under current state law.

    Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.

    I'd prefer to not speculate on the legality of this practice, as I'm not a lawyer.

Senate Judiciary Subcommittee on Privacy, Technology and the Law
Hearing on
Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phone and Your Privacy
May 10, 2011

1. **Senator Tom Coburn, M.D., Ranking Member of the Subcommittee for Privacy, Technology and the Law, asked Ms. Jessica Rich, Deputy Director, Bureau of Consumer Protection, Federal Trade Commission ("FTC" or "the Commission"), to indicate whether the FTC currently has the legal authority to implement the privacy protections set forth in the FTC's preliminary staff report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* ("FTC Staff Report").[1]**

Section 5 of the Federal Trade Commission Act ("FTC Act") empowers the Commission to take action against deceptive or unfair acts or practices in or affecting commerce.[2] In addition to this broad authority, the FTC enforces a number of sector-specific statutes, including the Gramm-Leach-Bliley Act ("GLB Act"), the Children's Online Privacy Protection Act ("COPPA"), the CAN-SPAM Act, and the Telemarketing and Consumer Fraud and Abuse Prevention Act (and the Do Not Call Rule).[3] The FTC has used Section 5 as well as these other laws to challenge a wide variety of practices that affect consumer privacy.

Over the years, many of the Commission's privacy cases – including actions against well-known companies such as Microsoft, ChoicePoint, and TJX – have involved practices that include the alleged failure to: (1) comply with posted privacy policies;[4] (2) take appropriate steps

---

[1] *See* FTC Preliminary Staff Report, *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (Dec. 1, 2010), *available at* www.ftc.gov/os/2010/12/101201privacyreport.pdf.

[2] 15 U.S.C. § 45.

[3] *See* GLB Act, 15 U.S.C. §§ 6801-6809 (2010) (consumer financial data); COPPA, 15 U.S.C. §§ 6501-6506 (2010) (information about children); CAN-SPAM Act, 15 U.S.C. §§ 7701-7713 (2010) (unsolicited electronic messages); Telemarketing and Consumer Fraud and Abuse Prevention Act, 15 U.S.C. §§ 6101-6108 (2010) (under which the Do Not Call Rule, 16 C.F.R. § 310.4, was promulgated).

[4] *See, e.g.*, *In re Premier Capital Lending, Inc.*, No. C-4241, 2008 WL 5266769 (F.T.C. Dec. 10, 2008) (consent order); *In re Life Is Good, Inc.*, No. C-4218, 2008 WL 1839971 (F.T.C. Apr. 16, 2008) (consent order); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005); *MTS, Inc.*, 137 F.T.C. 444 (2004) (consent order); *In re Microsoft Corp.*, 134 F.T.C. 709 (2002) (consent order).

to protect against common vulnerabilities;[5] (3) dispose of data properly;[6] and (4) take reasonable steps to ensure that customer data is not shared with unauthorized third parties.[7]

More recently, the Commission has focused on the privacy implications of emerging technologies that permit new ways of collecting and using consumer data. For example, in a complaint against the retailer Sears, the Commission claimed that the company had violated Section 5 by deceiving consumers about a tracking capability it deployed to collect detailed information about users' online activities.[8] Additionally, the Commission has challenged the collection and use of consumer data by interactive media services. In a complaint against the social media service Twitter, the FTC alleged that the company had deceived customers by offering them an opportunity to designate certain "tweets" as private and then failing to honor their choices.[9] The Commission also brought an action against Playdom, an operator of "virtual world" websites that hosted online games, alleging that it violated COPPA by collecting personal information from children under the age of 13 without obtaining verifiable parental consent.[10] Finally, in March of this year, the Commission announced proposed settlements with Chitika, an online advertising company that allegedly made deceptive claims regarding

---

[5] *See, e.g.*, *In re TJX Cos.*, No. C-4227, 2008 WL 3150421 (F.T.C. July 29, 2008) (consent order); *In re Guidance Software, Inc.*, No. C-4187, 2007 WL 1183340 (F.T.C. Mar. 30, 2007) (consent order); *In re Petco Animal Supplies, Inc.*, 139 F.T.C. 102 (2005) (consent order); *In re Guess?, Inc.*, 136 F.T.C. 507 (2003) (consent order).

[6] *See, e.g.*, *FTC v. Navone*, No. 2:08-CV-001842 (D. Nev. Dec. 30, 2008), http://www.ftc.gov/os/caselist/0723067/100120navonestip.pdf (consent order); *United States v. Am. United Mortg. Co.*, No. 1:07-CV-07064 (N.D. Ill. Dec. 18, 2007), http://www.ftc.gov/os/caselist/0623103/071217americanunitedmrtgstipfinal.pdf (consent order);
In re CVS Caremark Corp., No. C-4259, 2009 WL 1892185 (F.T.C. June 18, 2009) (consent order).

[7] *See, e.g.*, *United States v. Rental Research Serv.*, No. 09 CV 524 (D. Minn. Mar. 5, 2009), www.ftc.gov/os/caselist/0723228/090305rrsorder.pdf (consent order); *United States v. ChoicePoint, Inc.*, No. 1:06-CV-0198 (N.D. Ga. Feb. 15, 2006), www.ftc.gov/os/caselist/choicepoint/stipfinaljudgement.pdf (consent order).

[8] *See In re Sears Holdings Mgmt. Corp.*, No. C-4264 (Aug. 31, 2009), www.ftc.gov/os/caselist/0823099/090604searsdo.pdf (consent order).

[9] *See In re Twitter, Inc.*, FTC Docket No. C-4316 (Mar. 2, 2011) (consent order), *available at* www.ftc.gov/opa/2011/03/twitter.shtm.

[10] *See United States v. Playdom, Inc.*, No. SACV II-00724 (C.D. Cal. May 11, 2011) (proposed consent order), *available at* www.ftc.gov/opa/2011/05/playdom.shtm.

consumers' ability to opt out of tracking,[11] and Google, for allegedly violating its privacy promises in connection with the launch of its "Google Buzz" social network.[12]

The proposed privacy framework set forth in the FTC Staff Report includes three major recommendations for protecting consumer privacy. First, companies should adopt "privacy by design" by promoting consumer privacy throughout their organizations and should build privacy into their products and services at every stage of development. Second, companies should simplify consumer choice by offering necessary choices at a time, and in a context, that makes the choice meaningful to consumers. Third, companies should increase the transparency of their data practices by improving notices, offering reasonable access to the data they maintain,[13] obtaining affirmative express consent for material, retroactive changes to their privacy promises,[14] and expanding efforts to educate consumers about data practices.

The framework provides recommended best practices for addressing the privacy challenges that new technologies, practices, and business models dependent on consumer data raise, but it is not a document for enforcement. In issuing the FTC Staff Report and calling for public comment on the proposed privacy framework, the Commission has not taken a position on whether privacy legislation is currently needed. The Commission will continue to use its authority under Section 5 and through the sector-specific statutes it enforces to bring law enforcement actions against companies that engage in illegal practices that harm consumer privacy interests. To the extent that Congress decides that legislation is appropriate, the Commission believes that the recommendations and guidance contained in the FTC Staff Report can serve as a valuable resource for law makers.

---

[11] *See In re Chitika, Inc.*, FTC File No. 102 3087 (Mar. 14, 2011) (proposed consent order), *available at* www.ftc.gov/opa/2011/03/chitika.shtm.

[12] *See Google, Inc.*, FTC File No. 102 3136 (Mar. 30, 2011) (proposed consent order), *available at* www.ftc.gov/opa/2011/03/google.shtm.

[13] The Commission has brought a number of cases against companies for failing to take reasonable steps to ensure the security of consumer data. In addition, the FTC enforces specific data security laws and rules involving certain entities or practices. The FTC's Safeguards Rule promulgated under the GLB Act provides data security requirements for most nondepository financial institutions. *See* 16 C.F.R. § 314 (implementing 15 U.S.C. § 6801(b)). The FCRA requires consumer reporting agencies to use reasonable procedures to ensure that the entities to which they disclose sensitive consumer information have a permissible purpose for receiving that information, and imposes safe disposal obligations on entities that maintain consumer report information. *See* 15 U.S.C. §§ 1681e, 1681w.

[14] The Commission has brought cases against companies for unilaterally changing their data practices and using previously collected data in ways that materially contradict claims made to consumers at the time of collection. *See, e.g.*, *Gateway Learning Corp.*, No. C-4120, 2004 WL 2618647 (F.T.C. Sept. 10, 2004).

Apple's Responses to Senator Al Franken's May 18, 2011 Questions

1. Will Apple commit to requiring that all apps in the Apple App Store have a clear, understandable privacy policy?

Response:

For Apple's response to this question, please see the attached June 1, 2011 letter responding to Senator Franken's May 25, 2011 letter.

2. If not, will Apple at least commit to requiring that all location-aware apps in the Apple App Store have a clear, understandable privacy policy?

Response:

For Apple's response to this question, please see the attached June 1, 2011 letter responding to Senator Franken's May 25, 2011 letter.

3. In your testimony you said that requiring apps to have privacy policies is not enough to protect user's privacy. I agree. What further steps can you take, in addition to requiring privacy policies, that will help users understand where their information is going and have greater control over it?

Response:

Apple has taken steps to help customers understand where their information is going and to provide customers with greater control over it. First, Apple's Privacy Policy, which is available from links on every page of Apple's website, contains express disclosures regarding Apple's collection and use of location data and non-personal information:

> **Location-Based Services**
>
> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.
>
> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.
>
> **********

Collection and Use of Non-Personal Information

We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information for any purpose. The following are some examples of non-personal information that we collect and how we may use it:

- We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.

...

If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

Second, Apple's Software License Agreements for products that provide location-based services provide express disclosures regarding Apple's collection and use of location information. For example, to activate an iPhone, the customer must accept and agree to the iPhone SLA, including the following provision regarding location data:

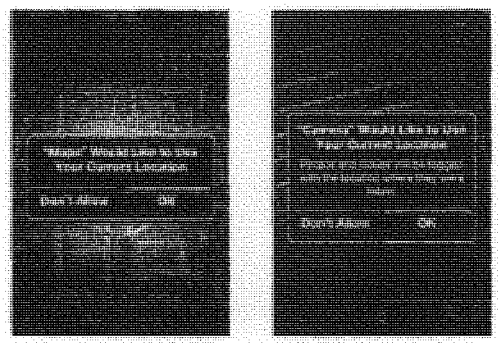
4. Consent to Use of Data.

...

(b) Location Data. Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide and improve these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide and improve location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** (emphasis exists in the SLA) You may withdraw this consent at any time by going to the Location Services setting on your iPhone and either turning off the global Location Services setting or turning off the individual location settings of each location-aware application on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party

> applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services. ...
>
> At all times your information will be treated in accordance with Apple's Privacy Policy, which is incorporated by reference into this License and can be viewed at: www.apple.com/legal/privacy/.

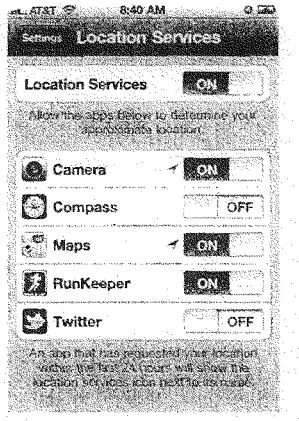
Third, as described above, before any app can access or use location information, iOS, the device's operating system, discloses to the customer that the app "would like to use [the customer's] current location" and requests the customer's express consent.



Fourth, before Apple will collect any diagnostic information from an iOS customer, that customer must explicitly agree that Apple may collect and use such information. For example, iPhone customers must click "Agree" in response to the following disclosure:

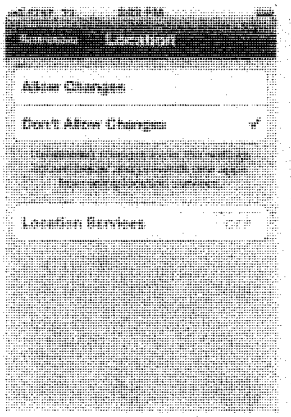
> You can help Apple improve its products by sending us anonymous diagnostic and usage information about your iPhone.
>
> By clicking "Agree" you agree that Apple may periodically collect and use this information as part of its support services and to improve its products and services. This information is collected anonymously. To learn more about Apple's Privacy Policy, see http://www.apple.com/legal/privacy.

Fifth, Apple provides its customers with functionality to control the location-based service capabilities of their devices. Apple has always required express customer consent, as described above, when any app requests location-based information for the first time. If the customer does not consent, iOS will not provide any location-based information to the app. iOS also permits customers to identify individual apps that may not access location-based information, even if Location Services is on.



Customers can change their individual app settings at any time. As mentioned in Dr. Tribble's May 20, 2011 testimony, an arrow icon ( ) alerts customers that an app is using or has recently used location-based information. This icon appears in real-time for currently running apps and next to the "On/Off" toggle switch for any app that has used location-based information in the past twenty-four hours.

Customers can use Restrictions, also known as Parental Controls, on a mobile device to prevent access to specific features, including Location Services. When a customer enables Restrictions, the customer must enter a passcode (this passcode is separate from the device passcode that the customer may set).



If the customer turns Location Services off and selects "Don't Allow Changes," the user of the device cannot turn on Location Services without that passcode. In addition, iOS will not (1)

provide any location information to any apps, including apps that may have previously received consent to use location information; (2) collect or geo-tag information about nearby Wi-Fi hotspots or cell towers; or (3) upload any location information to Apple from the device.

Finally, for iOS versions 4.1 and later, if the customer turns Location Services off, the mobile device does not send geo-tagged data about Wi-Fi hotspots and cell towers to Apple.

Apple's recent public statements and testimony have also provided customers with more information about how Apple and Apple devices use location information.

Apple is always investigating new ways to improve its customers' experiences, including helping customers learn more about Apple's privacy policy and the privacy protections available on Apple mobile devices.

4. Will Apple commit to informing users though a clear, conspicuous method (i.e. a permission screen) of the non-location information (i.e. calendar information, address book information, etc.) that an app will access once it is downloaded onto an Apple mobile device?

Response:

Apple is committed to the protection of all user personal data. As described in Apple's previous responses and testimony, Apple requires that all third-party app developers provide clear and complete information to customers regarding the collection, use and disclosure of any user or device data.

Specifically, third-party app developers must register with Apple, pay a fee, and sign a licensing agreement containing numerous provisions governing the collection and use of user data, device data, and location-based information, including the following:

- The developer must provide clear and complete information to users regarding the developer's collection, use and disclosure of user or device data (e.g., the developer must include a description on the App Store or add a link to the applicable privacy policy);
- The developer may collect, use, or disclose to a third party user or device data only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the app;
- If the customer denies or withdraws consent, apps may not collect, transmit, process or utilize the customer's user or device data;
- The developer must take appropriate steps to protect customers' user and device data from unauthorized use, disclosure, or access by third parties;
- The developer must comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data;

- The app must not disable, override, or otherwise interfere with Apple-implemented system alerts, display panels, consent panels and the like, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Apps submitted to Apple for placement in the App Store that fail to comply with these rules are returned to the developer to be fixed. If the developer successfully corrects the app, it goes into the App Store; if not, Apple will not offer the app to its customers.

Product improvement and evolution at Apple is a way of life. We are constantly examining ways to improve the user experience and the functionality of our devices. This applies to privacy just as much as it does to every other product or service we offer. We will continue to investigate new ways to offer user enhancements in the area of data protection.

5. Will Apple commit to informing users through a clear, conspicuous method (i.e. a permission screen) that the apps they download have the technical ability to share or disclose the information they gather from the user to third parties?

Response:

Please see response to Question No.4 above.

As described in greater detail below, Apple has also documented in the App Store Review Guidelines a set of technical, content, and design criteria that every app must satisfy before Apple will accept the app for inclusion in the App Store. Pursuant to these Guidelines:

- "Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used."

- Developers and apps "may not collect user or device data without prior user consent, and then only to provide a service or function that is directly relevant to the use of the Application, or to serve advertising. [Developers] may not use analytics software in [their] Application to collect and send device data to a third party."

Apps submitted to Apple for inclusion in the App Store that fail either of these requirements are returned to the developer and are not offered in the App Store until the deficiency is corrected.

6. Apple appears to acknowledge that it has not done enough to educate users about how their location information is being used. See Apple Q&A on Location Data, April 27, 2011 ("Users are confused, partly because the creators of this new technology (including Apple) have not provided enough education about these issues to date.") Can you explain how Apple will improve its education of users about the way their location information is gathered, used and shared by Apple and others?

Response:

In addition to the policies and systems described above, Apple's recent statements, including Apple's April 27, 2011 public Q&A on Location Data, press interviews, and testimony have provided customers with extensive information about how Apple and Apple devices use location information.

Apple is strongly committed to protecting our customers' privacy and will continue to explore new ways to educate customers about the collection and use of their location information.

7. You have said that Apple audits the applications in the App Store and that if Apple finds an app is violating the Registered Apple Developer Agreement, it will remove it from the store. Yet when I asked you at the hearing how many apps had been kicked out of the store for violating these terms, you said "zero". Do you believe that there is not a single app that is currently violating your Developer Agreement?

Response:

In response to Senator Franken's question, Dr. Tribble explained that Apple has not yet had to remove any app from the App Store because the app was improperly sharing a customer's location information with third parties. In fact, at the time of Dr. Tribble's May 10, 2011 testimony Apple was unaware of any app that had been (a) admitted into the App Store, (b) was subsequently determined to violate some aspect of the rules relating to the collection, retention or transmission of location data, (c) was not corrected after the developer was notified and given an opportunity to resolve the problem, and then (d) was "kicked out of the store" for violating these terms. As discussed below, Apple, however, has removed and continues to remove apps from the App Store for other types of violations.

As Dr. Tribble further explained, Before Apple will even consider accepting a third-party app for the App Store, the app developer must register with Apple, pay a fee, and sign developer and license agreements that contain numerous provisions governing, among other things, the collection and use of user data, device data, and location-based information, including those outlined above. Once the developer agrees to comply with these requirements, the developer may submit apps for review through Apple's approval process.

Apple performs a rigorous review of every app submitted based on a set of technical, content, and design criteria. The review criteria are documented in Apple's App Store Review Guidelines for iOS apps, which is made available to every app developer. A copy of the Guidelines is attached to these responses. The Guidelines include myriad requirements, including requirements about an app's functionality, content, and use of location or personal information. For example, the Guidelines state that:

4. Location

4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected

...

4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

...

16. Objectionable content

16.1 Apps that present excessively objectionably or crude content will be rejected

16.2 Apps that are primarily designed to upset or disgust users will be rejected

...

17. Privacy

17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used

17.2 Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected

17.3 Apps that target minors for data collection will be rejected

...

18. Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings," will be rejected

18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" alls) will be rejected

...

On average, Apple rejects approximately 30% of the apps initially submitted for consideration. The most common reasons for rejection relate to functionality issues, such as the app crashing, exhibiting bugs, or not performing as advertised by the developer. But Apple will reject an app for violating any of the criteria set forth in the Guidelines and/or any of the provisions of the developer's agreements with Apple.

When Apple rejects an app, most developers respond by correcting the issue or issues that led to Apple's rejection so that the app may ultimately be accepted. Apple will not, however, accept any app in the App Store unless and until the developer and app are in full compliance with Apple's criteria and the developer agreements.

Similarly, Apple will remove from the App Store any app that is determined to be in violation of any of these requirements. Some of the most common reasons for removal of an app from the App Store relate to an app's violation of some other party's intellectual property rights, violation of some law, or use of objectionable content.

8. In Apple's May 6, 2011 response to my letter of April 27, 2011, Apple wrote that when "using only the crowd-sourced locations of Wi-Fi hotspots and cell towers... the device location calculated by iOS will only be an approximation." Please give the mean, median, and mode of how accurately the device's location can be calculated using only the crowd-sourced database Apple maintains on mobile devices. Please use precise figures, e.g. 50m, 100m, etc.

Response:

iOS can use the information in the crowd-sourced database to triangulate the device location when GPS is not available (such as when the device is indoors or in a basement). It is difficult to provide specific information regarding how accurate that determination will be because the accuracy can vary greatly based on factors such as whether the device is indoors or outdoors, in a rural or urban area, at a high or low altitude, etc. In general, iOS can calculate the device location using the crowd-sourced database to within 65 to 300 meters. The accuracy, however, will be worse than 300 meters – and, in some cases, significantly worse than 300 meters – in situations such as when the device is in very rural areas.

9. In various statements, Apple has stressed that the hotspots and cell towers in the crowd-sourced database downloaded to users' mobile devices "could be more than one hundred miles away." Please give the mean, median, and mode of the distance these hotspots and cell towers are from users' devices. Please use precise figures, e.g. 50m, 100m, etc.

Response:

As described previously, Apple downloads a subset of its crowd-sourced database content to a local cache on the device when the iOS has made a request for location information. Apple downloads the calculated locations of: (1) the hotspots and cell towers that the device can "see" (the "visible" hotspots and cell towers); (2) the hotspots and cell towers that are nearby; and (3) nearby cell location area codes.

To identify "nearby" hotspots and cell towers, Apple's servers search in the crowd-sourced database for hotspots and cell towers that are within up to a 2° North/South range and 4° East/West range of each visible hotspot and cell tower. Note that to ensure prompt response times, Apple limits the download to no more than 1600 hotspot locations and 100 cell tower

locations at any given time. Thus, Apple does not necessarily download all nearby hotspots and cell towers that fall within this North/South and East/West range.

Again, it is difficult to provide specific information regarding the distance that the hotspots and cell towers in the cached subset of the crowd-sourced database are from the device because the distance can vary greatly based on factors such as those identified above, the cellular carrier used by the device, etc. In some cases, the hotspots and cell towers could be within a range of more than one hundred miles; in other cases, they could be within a range of only a few hundred meters.

It is also important to note that the cached subset of the crowd-sourced database does not contain any information that indicates the distance of the hotspots and cell towers from the device's location at the time the cache was downloaded or at any other time. Thus, the database does not reveal that one particular hotspot may have been only a few hundred meters away while another was more than one hundred miles away. As described below in response to Question No. 10, the cached crowd-sourced database is just a localized map of the general vicinity of the device. As with a paper map, this map does not reveal the specific location of a device – it simply provides the device with the information needed for the device to determine, by looking at the map (among other things), its specific location.

10. In an interview with All Things Digital, Apple founder Steve Jobs stated that the hotspots and cell tower data in the crowd-sourced database downloaded to users' mobile devices "are not telling you anything about your location." *See* Hayley Tsukayama, "Post Tech: Jobs explains mobile policies, says Apple will testify in hearing," *Washington Post*, April 27. Is it Apple's position that the WiFi hotspot and cell tower data in the crowd-sourced database downloaded to users' mobile devices do not in any way communicate anything about a user's location?

Response:

As described in Apple's previous responses and testimony, the crowd-sourced database does not reveal personal or location information about any customer. The crowd-sourced database includes anonymous location information for Wi-Fi hotspots and cell towers that is derived in part from the geo-tagged hotspot and cell tower information sent by Apple devices.

Although a local cache of a subset of Apple's crowd-sourced database is temporarily stored on the iOS-based mobile device, it is not the data collected from that device or any other device – instead, it comprises the locations for hotspots and cell towers as calculated by Apple using crowd-sourced data obtained from Apple mobile devices. In addition, Apple's servers do not track what specific subsets of the crowd-sourced database are downloaded to and/or cached on a device. Thus, while the information that is downloaded is selected based on the device's location at the time of the download, Apple does not collect, track, or store what information is downloaded.

One useful way to think of the crowd-sourced database is to compare it to a world map. Like a world map, the crowd-sourced database of cell towers and Wi-Fi hotspots contains the calculated locations of cell towers and Wi-Fi hotspots that Apple has gathered. It does not have any information about where any individual person or iPhone is located on that map at any time. The cache that is temporarily stored on an iPhone is like a series of localized city street maps.

For example, consider a customer who is in Paris and wants to get information about his or her current location. The customer's iPhone will send a request to Apple's servers that indicates that the iPhone can "see" the Eiffel Tower. The Apple servers respond by returning the location of cell towers and hotspots in Paris – a local map of Paris. The iPhone uses the fixed locations of those nearby cell towers and Wi-Fi hotspots to determine its own location relative to those points. Apple's servers do not retain the initial request from the iPhone nor any record that a map of Paris was dispatched. The iPhone itself "knows" that it can "see" the Eiffel Tower and that it now has access to a map of Paris, but no record of the transaction is retained within Apple and no association exists between any individual or individual device and the sending out of the map of Paris.

The data stored in the local cache of Apple's crowd-sourced database does not communicate anything to Apple – and, specifically, does not communicate anything to Apple about a user's location.

11. Apple has acknowledged that the crowd-sourced database cache stored on the iPhone should not have kept up to a year's worth of data. See Apple Q&A on Location Data, April 27, 2011 ("The reason the iPhone stores so much data is a bug we uncovered..."). On what date did Apple employees discover this "bug"?

Response:

Apple discovered the bug in late April 2011 when Apple was investigating the O'Reilly researchers' claims that consolidated.db included a large amount of hotspot and cell tower data. The May 4, 2011 free iOS update fixed this bug. After this update, iOS will purge records that are older than seven days, and the cache will be deleted entirely when Location Services are turned off.

12. On what date did Apple learn that the iPhone was submitting location information to Apple servers even when location services were turned off?

Response:

In September 2010, Apple released iOS version 4.1. In certain iOS versions prior to version 4.1, a bug caused iOS to send anonymous, geo-tagged information about Wi-Fi hotspots and cell towers to Apple even if the customer had turned off Location Services. At the time of the version 4.1 update, Apple was not aware of this bug; however, as a result of updates to location services that were included in the version 4.1 update, the bug was eliminated.

Apple did not discover that this bug had existed or that the iOS version 4.1 update had fixed the bug until late April 2011 when Apple was investigating the O'Reilly researchers' claims that consolidated.db included a large amount of hotspot and cell tower data. At approximately the same time, Apple discovered that, because of a different bug, even when Location Services was off, Apple's servers would update the local cache of crowd-sourced location information for Wi-Fi hotspots and cell towers in response to an app request for location information. Although the local cache was updated, none of the downloaded crowd-sourced location information, or

any other location information, was provided to or disclosed to the app. Apple's May 4, 2011 free iOS update fixed this bug.

13. Under what circumstances does Apple consider location information obtained from a user's device to be non-content customer records data subject to the voluntary disclosure permission in the Electronic Communications Privacy Act, 18 U.S.C. § 2702(c)(6)?

Response:

As described above and in Apple's previous responses and testimony, the geo-tagged information for Wi-Fi hotspots and cell towers obtained by Apple from Apple mobile devices does not identify any particular customer or device. Accordingly, even if Apple were considered subject to the provisions of 18 U.S.C. § 2702(c)(6), this information collected by Apple is not *customer* records data.

Apple's Responses to Senator Tom Coburn's May 18, 2011 Questions

1. **Mr. Tribble, in Mr. Soltani's testimony, he gave the committee an example whereby he seemed to imply that Apple had knowledge of his own iPhone's location within a few feet when he was sitting in the atrium of the Senate Hart Office Building using Wi-Fi. Your testimony states that Apple does not track users' locations. Can you clarify the seeming contradiction regarding the location data on Mr. Soltani's iPhone in his example?**

Response:

As described in Apple's previous responses and testimony, Apple does not track users' locations. In Mr. Soltani's example, iOS, the operating system running on his iPhone, not Apple, determined the iPhone's location. Apple did not obtain or record Mr. Soltani's location.

When Mr. Soltani ran an app that requested the current location of the device (apparently the Maps app), Apple would have downloaded a subset of the crowd-sourced database content to the local cache on his iPhone. Mr. Soltani's iPhone would then have been able to use the information in the local cache to calculate his approximate location. The iPhone would have performed this calculation without any further contact with Apple, and the iPhone would not have communicated the calculated location back to Apple.

One useful way to think of our cell tower and Wi-Fi hotspot database is to compare it to a world map, like the Rand McNally World Atlas. Like a world map, our database of cell towers and Wi-Fi hotspots contains the calculated locations of cell towers and Wi-Fi hotspots we have gathered. It does not have any information about where any individual person or iPhone is located on that map at any time. The cache on your iPhone is like a series of localized city street maps. When you enter a new area, Apple downloads a subset of the World Atlas – a more localized map of cell towers and Wi-Fi hotspots – to your iPhone to assist the iPhone in providing the location services you have requested. Your iPhone uses the fixed locations of the cell towers and Wi-Fi hotspots to determine its own location relative to those points. Your iPhone, not Apple, determines its actual location without any further contact with Apple. After the location is determined, it is not transmitted to Apple.

Mr. Soltani's example does not contradict Apple's explanation or previous testimony. The iPhone "knows" its location because iOS on the iPhone calculated the location. This location is not communicated to Apple.

2. **Apple states it does not sell users' personally identifiable information to third parties. However, Apple operates advertising services that are connected to mobile devices using its platform. Can you comment on how you operate your ad services, particularly whether you send targeted ads to mobile device users, and if so, what user information you collect in order to send targeted ads?**

Response:

On July 1, 2010, Apple launched the iAd mobile advertising network. The network can serve ads to iPhone, iPod touch, and iPad devices running iOS 4, and the network offers a

dynamic way to incorporate and access advertising within apps. Customers can receive advertising that relates to their interests ("interest-based advertising") and/or their location ("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

Customers may opt out of location-based advertising by toggling the device's location-based service capabilities Off. For customers who do not toggle location-based service capabilities Off, Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Similarly, as specified clearly in Apple's privacy policy as well as in all relevant Apple device software licensing agreements, customers may opt out of interest-based advertising by visiting the following site from their mobile device: http://oo.apple.com. For customers who do not opt-opt of interest-based advertising, Apple uses information from the customer's iTunes account along with information obtained from Acxiom, a third party data aggregator, to send better targeted ads to our customers. For example, Apple may obtain information from iTunes about the customer's media preferences based on the categories of apps, movies, music, TV shows, and books downloaded by the customer – such as, "travel apps" or "documentary movies." The iAd server can then select ads that are relevant to and consistent with those media preferences – such as, ads relating to travel services or a newly-released documentary movie.

As stated in Apple's Privacy Policy, Apple uses this "personal information to help us develop, deliver, and improve our products, services, content, and advertising." Unless a customer provides express prior consent, as discussed below, Apple does not sell or share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

In some cases, an advertiser may want to provide – in the ad – more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialog box will appear stating: "'Advertiser' would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad app with more specific location information.

a. **Is advertising the largest source of revenue for Apple? If not, what services or products contribute most to your bottom line?**

Response:

Advertising revenue currently makes up less than one percent of Apple's total revenue. Apple's sales of hardware and software products and related services account for the vast majority of Apple's revenue.

b. **Are there any apps to which Apple refuses to provide advertising services? If so, what are the primary reasons for refusing such services? If not, why?**

Response:

Apple offers its iAd services only to apps that have been approved for inclusion in the App Store. As discussed below in response to Question 2.c., Apple reviews all apps before adding them to the App Store to ensure, among other things, that the app complies with the provisions of Apple's developer agreements and app store review guidelines. If an app does not comply with all provisions, Apple will not add the app to the App Store or provide iAd services to the app.

In addition, Apple attempts to identify apps that appear to be targeted predominantly to children, and Apple does not provide iAd services to those apps.

c. **Are there any apps Apple refuses to host in its app stores? If so, what are the primary reasons for refusing to provide those apps, and how often, on average, do you reject an app or later remove it from your store for questionable behavior?**

Response:

Before Apple will even consider accepting a third-party app for the App Store, the app developer must register with Apple, pay a fee, and sign developer and license agreements that contain numerous provisions governing, among other things, the collection and use of user data, device data, and location-based information, including the following:

- The developer must provide clear and complete information to users regarding the developer's collection, use and disclosure of user or device data (e.g., the developer must include a description on the App Store or add a link to the applicable privacy policy);
- If the customer denies or withdraws consent, the app may not collect, transmit, process or utilize the customer's user or device data, including location data;
- The developer must take appropriate steps to protect customers' user and device data, including location-based information, from unauthorized use, disclosure, or access by third parties;

- The developer must comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data, including location-based information;

- The app must not disable, override, or otherwise interfere with Apple-implemented system alerts, display panels, consent panels and the like, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Once the developer agrees to comply with these requirements, the developer may submit apps for review through Apple's approval process.

Apple performs a rigorous review of every app submitted based on a set of technical, content, and design criteria. The review criteria are documented in Apple's App Store Review Guidelines for iOS apps, which is made available to every app developer. A copy of the Guidelines is attached to these responses.

The Guidelines include myriad requirements, including requirements about an app's functionality, content, and use of location or personal information. For example, the Guidelines state that:

> **4. Location**
>
> 4.1 Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected
>
> ...
>
> 4.4 Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses
>
> ...
>
> **16. Objectionable content**
>
> 16.1 Apps that present excessively objectionably or crude content will be rejected
>
> 16.2 Apps that are primarily designed to upset or disgust users will be rejected
>
> ...
>
> **17. Privacy**
>
> 17.1 Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used
>
> 17.2 Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected
>
> 17.3 Apps that target minors for data collection will be rejected

...

18. Pornography

18.1 Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings," will be rejected

18.2 Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" alls) will be rejected

...

On average, Apple rejects, through its review process, approximately 30% of the apps initially submitted for consideration. The most common reasons for rejection relate to functionality issues, such as the app crashing, exhibiting bugs, or not performing as advertised by the developer. But Apple will reject an app for violating any of the criteria set forth in the Guidelines and/or any of the provisions of the developer's agreements with Apple.

When Apple rejects an app, most developers respond by correcting the issue or issues that led to Apple's rejection so that the app may ultimately be accepted. Apple will not, however, accept any app in the App Store unless and until the developer and app are in full compliance with Apple's criteria and the developer agreements.

Similarly, Apple will remove from the App Store any app that is determined to be in violation of any of these requirements. Some of the most common reasons for removal of an app from the App Store relate to an app's violation of some other party's intellectual property rights, violation of some law, or use of objectionable content.

d. How many employees and/or automated services are dedicated to crawling Apple's app store to weed out apps that inappropriately use consumers' personal information or violate its privacy policy?

Response:

Apple currently has a team of approximately 80 employees dedicated to performing the rigorous app review process described above. This process is not uniquely focused on the protection of consumer information but rather applies to testing for compliance with all of the rules pertaining to apps within the App Store. Once an app is accepted into the App Store, Apple requires the developer resubmit the app for approval if the developer wants to modify the app in any way. In some instances, however, apps have been changed after the review process and after they have been made available on the App Store.

Apple employees from several teams are responsible for addressing issues that arise with apps that are already in the App Store. For example, members of Apple's legal team routinely address issues raised by third parties who, once the app has gone public, complain that it violates some aspect of their intellectual property. Apple relies heavily on communications from other App Store users, competitors, and industry observers to alert Apple that an app that is operating outside of Apple's Guidelines. Whenever such a case is brought to

Apple's attention, either through internal vigilance or by an external party, Apple investigates and provides the developer with an opportunity to remediate. If no correction is made, Apple removes the app from the App Store.

e. **In other contexts, such as the sale of counterfeit pharmaceuticals online, there has been a recent push in the industry (with the suggestion of the Intellectual Property Enforcement Coordinator) to form a working group in order for the industry to take the lead on how to combat the dangerous use of these products online. Is there any such industry working group to address the unique issues surrounding mobile device products and/or location based services?**

Response:

There are numerous and robust efforts underway in industry trade associations and think tanks partnering with industry aimed at addressing the unique challenges presented by mobile devices and location based services, including issues related to privacy. Apple is aware of at least the following groups already actively working on these issues: CTIA (The Wireless Association), ACT (Association for Competitive Technology), CEA (Consumer Electronic Association), ITI (Information Technology Industry Council), TechAmerica, Center for Democracy and Technology (CDT).

Apple's Responses to Senator Richard Blumenthal's May 18, 2011 Questions

1. **Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and wireless access points for any purpose? If so:**

Response:

No. Apple has never intercepted wireless data transmissions between third party computers and Wi-Fi hotspots.

As described in Apple's previous responses and testimony, Apple collects anonymous location information about Wi-Fi hotspots from broadcast messages transmitted by the hotspots. Such broadcast messages are not transmissions directed between any specific third party computer and the hotspot, but are instead messages, or "beacons," broadcast by the hotspot that do not identify any intended recipient.

Also as described previously, Apple pays a fee to Skyhook Wireless ("Skyhook") for access to Skyhook's location data for Wi-Fi hotspots. Apple has no information indicating that any of the location data obtained from Skyhook was derived from the interception of wireless data transmissions between third party computers and wireless access points; however, Apple cannot speak to the specifics of Skyhook's technology.

Note that in connection with testing and debugging network performance issues with iOS, Apple's mobile device operating system, and Mac OS X, Apple's laptop and computer operating system, Apple may perform targeted diagnostic monitoring of network performance on Apple Wi-Fi networks and, occasionally, on a public Wi-Fi network based on specific feedback received about network performance on that public network. Apple does not use any diagnostic information obtained from such monitoring for location-based services; the diagnostic information is used solely for the purpose of improving product network performance.

A. **Please indicate any and all foreign and domestic jurisdictions where your company has contemplated, implemented, or purchased information derived from *the interception of wireless data transmissions described above.***

Response:

N/A

B. **Please indicate any and all purpose(s) underlying any such signal interceptions.**

Response:

N/A

C. **Please provide a precise timeline of events related to the interception of wireless data transmissions by your company and/or the purchase of information derived**

from such interceptions, including when such interceptions were initially contemplated, initially implemented, and subsequently revised, if applicable.

Response:

N/A

D. Please describe any and all methods initially contemplated and/or implemented for these purposes.

Response:

N/A

E. Subsequent to any initial steps toward intercepting wireless data transmissions, please describe any and all methods subsequently contemplated and/or implemented for these purposes.

Response:

N/A

F. Please indicate any and all types of data captured from signals traveling between third party computers and wireless access points that that your company has ever intercepted, stored, or purchased (including but not limited to data frames, management frames, control frames, payload data, SSIDs, RSSI measurements, etc.). For each category of data, please define the term used to reference that category, including an indication of how it is derived.

Response:

N/A

G. Please provide text and citations for any and all materials directly or indirectly associated with your company that describe or contemplate methods for intercepting wireless data transmissions traveling between third party computers and wireless access points (including foreign or domestic patents, patent applications, published works, or other publicly available materials).

Response:

N/A

H. Do all of the methods (described in 1.D.) contemplated or implemented by your company (or implemented by other companies from whom you subsequently purchased derived data) for intercepting wireless data transmissions explicitly exclude the interception of "content data" transmitted between third party users and wireless access points? *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

1) If so, please explain how and why such content data is excluded from interception.

2) If not, please explain how and why such content data is not excluded from interception.

Response:

N/A

I. Do any of the methods (described in 1.D.) contemplated or implemented by your company for intercepting wireless data transmissions utilize the interception of "content data" transmitted between third party users and wireless access points to facilitate the underlying purpose of intercepting that data? If so, please explain how and why such content data is utilized. *Content data is defined as any data that may contain, in whole or in part, the content of a user's internet communications over a wireless network, including but not limited to data frames, payload data, etc.*

Response:

N/A

J. Has your company ever contemplated, implemented, or purchased information derived from the interception of wireless data transmissions traveling between third party computers and encrypted wireless access points and/or hidden wireless access points? If so, please explain how these methods differ from the methods associated with the interception of wireless data transmissions traveling between third parties and unencrypted wireless access points, if at all.

Response:

N/A

K. Has your company ever shared, sold, or distributed information acquired through interception and storage of wireless data transmissions traveling between third parties and wireless access points? If so, to whom and for what purpose(s)?

Response:

N/A

2. Has your company ever contemplated, constructed, or purchased information related to the location of wireless access points? If so, please ensure that Questions 1.A. through 1.H. are fully answered with respect to the purpose of locating wireless access points.

Response:

Yes, to provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer's request for current location information, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points – also referred to as Wi-Fi hotspots. As described in greater detail in Apple's previous responses and testimony, Apple collects from millions of Apple devices anonymous location information for cell towers and Wi-Fi hotspots. From this anonymous information, Apple has been able, over time, to calculate the known locations of many millions of Wi-Fi hotspots and cell towers. Because the basis for this location information is the "crowd" of Apple devices, Apple refers to this as its "crowd-sourced" database.

Apple collects this location-based information for only one purpose – to enhance and improve the services we can offer to our customers.

As noted above, Apple does not collect or derive information about Wi-Fi hotspots from the interception of wireless data transmissions between third party computers and Wi-Fi hotspots. Instead, Apple mobile devices collect information about Wi-Fi hotspots that the devices can "see" from broadcast messages transmitted by the hotspots. The devices then tag that information with the device's current GPS coordinates, i.e., the devices "geo-tag" the hotspots.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a local cache on the device. Every twelve hours, or later if the device does not have Wi-Fi access at that time, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection. (Note that as of Apple's May 4, 2011 free iOS software update, iOS will clear this data from the local cache after twenty-four hours, even if the device never had Wi-Fi access and, thus, was not able to transmit the data to Apple.) Apple's servers use this information to re-calculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced database. Apple cannot identify the source of this information, and Apple collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced database. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one app's request to use location information.

In addition, for computers and laptops running Apple's Mac OS X operating system and mobile devices running older versions of Apple's mobile operating system (iPhone OS versions 1.1.3 to 3.1), Apple relied on (and still relies on) a database of Wi-Fi hotspot location information maintained by Skyhook. Beginning with iOS version 3.2 released in April 2010, Apple relies on its own crowd-sourced database of Wi-Fi hotspot location information.

As noted above, Apple has no information indicating that any of the data that Apple obtained from Skyhook was derived from the interception of wireless data transmissions between third party computers and wireless access points. Apple cannot, however, speak to the specifics of Skyhook's technology.

A. How many wireless access points exist, or have ever existed, in any database of wireless access point locations?

Response:

As of March 22, 2011, Apple's crowd-sourced database includes approximately 223 million active Wi-Fi hotspots.

1) How many of these wireless access points were unencrypted when identified?

Response:

Apple does not collect information about the encryption scheme of Wi-Fi hotspots and, thus, does not know how many of these hotspots were unencrypted.

2) How many of these wireless access points were encrypted when identified?

Response:

Apple does not collect information about the encryption scheme of Wi-Fi hotspots and, thus, does not know how many of these hotspots were encrypted.

3) How many of these wireless access points were "hidden" when identified?

Response:

On March 2, 2011, with the release of iOS version 4.3, iOS first began collecting from hotspot broadcasts a single Boolean value indicating whether the SSID is or is not present for the hotspot (i.e., whether the hotspot is or is not "hidden"). Note that Apple does not collect the SSID for any hotspot, regardless of whether or not the hotspot is hidden. Because Apple only recently started collecting the Boolean value indicating whether the hotspot is or is not hidden, Apple does not yet have statistical information available for how many hotspots were "hidden."

3. Please describe any and all ways in which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Indirectly valuable for effectuating the purpose of efficiently locating wireless access points; and

Response:

Apple does not intercept or store "content data" transmitted between third party users and wireless access points for locating wireless access points.

Apple is aware of public studies, papers, and patents discussing the use of content or payload data, payload transmissions, and bit-error rates for certain location purposes. Apple does not implement any of these techniques.

B. Indirectly valuable to your company for any other purpose.

Response:

Again, Apple does not intercept or store "content data" transmitted between third party users and wireless access points and does not have an opinion regarding how such information might or might not be valuable for any other purpose.

4. Please describe your view of the circumstances under which the interception and/or storage of "content data" transmitted between third party users and wireless access points might be:

A. Legal or illegal under current federal law;

Response:

Apple does not intercept or store "content data" transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under current federal law.

B. Legal or illegal under current state law; and

Response:

Apple does not intercept or store "content data" transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under the current laws of any state.

C. Legal or illegal in any foreign jurisdictions in which your company has engaged in the interception and/or storage of wireless data transmissions traveling between third party computers and wireless access points.

Response:

Apple does not intercept or store "content data" transmitted between third party users and wireless access points and, thus, does not have an opinion regarding whether such interception and/or storage is or is not legal under the laws of any foreign country.

Department of Justice

STATEMENT OF

JAMES A. BAKER
ASSOCIATE DEPUTY ATTORNEY GENERAL

BEFORE THE

COMMITTEE ON JUDICIARY
UNITED STATES SENATE

ENTITLED

"THE ELECTRONIC COMMUNICATIONS PRIVACY ACT:
GOVERNMENT PERSPECTIVES ON PROTECTING PRIVACY IN THE DIGITAL AGE"

PRESENTED

APRIL 6, 2011

Good afternoon, Chairman Leahy, Ranking Member Grassley, and Members of the Committee. Thank you for the opportunity to testify on behalf of the Department of Justice regarding the Electronic Communications Privacy Act (ECPA). ECPA, which includes the Stored Communications Act and the Pen Register statute, is part of a set of laws that controls the collection and disclosure of both content and non-content information related to electronic communications, as well as content that has been stored remotely. These laws serve two functions. They are critical tools for law enforcement, national security, and cyber security activities, and they are essential for protecting the privacy interests of all Americans.

ECPA has never been more important than it is now. Because many criminals, terrorists and spies use telephones or the Internet, electronic evidence obtained pursuant to ECPA is now critical in prosecuting cases involving terrorism, espionage, violent crime, drug trafficking, kidnappings, computer hacking, sexual exploitation of children, organized crime, gangs, and white collar offenses. In addition, because of the inherent overlap between criminal and national security investigations, ECPA's standards affect critical national security investigations and cyber security programs.

ECPA has three key components that regulate the disclosure of certain communications and related data. First, section 2701 of Title 18 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties. Second, section 2702 of Title 18 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-governmental entities. Third, section 2703 of Title 18 regulates government access to stored communications; it creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications. ECPA was initially enacted in 1986 and has been amended repeatedly since then, with substantial revisions in 1994 and 2001.

Mr. Chairman, the Department of Justice is charged with the responsibility of enforcing the laws, safeguarding the constitutional rights of Americans, and protecting the national security of the United States. As such, we welcome these hearings on this important topic. We appreciate the concerns that some in Congress, the courts, and the public have expressed about ECPA. We know that some believe that ECPA has not kept pace with technological changes or the way that people today communicate and store records, notwithstanding the fact that ECPA has been amended several times for just that purpose. We respect those concerns, and we appreciate the opportunity to discuss them here today. We also applaud your efforts to undertake a renewed examination of whether the current statutory scheme appropriately accommodates such concerns and adequately protects privacy while at the same time fostering innovation and economic development. It is legitimate to have a discussion about our present conceptions of privacy, about judicially-supervised tools the government needs to conduct vital law enforcement and national security investigations, and how our statutes should accommodate both. For example, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a

warrant to obtain the content of emails that are stored for more than 180 days. We are ready and willing to engage in a robust discussion of these matters to ensure that the law continues to provide appropriate protections for the privacy and civil liberties of Americans as technology develops.

As we engage in that discussion, what we must not do – either intentionally or unintentionally – is unnecessarily hinder the government's ability to effectively and efficiently enforce the criminal law and protect national security. The government's ability to access, review, analyze, and act promptly upon the communications of criminals that we acquire lawfully, as well as data pertaining to such communications, is vital to our mission to protect the public from terrorists, spies, organized criminals, kidnappers, and other malicious actors. We are prepared to consider reasonable proposals to update the statute – and indeed, as set forth below, we have a few of our own to suggest – provided that they do not compromise our ability to protect the public from the real threats we face.

Significantly, ECPA protects privacy in another way as well: by authorizing law enforcement officers to obtain evidence from communications providers, ECPA enables the government to investigate and prosecute hackers, identity thieves, and other online criminals. Pursuant to ECPA, the government obtains evidence critical to prosecuting these privacy-related crimes.

I. ECPA Plays a Critical Role in Protecting Public Safety.

The government is responsible for catching and punishing criminals, deterring crime, protecting national security, and guarding against cyber threats. The government also plays a significant role in protecting the privacy and civil liberties of all Americans. The government enforces laws protecting privacy, and pursues cyber criminals and others who engage in identity theft and other offenses that violate privacy laws. Over the decades, government access to certain electronic communications, including both content and non-content information, has become even more important to upholding our law enforcement and national security responsibilities.

Pursuing criminals and tracking national security threats, however, is no simple task. Not only does the rapidly changing technological environment affect individual privacy, it also can impact adversely on the government's ability to investigate crime and respond to national security and cyber threats. As originally enacted, ECPA endeavored to establish a framework for balancing privacy and law enforcement interests – and to do so notwithstanding technological change. But the actual pace of change puts pressure on that framework that has in the past necessitated periodic amendments to it. As noted above, we look forward to working with the Congress to assess whether amendments to ECPA are appropriate at this time to keep pace with changes in technology.

It is important to understand both the kind of information that the government obtains under ECPA and how that information is used in criminal investigations. Under ECPA, the government may compel service providers to produce both content and non-content information related to electronic communications. It is obvious that the contents of a communication – for example, a text message related to a drug deal, an email used in a fraud scheme, or an image of child pornography – can be important evidence in a criminal case. But non-content information may be equally important, particularly at the early stages of a criminal or national security investigation.

Generally speaking, service providers use non-content information related to a communication to establish a communications channel, route a communication to its intended destination, or bill customers or subscribers for communications services. Service providers often collect and store such records in order to operate their networks and for other legitimate business purposes. Non-content information about a communication – also referred to as "metadata" – may include information about the identity of the parties to the communication, the time and duration of the communication, and the communicants' location. During the early stages of an investigation, it is often used to gather information about a criminal's associates and eliminate from the investigation people who are not involved in criminal activity. Importantly, non-content information gathered early in investigations is often used to generate the probable cause necessary for a subsequent search warrant. Without ready access to non-content information, it may be impossible for an investigation to develop and reach a stage where agents have the evidence necessary to obtain a warrant for a physical search.

In my September 22, 2010, testimony before the Committee, I discussed several examples of how ECPA currently assists law enforcement in accomplishing our mission to protect public safety. For the sake of completeness of the record before the Committee in this Congress, I repeat them below.

Here is one example of how communications metadata can help in an investigation. In April 2010, a Sheriff's Office Uniformed Patrol Lieutenant in Baton Rouge, Louisiana attempted to stop a suspect. The suspect shot the Lieutenant through the neck and fled. An investigation later identified the suspect, and agents obtained an arrest warrant for attempted first degree murder of a police officer. In their efforts to locate and arrest the suspect, officers determined that the suspect used several cell phones to communicate with his girlfriend and other associates. Officers used ECPA subpoenas and court orders to the cell phone companies to obtain the suspect's calling records and location records. This information ultimately allowed officers to confirm the suspect's location.

As a second example, in a DEA investigation in 2008, investigators seized approximately $900,000 from a tractor trailer during a traffic stop in Detroit. After gaining the cooperation of the driver, the DEA identified a number of cellular telephones with "Push-To-Talk" features that were being used to contact organizational leaders in Mexico. Telephone toll record analysis along with additional investigation revealed a pattern of switching cellular telephones to avoid

detection and law enforcement interception. This technique effectively prevented the agents from obtaining the authority to conduct wiretap intercepts on these phones. The DEA was still able to use ECPA process to obtain cell site data to identify members of the criminal organization near Detroit. Obtaining this non-content information was critical to this outcome. Without the use of telephone toll record data, cell site information, and pen register data, the DEA would not have been able to identify these dangerous drug traffickers.

ECPA legal process has also proven instrumental in thwarting child predators. In a recent undercover investigation, an FBI agent downloaded images of child pornography and used an ECPA subpoena to identify the computer involved. Using that information to obtain and execute a search warrant, agents discovered that the person running the server was a high school special-needs teacher, a registered foster care provider, and a respite care provider who had adopted two children. The investigation revealed that he had sexually abused and produced child pornography of 19 children: his two adopted children, eight of their friends, three former foster children, two children for whom he provided respite care, and four of his special needs students. This man pleaded guilty and is awaiting sentencing.

One final example illustrates how communications service providers' records are important not only to regular criminal investigations, but also to keeping our law enforcement officers safe. Recently, a homicide detective in Prince George's County reported that, at 2:00 a.m., he and his partner were chasing a man wanted for a triple murder. Consistent with ECPA, they made use of cell tower information about the fugitive's mobile phone. Having this information immediately accessible increased officer safety and allowed them to marshal effectively available law enforcement resources. They successfully captured the fugitive in nine hours without placing officers, or the public, at undue risk.

These are only a few examples of how ECPA has become a critically important public safety tool. The Department of Justice thinks it is important that any changes to ECPA be made with full awareness of whether, and to what extent, the changes could adversely affect the critical goal of protecting public safety and the national security of the United States. For example, if an amendment were unduly to restrict the ability of law enforcement to quickly and efficiently determine the general location of a terrorist, kidnapper, child predator, computer hacker, or other dangerous criminal, it would have a very real and very human cost.

Congress should also recognize that raising the standard for obtaining information under ECPA may substantially slow criminal and national security investigations. In general, it takes longer for law enforcement to prepare a 2703(d) order application than a subpoena, and it takes longer to obtain a search warrant than a 2703(d) order. In a wide range of investigations, including terrorism, violent crimes, and child exploitation, speed is essential. In drug investigations, where targets frequently change phones or take other steps to evade surveillance, lost time can eliminate law enforcement's ability to collect useful evidence.

II. Portions of ECPA May Be Appropriate for Further Legislation or Clarification.

ECPA was enacted in 1986, but it has been amended on numerous subsequent occasions in light of the advance of technology and privacy concerns. Congress amended its provisions as recently as 2009; substantial revisions occurred in 1994 and 2001.

As we previously have testified, the Department of Justice stands ready to work with the Committee as it considers changes to portions of ECPA and the Pen Register statute (which was also enacted as part of the Electronic Communications Privacy Act in 1986). Although the Department does not endorse any particular legislative changes in today's testimony, we discuss matters that may be appropriate for amendment and the problems we see in those areas. In particular, this testimony addresses eight separate issues: the standard for obtaining prospective cell-site information, providing appellate jurisdiction for ex parte orders in criminal investigations, clarifying the standard for issuing 2703(d) orders, extending the standard for non-content telephone records to other similar forms of communication, clarifying the exceptions in the Pen Register statute, restricting disclosures of personal information by service providers, provider cost reimbursement, and the compelled disclosure of the contents of communications.

(1) Prospective cell-site information

One appropriate subject for further legislation is the legal standard for obtaining, on a prospective basis, cell tower information associated with cell phone calls. Cellular telephones operate by communicating through a carrier's infrastructure of fixed antennas. For example, whenever a user places or receives a call or text message, the network is aware (and makes a record) of the cell tower and usually which of three pie-slice "sectors"" covered by that tower serving the user's phone. This information, often called "cell-site information," is useful or even critical in a wide range of criminal cases, even though it reveals the phone's location only approximately (since it can only place the phone somewhere within that particular "cell" and sector). It is also often useful in early stages of criminal or national security investigations, when the government lacks probable cause for a warrant.

The appropriate legal standard for obtaining prospective cell-site information is not entirely uniform across the country. Judges in many districts issue prospective orders for cell-site information under the combined authority of a pen/trap order under the Pen Register statute and a court order under ECPA based upon "specific and articulable facts." (CALEA prohibits providers from making wireless location information available "solely pursuant" to the Pen Register statute.) Starting in 2005, however, some magistrate and district judges began rejecting this approach and holding that the only option for compelled ongoing production of cell location information is a search warrant based on probable cause. Courts' conflicting interpretations of the statutory basis for obtaining prospective cell-site information have created uncertainty regarding the proper standard for compelled disclosure of cell-site information, and some courts'

requirement of probable cause has hampered the government's ability to obtain important information in investigations of serious crimes. Legislation to clarify and unify the legal standard and the proper mechanism for obtaining prospective cell-site information could eliminate this uncertainty.

It should be noted that cell-site information is distinct from GPS coordinates generated by phones as part of a carrier's Enhanced 911 Phase II capabilities. Such data is much more precise, although wireless carriers generally do not keep it in the ordinary course of business. When the government seeks to compel the provider to disclose this sort of GPS data prospectively, it relies on a warrant. When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department recommends the use of a warrant based on probable cause. Some courts, however, have conflated cell site location information with more precise GPS (or similar) location information.

(2) Appellate jurisdiction for ex parte orders in criminal investigations

A second potential topic for legislation is to clarify the basis for appellate jurisdiction for denials of warrants or other ex parte court orders in criminal or national security investigations. Appellate review serves to clarify the law. Differences among district courts are typically resolved through review by a court of appeals, and the normal way to resolve differences among courts of appeals is through Supreme Court review. But under existing law, the government may have no mechanism to obtain review of the denial of a court order or search warrant, even when the denial is based primarily on questions of law rather than questions of fact.

The lack of clear jurisdiction for appeals of denials of *ex parte* orders in criminal cases has led to some confusion in the federal courts. For example, although there are numerous written opinions from magistrates and district courts on hybrid orders for prospective cell-site information, there remains no appellate authority addressing this issue. Congress could examine this issue further.

(3) Clarifying the standard for issuing 2703(d) orders

A third potentially appropriate topic for legislation is to clarify the standard for issuance of a court order under § 2703(d) of ECPA. ECPA provides that the government can use a court order under § 2703(d) to compel the production of non-content data, such as email addresses, IP addresses, or historical location information stored by providers. These orders can also compel production of some stored content of communications, although compelling content generally requires notice to the subscriber.

According to the statute, "[a] court order for disclosure... may be issued by any court that is a court of competent jurisdiction and shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d).

Until recently, no court had questioned that the United States was entitled to a 2703(d) order when it made the "specific and articulable facts" showing specified by § 2703(d). However, the Third Circuit recently held that because the statute says that a 2703(d) order "may" be issued if the government makes the necessary showing, judges may choose not to sign an application even if it provides the statutory showing. *See In re Application of the United States*, 620 F.3d 304 (3d Cir. 2010). The Third Circuit's approach thus makes the issuance of § 2703(d) orders unpredictable and potentially inconsistent; some judges may impose additional requirements, while others may not. For example, some judges will issue these orders based on the statutory "reasonable grounds" standard, while others will devise higher burdens.

In considering the standard for issuing 2703(d) orders, it is important to consider the role they play in early stages of criminal and national security investigations. In the Wikileaks investigation, for example, this point was recently emphasized by Magistrate Judge Buchanan in the Eastern District of Virginia. In denying a motion to vacate a 2703(d) order directed to Twitter, Judge Buchanan explained that "at an early stage, the requirement of a higher probable cause standard for non-content information voluntarily released to a third party would needlessly hamper an investigation." *In re 2703(d)*, 2011 WL 900120, at *4 (E.D. Va. March 11, 2011).

Other statutes and rules governing the issuance of legal process, such as search warrants and pen/trap orders, *require* a magistrate to issue legal process when it finds that the United States has made the required showing. The Third Circuit's interpretation of § 2703(d), under which a court is free to reject the government's application even when it meets the statutory standard, is at odds with this approach. Legislation could address this issue.

(4) Extending the standard for non-content telephone records to other similar forms of communication

A fourth potential subject for legislation is the standard appropriate for compelling disclosure of addressing information associated with communications, such as email addresses. Traditionally, the government has used a subpoena to compel a phone company to disclose historical dialed number information associated with a telephone call, and ECPA has followed this practice. However, ECPA treats addressing information associated with email and other electronic communications differently from addressing information associated with phone calls. Although an officer can obtain records of calls made to and from a particular phone using a subpoena, "to" and "from" addressing information associated with email can be obtained only with a court order or a warrant. This results in a different level of protection for the same kind of information (e.g. addressing information) depending on the particular technology (e.g. telephone or email) associated with it.

Addressing information associated with email is increasingly important to criminal investigations as diverse as identity theft, child pornography, and organized crime and drug organizations, as well as national security investigations. Moreover, email, instant messaging, and social networking are now more common than telephone calls, and it makes sense to examine whether there is a reasoned basis for distinguishing between the processes used to obtain addressing information associated with wire and electronic communications. In addition, it is important to recognize that addressing information is an essential building block used early in criminal and national security investigations to help establish probable cause for further investigative techniques. Congress could consider whether this is an appropriate area for clarifying legislation.

(5) Clarifying the exceptions in the Pen Register statute

A fifth potential topic of legislation is to clarify the exceptions to the Pen Register statute. The Pen Register statute governs the collection of "dialing, routing, addressing, or signaling information" associated with wire or electronic communications. This information includes phone numbers dialed and "to" and "from" fields of email. In general, the statute requires a court order authorizing such collection on a prospective basis, unless the collection falls within a statutory exception.

It makes sense that a person using a communication service should be able to consent to another person monitoring addressing information associated with her communications. For example, a person receiving threats over the Internet should be able to consent to the government collecting addressing information that identifies the source of those threats. And indeed, the Pen Register statute does contain an exception for use of a pen/trap device with the consent of the user. But there is an issue with the consent provision: it may only allow the use of the pen/trap device by a provider of electronic communication service, not the user or some other party

designated by the user. So in the Internet threats example, the provider is the ISP, not the victim herself or the government. If the provider is unwilling or unable to implement the pen/trap device, even with the user's consent, the statute may prohibit the United States from assisting the victim. Clarifying the Pen Register statute on this point may be appropriate.

(6) Restricting disclosures of personal information by service providers

A sixth potentially appropriate topic for legislation is the disclosure by service providers of customer information for commercial purposes. Under § 2702(c)(6) of ECPA, there are currently no explicit restrictions on a provider disclosing non-content information pertaining to a customer or subscriber "to any person other than a government entity." This approach may be insufficiently protective of customer privacy. Congress could consider whether this rule strikes the appropriate balance between providers and customers.

(7) Provider cost reimbursement

A seventh potential subject for legislation is ECPA's § 2706 cost reimbursement provision. Currently, ECPA does not require the government to pay providers when it obtains "telephone toll records and telephone listings" from a communications common carrier, unless the information obtained is unusually voluminous or burdensome. Other than this narrow category of information, ECPA requires the government to pay providers for producing information under ECPA.

As an initial matter, ambiguity has arisen in the phrase "telephone toll records and telephone listings," as most users now have nationwide calling plans. Some phone service providers claim that because of the billing methods they use, they do not maintain "toll records" or "telephone listings," and thus they seek payment for all compliance with legal process. Legislation could clarify this issue.
In addition, as criminals, terrorists, spies and other malicious actors shift from voice telephone to other types of electronic communications, the category of "telephone toll records and telephone listings," is diminishing in importance. Moreover, the cost to law enforcement to pay providers for responding to subpoenas is substantial. For example, it is not unusual for the United States to be billed $40.00 by a provider merely to produce a customer's name, address, and related identifying information. Congress may wish to consider the extent to which it remains appropriate to require law enforcement agencies to pay for records of non-telephone forms of communication.

(8) Compelled disclosure of the contents of communications

Finally, the eighth and last potentially appropriate topic for legislation is the standard for compelling disclosure of the contents of stored communications. As noted above, we appreciate that there are concerns regarding ECPA's treatment of stored communications – in particular, the rule that the government may use lawful process short of a warrant to obtain the content of emails that are stored for more than 180 days. Indeed, some have argued recently in favor of a

probable cause standard for compelling disclosure of all such content under all circumstances. Because communication services are provided in a wide range of situations, any simple rule for compelled disclosure of contents raises a number of serious public safety questions. In considering whether or not there is a need to change existing standards, several issues are worthy of attention.

First, current law allows for the acquisition of certain stored communications using a subpoena where the account holder receives prior notice. This procedure is similar to that for paper records. If a person stores documents in her home, the government may use a subpoena to compel production of those documents. Congress should consider carefully whether it is appropriate to afford a higher evidentiary standard for compelled production of electronically-stored records than paper records.

Second, it is important to note that not all federal agencies have authority to obtain search warrants. For example, the Securities and Exchange Commission (SEC) and Federal Trade Commission (FTC) conduct investigations in which they need access to information stored as the content of email. Although those entities have authority to issue subpoenas, they lack the ability to obtain search warrants. Raising the standard for obtaining stored email or other stored communications to a search warrant could substantially impair their investigations.

Third, Congress should recognize the collateral consequences to criminal law enforcement and the national security of the United States if ECPA were to provide only one means – a probable cause warrant – for compelling disclosure of all stored content. For example, in order to obtain a search warrant for a particular email account, law enforcement has to establish probable cause to believe that evidence will be found in that particular account. In some cases, this link can be hard to establish. In one recent case, for example, law enforcement officers knew that a child exploitation subject had used one account to send and receive child pornography, and officers discovered that he had another email account, but they lacked evidence about his use of the second account.

Thus, Congress should consider carefully the adverse impact on criminal as well as national security investigations if a probable cause warrant were the only means to obtain such stored communications.

* * *

In conclusion, these topics appear appropriate for further clarification or legislation, but I want to emphasize that Congress should take care not to disrupt the current balance of interests that is reflected in ECPA. ECPA is complex because our nation's communications systems are complex, and because governing the government's access to that system must resolve competing interests between privacy, innovation, international competitiveness, public safety and the national security in many different contexts. When making changes to ECPA, public safety, national security, and legitimate privacy interests must not be compromised.

The Department of Justice stands ready to work with the Committee as it considers whether changes to ECPA are called for. But we urge Congress to proceed with caution. Congress must protect privacy and foster innovation, but it also should refrain from making changes that would unduly impair the government's ability to obtain critical information necessary to build criminal, national security, and cyber investigations.

Law enforcement agents and prosecutors have extensive experience with actual application of ECPA, and this experience can serve as an important resource in evaluating the tangible impact of changes to ECPA. We appreciate the opportunity to discuss this issue with you, and we look forward to continuing to work with you.

This concludes my remarks. I would be pleased to answer your questions.

PATRICK J. LEAHY, VERMONT, CHAIRMAN

HERB KOHL, WISCONSIN
DIANNE FEINSTEIN, CALIFORNIA
CHARLES E. SCHUMER, NEW YORK
RICHARD J. DURBIN, ILLINOIS
SHELDON WHITEHOUSE, RHODE ISLAND
AMY KLOBUCHAR, MINNESOTA
AL FRANKEN, MINNESOTA
CHRISTOPHER A. COONS, DELAWARE
RICHARD BLUMENTHAL, CONNECTICUT

CHARLES E. GRASSLEY, IOWA
ORRIN G. HATCH, UTAH
JON KYL, ARIZONA
JEFF SESSIONS, ALABAMA
LINDSEY O. GRAHAM, SOUTH CAROLINA
JOHN CORNYN, TEXAS
MICHAEL S. LEE, UTAH
TOM COBURN, OKLAHOMA

United States Senate
COMMITTEE ON THE JUDICIARY
WASHINGTON, DC 20510-6275

BRUCE A. COHEN, *Chief Counsel and Staff Director*
KOLAN L. DAVIS, *Republican Chief Counsel and Staff Director*

April 12, 2011

The Honorable Lanny Breuer
Assistant Attorney General
Criminal Division
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530

Dear Assistant Attorney General Breuer:

This month, two independent events underscored our nation's need for stronger digital privacy protections. On Friday, April 1, one of the nation's largest digital marketing companies, Epsilon Data Management, LLC, announced that hackers had breached their security systems and stolen millions of consumers' email addresses. The following Monday, public securities filings revealed what appears to be an investigation by the U.S. Attorney's Office of New Jersey into allegations that certain smartphone applications were collecting sensitive consumer information and disclosing it to third parties unbeknownst to consumers. This information ranged from users' phone numbers to their friends lists to their geographic location. The alleged conduct in both cases will likely be investigated under a single statute called the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030. *See* Amir Efrati, Scott Thurm and Dionne Searcey, Mobile-App Makers Face U.S. Privacy Investigation, *The Wall Street Journal*, April 5, 2011.

These allegations raise broad questions about the need to better protect Americans' digital information and give them greater awareness and control over that information. They also highlight potential ambiguities and limitations of the CFAA which create uncertainties for industry and limit safeguards for consumers. In light of these incidents, we are writing to ask that you do everything possible to ensure that this specific statute is enforced effectively and transparently. Specifically, we ask that you clarify the Department's understanding of the scope of the CFAA's consumer protection provisions, update the Department's prosecutorial guidance for the statute, and indicate to us where additional funding or legislation may be needed.

First, while the hacking of Epsilon would appear to be a clear violation of the CFAA, the application of that statute can be ambiguous in other circumstances. In addition to covering outsider hacking activities, the CFAA also covers situations where an insider who already has access to a computer "exceeds authorized access" to obtain information from that computer. Where there is a privacy policy, employee contract, or other document laying out the scope of an individual or entity's authorization to access a computer, courts have found it easy to determine whether someone has exceeded their authorized access and violated the CFAA. *See, e.g. EF Cultural Travel BV v. Explorica*, 274 F.3d 577 (1st Cir. 2001) (defining scope of authorization based on a confidentiality agreement).

But where there *isn't* a document clearly laying out the scope of authorization, the law is more unclear. As the Department itself has acknowledged, federal circuits are split on the question of whether limits on authorized access can be inferred from the relationship between the user and the entity accessing the user's computer. *Compare EF Cultural Travel BV v. Zefer Corp.*, 318 F.3d 58 (1st Cir. 2003) (refusing to limit authority based on "reasonable expectations" test), *with United States v. Phillips*, 477 F.3d 215, 219 (5th Cir. 2007) ("Courts have... typically analyzed the scope of a user's authorization to access a protected computer on the basis of the expected norms of intended use or the nature of the relationship established between the computer owner and the user."). Because many smartphone apps lack privacy policies, many of the applications being investigated by the U.S. Attorney's Office may fall into this legal gray area.

We write to ask the Department to clarify how it determines the scope of authorization under the CFAA in the absence of a written policy or agreement addressing the issue. We further ask that the Department communicate this interpretation to consumers, prosecutors, and industry stakeholders. We believe that a clear statement on the application of the CFAA in these circumstances will help consumers know their rights, help industry develop new products and services, and help law enforcement take action against bad actors.

Second, we also think it is important for all prosecutors to be aware that the Computer Fraud and Abuse Act protects more than traditional desktop and laptop computers. The definition of "computer" in the CFAA is a broad one and the U.S. Court of Appeals for the Eighth Circuit recently reaffirmed that the CFAA protects smartphones and a broad range of other electronic devices. *See U.S. v. Kramer*, 2011 WL 383710 (8th Cir. 2011). We ask that the Department update its *Prosecuting Computer Crimes* manual to reflect this recent federal court precedent. Establishing that the CFAA covers smartphones and other electronic devices will help U.S. Attorneys and Department officials recognize and stop violations of the CFAA's modest protections.

Finally, we write to ask how we as the Senate can help you enforce this critical protection of Americans' security and privacy. Does the CFAA require updating in light of the Epsilon breach and the smartphone app allegations? Are there other areas of the law that should be enhanced to better protect digital privacy? Does the Computer Crime and Intellectual Property Section have the resources it needs to protect Americans from online criminals?

Your work is critical to Americans' digital privacy. We welcome the opportunity to support you in this important endeavor.

Sincerely,

Al Franken
United States Senator

Richard Blumenthal
United States Senator

AL FRANKEN
MINNESOTA

SUITE
SH-320
202-224-5641

United States Senate

WASHINGTON, DC 20510-2309

April 20, 2011

Mr. Steve Jobs
1 Infinite Loop
Cupertino, CA, 95014

Dear Mr. Jobs,

I read with concern a recent report by security researchers that Apple's iOS 4 operating system is secretly compiling its customers' location data in a file stored on iPhones, 3G iPads, and every computer that users used to "sync" their devices. According to the researchers, this file contains consumers' latitude and longitude for every day they used an iPhone or 3G iPad running the iOS 4 operating system—sometimes logging their precise geo-location up to 100 times a day. The researchers who discovered this file found that it contained up to a year's worth of data, starting from the day they installed the iOS 4 operating system. What is even more worrisome is that this file is stored in an unencrypted format on customers' iPads, iPhones, and every computer a customer has used to back up his or her information. *See* Alasdair Allen & Pete Warden, *Got an iPhone or 3G iPad? Apple is Recording Your Moves* (Apr. 20, 2011), *available at* http://radar.oreilly.com/2011/04/apple-location-tracking.html.

The existence of this information—stored in an unencrypted format—raises serious privacy concerns. The researchers who uncovered this file speculated that it generated location based on cell phone triangulation technology. If that is indeed the case, the location available in this file is likely accurate to 50 meters or less. *See* Testimony of Michael Amarosa, Before the House Judiciary Committee, Subcommittee on the Constitution, Civil Rights and Civil Liberties, June 24, 2010 at page 7 *available at* http://judiciary.house.gov/hearings/pdf/Amarosa100624.pdf. Anyone who gains access to this single file could likely determine the location of a user's home, the businesses he frequents, the doctors he visits, the schools his children attend, and the trips he has taken—over the past months or even a year. *Cf. People v. Weaver*, 909 N.E.2d 1195, 1199-1200 (N.Y. 2009) ("What this technology yields and records with breathtaking quality and quantity is a highly detailed profile, not simply of where we go, but by easy inference, of our associations … and of the pattern of our professional and avocational pursuits.").

Moreover, because this data is stored in multiple locations in an unencrypted format, there are various ways that third parties could gain access to this file. Anyone who finds a lost or stolen iPhone or iPad or who has access to any computer used to sync one of these devices could easily download and map out a customer's precise movements for months at a time. It is also entirely conceivable that malicious persons may create viruses to access this data from customers' iPhones, iPads, and desktop and laptop computers. There are numerous ways in which this information could be abused by criminals and bad actors. Furthermore, there is no indication that this file is any different for underage iPhone or iPad users, meaning that the millions of children and teenagers who use iPhone or iPad devices also risk having their location

collected and compromised. An estimated 13% of the 108 million iPhones and 19 million iPad devices sold are used by individuals under the age of 18, although some of these devices may not have been upgraded to iOS 4. *See* AdMob, *AdMob Mobile Metrics Report* at 5 (Jan. 2010), *available at* http://metrics.admob.com/wp-content/uploads/2010/02/ AdMob-Mobile-Metrics-Jan-10.pdf; Complaint of Apple Inc. v. Samsung Electronics, CV-11-1846 at 4-5 (N.D. Cal. Apr. 15, 2011).

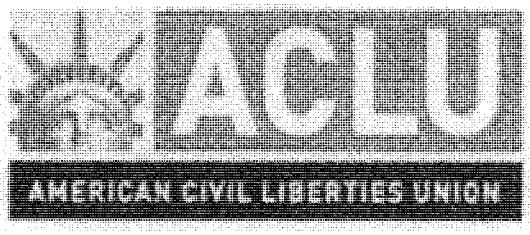
These developments raise several questions:

1. Why does Apple collect and compile this location data? Why did Apple choose to initiate tracking this data in its iOS 4 operating system?
2. Does Apple collect and compile this location data for laptops?
3. How is this data generated? (GPS, cell tower triangulation, WiFi triangulation, etc.)
4. How frequently is a user's location recorded? What triggers the creation of a record of someone's location?
5. How precise is this location data? Can it track a user's location to 50 meters, 100 meters, etc.?
6. Why is this data not encrypted? What steps will Apple take to encrypt this data?
7. Why were Apple consumers never affirmatively informed of the collection and retention of their location data in this manner? Why did Apple not seek affirmative consent before doing so?
8. Does Apple believe that this conduct is permissible under the terms of its privacy policy? *See* Apple Privacy Policy at "Location-Based Services" (accessed on April 20, 2011), *available at* www.apple.com/privacy.
9. To whom, if anyone, including Apple, has this data been disclosed? When and why were these disclosures made?

I would appreciate your prompt response to these questions and thank you for your attention to this matter.

Sincerely,

Al Franken
United States Senator



Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director
ACLU Washington Legislative Office

Christopher Calabrese
Legislative Counsel
ACLU Washington Legislative Office

Catherine Crump
Staff Attorney
ACLU Speech, Privacy and Technology Project

before the
Senate Judiciary Committee
Subcommittee on Privacy, Technology

May 10, 2011

Hearing on
Protecting Mobile Privacy: Your Smartphones, Tablets,

Cell Phones and Your Privacy

WASHINGTON LEGISLATIVE OFFICE
915 15th Street, NW Washington, D.C. 20005
(202) 544-1681 Fax (202) 546-0738

Chairman Franken, Ranking Member Coburn, and Members of the Committee:

The American Civil Liberties Union (ACLU) has more than half a million members, countless additional activists and supporters, and fifty-three affiliates nationwide. We are one of the nation's oldest and largest organizations advocating in support of individual rights in the courts and before the executive and legislative branches of government. In particular, throughout our history, we have been one of the nation's foremost protectors of individual privacy. We write today to applaud the committee for its focus on the privacy issues in mobile technologies and to describe the particular need for reform in the use of location tracking information by law enforcement.

While the increased use of smart phones raises a number of privacy issues it is imperative that the committee keep as a central focus law enforcement access to location information. Specifically that all such access should require a warrant issued by a court based on probable cause.

Unregulated location tracking poses a real, immediate, and universal danger to Americans' privacy. Because of the prevalence of mobile phones in modern society, every American is carrying a portable tracking device, one that can be used to reveal his or her current and past location. Whether it is a visit to a therapist or liquor store, church or gun range, many individuals' locations will be available either in real time or months later. Recent reports showing the extent to which Apple iPhones and smartphones running Google's Android operating system have been tracking and storing their users' location information were shocking to many and have created a public outcry. However we cannot focus on these two companies alone. Location tracking practices are widespread and fundamental to the provision of mobile communications services. Because of the sensitivity and invasiveness of location records, law enforcement agents should always be required to obtain a judicially-authorized warrant and show probable cause, no matter the technology employed or the age of the records.

Unfortunately, the government frequently obtains location tracking information without first obtaining a warrant and establishing probable cause. Law enforcement has obtained location information since at least the late 1990's[1] but more than a decade later we still have no uniform standard for when law enforcement can access to this information. While the Department of Justice (DOJ) has issued recommendations setting out when prosecutors should

[1] *See, e.g. United States v. Cell Site*, Case No. 99-00162 (S.D. Tex. Feb. 10, 1999); *United States v. Cell Site Info*, Case No. 00-02871 (S.D. Fl. May 28, 1999).

show probable cause, United States Attorneys are apparently free to ignore these recommendations, and some have chosen to do so. Worse the government seems to have engaged in a coordinated effort to prevent the creation of a uniform standard by refusing to seek appellate court decisions on the issue. This legal maneuvering has prevented public debate and allowed the entrenchment of a practice inconsistent with our constitutional principles.

Congress is the only branch of government that is well-positioned to ensure a respect for privacy in the face of new mobile tracking technologies. The Executive Branch has proven itself unwilling to show probable cause. The courts are not well-equipped to do so because the government chooses not to appeal lower court decisions, thereby frustrating development of the law. Accordingly, Congress must act. While some of the technical details are complicated, the principle is simple: almost every American is carrying a portable tracking device and if Americans are to continue enjoying a robust right of privacy, Congress should update the Electronic Communications Privacy Act (ECPA) to clarify that the government must obtain a warrant based on a showing of probable cause to track these devices.

Current Location Technology

As of December 2010, there were an estimated total of 302 million cell phone service subscribers in the United States.[2] Whenever these subscribers have their cell phones on, the phones automatically scan for the cell tower and the sector of that tower that provides the best reception and, approximately every seven seconds, the phones register their location information with the network.[3] The carriers keep track of the registration information in order to identify the cell tower through which calls can be made and received. The towers also monitor the strength of the telephone's signal during the progress of the call, in order to manage the hand-off of calls from one adjacent tower to another if the caller is moving during the call.[4]

The cell phone technology yields several types of location information of interest to law enforcement officers. The most basic type of data is "cell site" data, or "cell site location information," which refers to the identity of the cell tower from which the phone is receiving the strongest signal at the time and the sector of the tower facing the phone.[5] This data is less accurate because it relies on simple proximity to a cell phone tower so it can be anywhere from a

---

[2] *See* CTIA The Wireless Association, *CTIA's Semi-Annual Wireless Industry Survey* (2010) at 5, *available at http://files.ctia.org/pdf/CTIA_Survey_Year_End_2010_Graphics.pdf.*

[3] *See In the Matter of the Application of the United States of America for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 534 F. Supp. 2d 585, 589-90 (W.D. Pa. 2008) (Lenihan, M.J.), *aff'd*, No. 07-524M, 2008 WL 4191511 (W.D. Pa. Sept. 10, 2008), *appeal docketed*, No. 08-4227.

[4] *See* Decl. of Henry Hodor at 7 n.6, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_release_4805_001_20091022.pdf The Hodor Declaration offers a technical overview of how cell tracking is accomplished. The ACLU obtained it pursuant to an ongoing Freedom of Information Act lawsuit that it filed with the Electronic Frontier Foundation to access records related to the government's use of cell phone tracking. *See ACLU v. DOJ*, No. 08-1157 (D. D.C. filed July 1, 2008).

[5] *See, e.g.*, *In the Matter of the Application of the United States of America for an Order Authorizing the Disclosure of Prospective Cell Site Information*, 412 F. Supp. 2d 947, 948-49 (E.D. Wis. 2006) (Callahan, M.J.); *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827 (S.D. Tex. 2006) (Smith, M.J.).

200 meter to 30 kilometer (656 feet to 18 miles) radius from the tower.[6] This range is shrinking, as the number of active cellular towers is increasing by 11.5 % each year.[7] Currently some cell sites only cover limited areas, such as tunnels, subways, and specific roadways.[8] Further improvement in precision can be expected given the explosive demand for wireless technology and its new services, to the point that "[t]he gap between the locational precision in today's cellular call detail records and that of a GPS tracker is closing, especially as carriers incorporate the latest technologies into their networks."[9]

Beyond basic cell site location information, cellular service providers have the capacity and the obligation under the Wireless Communications and Public Safety Act of 1999 to create and disclose even more precise location information for E911 calls.[10] Cell phone providers generate this data in two ways. First, under the "network-based approach," the providers triangulate information regarding the strength of the signals from the cellular towers nearest to the phone.[11] Under Federal Communications Commission (FCC) guidelines, this information must be accurate within 100 meters for 67% of calls and within 300 meters for 95% of calls by 2012.[12]

The second approach is to track the location of the cell phone using its GPS capabilities.[13] The FCC requires the GPS to be accurate within 50 meters for 67% of calls and within 150 meters for 95% of calls by 2012.[14] This GPS is often much more accurate, frequently within a few meters.[15]

The recent reports of Google's and Apple's location tracking practices show the detail of information companies are capable of collecting. Security analyst Samy Kamkar found that an HTC Android phone collected location information every few seconds and transmitted the data to Google at least several times an hour.[16] In addition to the location, the phone was transmitting the name, location and signal strength of nearby Wi-Fi networks and a unique phone identifier. Apple says it "intermittently" collects location data, including Wi-Fi networks and transmits that data to itself every 12 hours. It was impossible to disable the tracking file on iPhone even when disabling location services. [17]

---

[6] But sometimes, depending on topography or other impediments to transmission, a phone receives the strongest signal from a cellular tower other than the one that is closest to it. Hodor Decl., *supra*, at 7-8.
[7] *See* CTIA, *supra*, at 9.
[8] *See* Thomas Farley and Ken Schmidt, *Cellular Telephone Basics: Basic Theory and Operation*, http://www.privateline.com/mt_cellbasics/iv_basic_theory_and_operation/ (last accessed Dec. 21, 2009).
[9] Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services Before the Subcomm. on the Constitution, Civil Rights, and Civil Liberties of the H. Comm. on Judiciary, 111th Cong. (2010) (statement of Professor Matt Blaze at 13-14), http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf (hereinafter, "Blaze testimony").
[10] Pub. L. No. 106-81, 113 Stat. 1286 (1999)
[11] *See* Note, *Who Knows Where You've Been? Privacy Concerns Regarding the Use of Cellular Phones as Personal Locators*, 18 Harv. J. L. & Tech. 307, 308-10 (2004); *See, e.g.*, *In re Application for Pen Register and Trap/Trace Device with Cell Site Location Authority*, 396 F. Supp. 2d 747, 749-51 (S.D. Tex. 2005) (Smith, M.J.).
[12] 47 C.F.R. § 20.18(h)(1)(i).
[13] *See Who Knows Where You've Been?*, *supra*, at 308.
[14] 47 C.F.R. § 20.18(h)(1)(ii).
[15] Mario Aguilar, *GPS Power-Up: Get Ready for New Sense of Place*, Wired, April 19, 2010
[16] Valetino-Devries, Jennifer, *IPhone Stored Location in Test Even if Disabled*, Wall Street Journal, April 25, 2011
[17] *Id.*

In addition some of the most popular "apps" are selling users' personal information including GPS location to third parties. Earlier this year the popular online radio service Pandora, received a subpoena from a federal grand jury investigating whether they were sharing information about their users with advertisers and other third parties. Last month the Wall Street Journal reported that 47 apps transmitted the phone's location in some way.[18]

This tracking is likely to become even more accurate in the near future. As discussed above, the number of cell towers is increasing rapidly.[19] Furthermore, "[GPS] technology is rapidly improving so that any person or object . . . maybe tracked with uncanny accuracy to virtually any interior or exterior location, at any time and regardless of atmospheric conditions."[20]

Current Legal Practices for Accessing Location Information

Unfortunately, it remains unclear under what circumstances federal prosecutors obtain a warrant and show probable cause to access cell phone location information, and under what circumstances courts have held that this is the legal minimum showing and process required under the law. Although DOJ has issued guidelines for prosecutors that require probable cause in some circumstances, these are not consistently followed. Because the vast majority of judicial decisions on point are sealed, and those limited number that are public are in conflict, the state of the law is unclear. Federal prosecutors generally decline to appeal adverse rulings to circuit courts. Clarity is unlikely anytime soon unless Congress acts.

Department of Justice Standards

The Department of Justice asserts it should have access to most kinds of location information without having to obtain a warrant and show probable cause. Instead, DOJ argues that the government should be able to obtain most cell phone location information by demonstrating to a judge or magistrate only that the information is relevant and material to an ongoing criminal investigation. According to testimony before this committee and a document obtained by the ACLU and the Electronic Frontier Foundation (EFF) through a FOIA request, it is DOJ's policy to obtain mobile location information under the following standards:[21]

	Historical Records	**Real-time Surveillance**
Cell-site data	Relevant and material	Relevant and material

[18] Efrati, Thurm, and Searcey, *Mobile-App Makers Face U.S. Privacy Investigation*, Wall Street Journal, April 5, 2011

[19] *See* CTIA, *supra*, at 9.

[20] *People v. Weaver*, 12 N.Y.3d 433, 441 (N.Y. 2009).

[21] Mark Eckenweiler, *Current Legal Issues In Phone Location*, slide 20, *available at* http://www.aclu.org/pdfs/freespeech/18cellfoia_release_CRM-200800622F_06012009.pdf and U.S. Congress, Hearing of the Senate Judiciary Committee, The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, Written Statement of Associate Deputy Attorney General James A. Baker, April 6, 2011.

GPS, triangulation	N/A (because usually doesn't exist)	Probable cause

According to internal DOJ documents, the Department maintains that the government need not obtain a warrant and show probable cause to track people's location with only one exception: real-time GPS and triangulation data. Since at least 2007, DOJ has recommended that U.S. Attorneys around the country obtain a warrant based on probable cause prior to engaging in these forms of cell phone tracking.[22]

In testimony before this Committee, DOJ has amplified that position by saying: "When prosecutors seek to obtain prospective E-911 Phase II geolocation data (such as that derived from GPS or multilateration) from a wireless carrier, the Criminal Division of the Justice Department **recommends** the use of a warrant based on probable cause" (emphasis added).[23] Focusing attention on the word 'recommends' is critical because not all U.S. Attorneys' offices obtain a warrant and show probable cause even in the limited circumstances in which DOJ recommends that they do so.[24] The ACLU's and EFF's FOIA litigation revealed that U.S. Attorneys' offices in the District of New Jersey and the Southern District of Florida have obtained even the most precise cell tracking information without obtaining a warrant and showing probable cause.[25] Because the FOIA focused on only a small number of U.S. Attorneys' offices around the country, it may well be that many other offices also do not follow DOJ's recommendation.

In fact, this practice may be widespread. There are no published legal opinions on the lawfulness of warrantless cell phone tracking in either the District of New Jersey or the Southern District of Florida, and yet the FOIA litigation proved conclusively that cell phone tracking occurs in those districts and indeed that federal prosecutors do not feel obligated to show probable cause even where DOJ recommends it. In the vast majority of judicial districts in this country, there are no decisions addressing cell phone tracking, yet cell phone tracking was occurring in every district subject to the FOIA, even where there is no published opinion setting out the circumstances in which the practice is permissible.[26] Given that cell phone tracking is now a decades-old law enforcement technique that has proven useful, we must assume authorities use it in all or essentially all parts of the country, most frequently under an unknown standard.

Procedures for Gathering Location Information

---

[22] Email from Brian Klebba, *GPS or "E-911-data" Warrants*, November 17, 2009, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_dojrecommendation.pdf.

[23] U.S. Congress, Hearing of the Senate Judiciary Committee, The Electronic Communications Privacy Act: Government Perspectives on Protecting Privacy in the Digital Age, Written Statement of Associate Deputy Attorney General James A. Baker, April 6, 2011.

[24] Letter from William G. Stewart II, to ACLU, *Mobile Phone Tracking (Items 3-5)/DNJ*, Dec. 31, 2008, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074132_12312008.pdf; Letter from William G. Stewart II to Catherine Crump, *Mobile Phone Tracking(Items 3-5)FLS*, Dec. 31, 2008, *available at* http://www.aclu.org/pdfs/freespeech/cellfoia_released_074135_12312008.pdf.

[25] *Id.*

[26] http://www.aclu.org/free-speech/aclu-lawsuit-uncover-records-cell-phone-tracking

The reason there is so little information available arises in part from the unique procedural posture in which cell phone tracking applications reach courts. For legitimate reasons, applications to track cell phones are often filed under seal. Law enforcement agents sometimes need to prevent the targets of government surveillance from learning that they are investigative subjects.

However, the orders granting or denying surveillance applications also are often also filed under seal, routinely with the notation "until further order of the Court."[27] Because there is no end date on sealing, and no one other than the government and court know the contents of the order, in most cases there is no one with both the motivation and the knowledge to move to unseal them. Public access to the courts would be better served were judges to require that redacted copies of both the applications and orders be filed publicly. This would allow the public to know the legal standards applied by the courts.

This is an unfortunate break with the usual working of the judiciary, where a commitment to transparency is not only embodied in the common law right of access but also constitutionally required by the First Amendment.[28] Some magistrate judges such as the Honorable Stephen Wm. Smith, who has testified before Congress on the issue, are notable exceptions to this trend. Judge Smith has issued an opinion putting an end to indefinite sealing of the surveillance orders he is called upon to issue.[29]

Ex parte adjudication of cell phone tracking applications also contributes to the dearth of published legal opinions on the subject. Ex parte proceedings – when the government presents its arguments in favor of surveillance without presentation of any opposing argument – will favor unpublished decisions because there is no motivation for the only party present, the government, to ask the court to issue a public decision. The ACLU and others have tried to remedy the situation by offering to submit amicus briefs to present the pro-privacy viewpoint. Unfortunately, because many applications for surveillance are so time-sensitive that they must be acted on immediately, some judges have taken the position that there is unlikely to be a practical way to permit amicus participation.[30]

Reaction from the Judiciary

From the few published opinions available, it is apparent that courts do not always find in favor of the government position that it need not obtain a warrant based on probable cause for some forms of cell phone tracking. In fact, the government frequently loses. A "strong majority" of district and magistrate judges have concluded in recently published opinions that the government lacks statutory authority to obtain real-time cell site location without a showing of

---

[27] *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 878 (S.D. Tex. 2008) (Smith, J.)

[28] *Press-Enterprise Co. v. Superior Court of California*, 478 U.S. 1, 8 (1986)

[29] *In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders*, 562 F. Supp. 2d 876, 891 (S.D. Tex. 2008) (Smith, J.) (holding that "documents authored or generated by the court itself" are entitled to heightened public access rights)

[30] *See, e.g.*, Letter from Hon. David Martin and Hon. Lincoln Almond to ACLU, *Cell phone tracking*, Mar. 12, 2010 (on file with author).

probable cause.[31] Because the government has never followed through on an appeal of an adverse decision addressing real-time tracking, no circuit court has had the opportunity to review these holdings.

The government did appeal an adverse decision addressing historical information. In a decision joined by all of the magistrate judges in the Western District of Pennsylvania, a magistrate judge there held that government requests for court orders requiring mobile carriers to disclose their customers' location information must be based upon probable cause.[32] After the decision was summarily affirmed by the district court, the government appealed to the Third Circuit. In a decision issued this month, the circuit concluded that judges have "the option to require a warrant showing probable cause," although it cautioned that "it is an option to be used sparingly."[33]

Until the action by the magistrate judges in the Western District of Pennsylvania forced the government's hand – by making it impossible to get an order under the "relevant and material" standard in that district –a location tracking case had never been appealed to the appellate court in any circuit. By not appealing, federal prosecutors avoid binding precedent which might tie the government's hands in further cases.[34] Decisions by magistrate judges and district court judges are not binding precedent, even on other judges of the same district court.[35] So long as there are at least some judges in a district who believe that warrantless cell phone tracking is permissible, the government will be able to get its applications approved at least some of the time.

This is exactly the situation in the Southern District of New York, where one district court judge has approved warrantless real-time cell phone tracking in the absence of probable cause and another has held that probable cause is required.[36] Although the government initially filed a notice of appeal with regard to the adverse ruling, after the ACLU received permission to submit an amicus brief in the Second Circuit, the government sought and obtained multiple extension requests and then voluntarily dismissed its appeal.[37] Judges in the Eastern District of

---

[31] *In re Applications of the United States of America for Orders Pursuant to Title 18, United States Code, Section 2703(d)*, 509 F. Supp. 2d 76, 78 (D. Mass. 2007) (Stearns, D.J.).

[32] *In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, 534 F.Supp.2d 585, 585-86 (W.D. Pa. 2008).

[33] *In The Matter Of The Application Of The United States Of America For An Order Directing A Provider Of Electronic Communication Service To Disclose Records To The Government*, No. 08-4227, ___F.3d ___ (3d Cir. Sept. 7, 2010).

[34] *In the Matter of the Application of the United States of America for an Order Authorizing (1) Installation and Use of a Pen Register and Trap and Trace Device or Process, (2) Access to Customer Records, and (3) Cell Phone Tracking*, 441 F. Supp. 2d 816, 827-28 (S.D. Tex. 2006) (Smith, M.J.).

[35] *Federal Trade Commission v. Tariff*, 584 F.3d 1088, 1092 (D.C. Cir. 2009).

[36] *Compare In re: Application of the United States of America for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone*, 460 F. Supp. 2d 448 (S.D.N.Y. 2006) (Kaplan, D.J.) *with In the Matter of an Application of the United States of America for an Order Authorizing the Use of a Pen Register With Caller Identification Device Cell Site Location Authority on a Cellular Telephone*, 2009 WL 159187 (S.D.N.Y. 2009) (McMahon, D.J.).

[37] *In re application for a cell site order*, Case No. 09-0807 (2d Cir. docketed Feb. 27, 2009).

New York also split on the question, and only prosecutors and the courts know how this issue is handled in the majority of the country where there are no published opinions.[38]

The state of the law regarding cell phone tracking is characterized by secrecy and contradictory rulings. This is precisely the opposite of the uniformity and openness that are cornerstones of the rule of law in the United States.

Resulting Harms

In addition to frustration and lack of transparency, this low legal standard has already led to misuse by law enforcement. A recent *Newsweek* article highlighted the problem:

> Some abuse has already occurred at the local level, according to telecom lawyer Gidari. One of his clients, he says, was aghast a few years ago when an agitated Alabama sheriff called the company's employees. After shouting that his daughter had been kidnapped, the sheriff demanded they ping her cell phone every few minutes to identify her location. In fact, there was no kidnapping: the daughter had been out on the town all night. A potentially more sinister request came from some Michigan cops who, purportedly concerned about a possible "riot," pressed another telecom for information on all the cell phones that were congregating in an area where a labor-union protest was expected.[39]

It is likely that these examples are the simply the tip of the iceberg. As described extensively above, much of this tracking is happening in secret and for the most part the parties involved don't have any incentive to draw attention to it: law enforcement wants to limit discussion of their investigatory techniques and telecommunications carriers are afraid of spooking their customers.

In addition to abuse, location tracking has also led to the creation of an entire surveillance apparatus, much of it outside the public view. It came to light last year that:

> Sprint Nextel has even set up a dedicated Web site so that law-enforcement agents can access the records from their desks—a fact divulged by the company's "manager of electronic surveillance" at a private Washington security conference last October. "The tool has just really caught on fire with law enforcement," said the Sprint executive, according to a tape made by a privacy activist who sneaked into the event.[40]

This allows detailed disclosure of an individual's movements to law enforcement with a click of a mouse.

---

[38] *Compare* 396 F. Supp. 2d 294 (E.D.N.Y. 2005) (Orenstein, M.J.) (probable cause for prospective tracking) *and* 2009 WL 1530195 (E.D.N.Y. 2009) (Pollak, M.J.), (probable cause for prospective tracking, reversed by Judge Garaufis) *with* 2009 WL 1594003 (E.D.N.Y. 2009) (Garaufis, D.J.) (no probable cause necessary for prospective tracking).

[39] Michael Isikoff, *The Snitch in Your Pocket*, Newsweek, Feb. 19, 2010.

[40] *Id.*

In the most recent example, the ACLU and EFF filed an amicus brief last year in the case of *U.S. v. Soto*.[41] The FBI sought and received tracking information without a warrant, not just for the criminal defendant, but for *about 180 other people*. Because the government's surveillance application is apparently under seal, the details remain unclear. But it appears that the government took the dragnet approach of getting location information for a large number of innocent people in order to figure out the very small number of people who were involved in the underlying crime.

This is even more troubling in light of the FBI policy on record retention. This exchange is from FBI Director Robert Mueller's appearance before an oversight hearing of the House Judiciary Committee in May 2009:

> Mr. NADLER. You keep for 20 years information about innocent people, private information that you have collected in the course of an investigation in which it turns out they had nothing to do with.
> Mr. MUELLER. We may well undertake an—an allegation may come in as to the involvement of a person in a mortgage fraud scheme. We go and investigate, find that that person is innocent, the allegation is false, we keep those records, yes.[42]

So the collection of the movements and habits of innocent people – regardless that it has no bearing on a criminal investigation - will remain part of an FBI profile for 20 years.

The mass tracking in *Soto* is not an isolated incident of overreaching by the FBI. It is just one manifestation of the "communities of interest" approach the government has adopted to tracking down criminals. According to Albert Gidari's testimony before the House Judiciary Committee last year:

> The following issues are faced by service providers every day in response to government demands for acquisition and use of location Information:
>
> ...
>
> d. Target v. Associates (hub and spokes). Regardless of the legal standard applicable to the target phone, what standard applies to obtain the location information for all those with whom the target communicates? **It is common in hybrid orders for the government to seek the location of the community of interest – that is, the location of persons with whom the target communicates** (emphasis added). [43]

---

[41] Brief of Amici Curiae in Support of Motion To Suppress, *United States v. Soto*, Case No. 09-cr-200 (D. Conn. June 18, 2010), *available at* http://www.aclu.org/files/assets/2010-6-18-USvSoto-AmiciBrief.pdf.

[42] *Federal Bureau of Investigation: Hearing Before the H. Judiciary Comm.*, 111th Cong. 35-36 (2009) (statement of Robert Mueller, Director, FBI).

[43] *Electronic Communications Privacy Act Reform: Hearing Before the Subcomm. on the Constitution, Civil Rights and Civil Liberties*, 111th Cong. (2010) (statement of Albert Gidari, Partner, Perkins Coie LLP).

This type of mass, generalized surveillance raises the prospect that the movements and habits of many innocent people are tracked and stored for decades.[44]

Conclusion

It has been, and continues to be, the practice of the government to obtain very private and sensitive information based on a very low legal standard – relevance and materiality – and, at least in the case of the FBI, to store it for decades. The government has gone to great lengths to preserve this authority, even to the extent of giving up the power in particular cases, in order to continue to submit secret motions in jurisdictions around the country.

The information in question reveals individual movements for months or years and potentially reveals personal information across a broad range of subjects from medical information (visits to a therapist or an abortion clinic) to First Amendment protected activity (attendance at a church or political protest) to personal habits (visits to a gun range or bar).

There is a compelling need for Congress to act in this case. It must amend ECPA in order to move from a confusion of legal standards that serve the American public very poorly to a uniform probable cause standard which respects the intent of the Founding Fathers and the Fourth Amendment.

[44] It may be that the problem is actually *worse* than described here. In a report on the misuse of exigent letters the Department of Justice Inspector General describes widespread requests for community of interest information. Apparently it was part of "boilerplate" request language for at least some National Security Letters. *A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records*, Inspector General, Department of Justice, January 2010 at 56. Further according to an Office of Legal Counsel opinion there may be some telephone records that the FBI can access without any process under ECPA. *Id.* at 264.

Additional Documents for the Record
From Senator Al Franken
Following the Senate Judiciary Committee Hearing on:
"Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy"
May 10, 2011

In the interest of efficiency, the following documents, which are lengthy, are incorporated by reference into the record:

1. Time Warner Telecom, Inc. v. F.C.C., 507 F.3d 205 (3d Cir. 2007).

2. In re Applications of U.S. for Orders Pursuant to Title 18, U.S. Code, Section 2703(d), 509 F.Supp.2d 76 (D. Mass. 2007).

3. In the Matter of Appropriate Regulatory Treatment for Broadband Access to the Internet over Wireless Networks, 22 F.C.C.R. 5901 (2007).

Android phones keep location cache, too, but it's harder to access

By Chris Foresman | Published 25 days ago

After this week's disturbing revelation that iPhones and 3G iPads keep a log of location data based on cell tower and WiFi base station triangulation, developer Magnus Eriksson set out to demonstrate that Android smartphones store the exact same type of data for its location services. While the data is harder to access for the average user, it's as trivial to access for a knowledgeable hacker or forensics expert.

On Wednesday, security researchers Alasdair Allan and Pete Warden revealed their findings that 3G-capable iOS devices keep a database of location data based on cell tower triangulation and WiFi basestation proximity in a file called "consolidated.db." The iPhone, as well as 3G-equipped iPads, generate this cache even if you don't explicitly use location-based services. This data is also backed up to your computer every time it is synced with iTunes. Warden wrote an application which can find, parse, and map the location data on a user's computer if the iOS device backups are not optionally encrypted.

Allan and Warden's findings sparked major concerns over privacy, leading some to speculate that Apple was tracking all iPhone users. The controversy prompted letters from Sentator Al Franken (D-MN) and US Representative Ed Markey (D-MA) demanding that Apple answer questions about how the data is collected, how or when it is sent to Apple, and how Apple could protect a user's privacy.

iOS data forensics expert Alex Levinson later on Wednesday revealed that the consolidated.db file was neither new—iOS has kept the same information in the past, just in a different database—nor was its existence necessarily a secret—Levinson had collaborated on a book with fellow security researcher Sean Morrisey that discussed consolidated.db in detail.

Eriksson suspected that his Android device collected similar information. "Following the latest internet outrage to the revelation that iPhone has a cache for its location service, I decided to have look what my Android device caches for the same function," he wrote in a note on GitHub. He put together an application similar to Warden's based on open source cache parsing code, which extracts data from "cache.cell" and "cache.wifi" and displays it on a map.

Like iOS, Android stores these databases in an area that is only accessible by root. To access the caches, an Android device needs to be "rooted," which removes most of the system's security features. Unlike iOS, though, Android phones aren't typically synced with a computer, so the files would need to be extracted from a rooted device directly. This distinction makes the data harder to access for the average user, but easy enough for an experienced hacker or forensic expert.

Another important difference, according to developer Mike Castelman, is that Android keeps less data overall than iOS devices. "The main difference that I can see is that Android seems to have a *cache* versus iOS's *log*," Castleman, who contributed some code improvements to Eriksson's tool, told Ars. That is, Android appears to limit the caches to 50 entries for cell tower triangulation and 200 entries for WiFi basestation location. iOS's consolidated.db, on the other hand, seems to keep a running tally of data since iOS is first installed and activated on a device. iOS will also keep multiple records of the same tower or basestation, while Android only keeps a single record.

Regardless of those differences, however, the data could be used in the same way. For instance, said Castleman, "if you were arrested or something shortly after a crime was committed, either device would contain evidence that could be used against you."

The data in these caches is used when GPS data isn't available, or to more quickly narrow down a location while GPS services are being polled (known as "assisted" or aGPS). Apple and Google both collect some of this data to build and maintain databases of known cell tower and WiFi basestation locations. Both companies previously used similar data from Skyhook, but both recently moved to building and using their own databases (presumably for cost and/or performance reasons).

A security researcher revealed to the *Wall Street Journal* that Google is also collecting a wide variety of location data

from Android devices which could lead to privacy breaches. "According to new research by security analyst Samy Kamkar, an HTC Android phone collected its location every few seconds and transmitted the data to Google at least several times an hour," the *WSJ* reported.

While Google is also using the data to improve its internal cell tower and WiFi location database or to improve call routing like Apple, it also uses the data to improve Google Maps and collect information about traffic patterns. The problem with Google's data collection is that unlike Apple, the information sent to Google contains a unique identification number that can be tied to a particular phone. While technically anonymous, that number could potentially be used to trace back to an individual user.

The fact that smartphones equipped with GPS could be used to track individual users isn't new, and a recent Nielsen survey revealed that many users are extremely wary about privacy when using location-based services via a mobile device. However, the details revealed in the past few days about the extent of location data collection and how easy it can be to access it have heightened privacy concerns even further.

UPDATE: Google spokesperson Randall Sarafa contacted Ars to clarify that its data collection practices are opt-in, as is Apple's. "All location sharing on Android is opt-in by the user. We provide users with notice and control over the collection, sharing and use of location in order to provide a better mobile experience on Android devices," he told Ars.

Furthermore, he explained that the unique identifier number is random, not hashed from the unique IMEI or MEID number associated with all mobile devices. "Any location data that is sent back to Google location servers is anonymized and is not tied or traceable to a specific user," Sarafa said. However, as researchers have shown numerous times in the past, "anonymized" data can often be analyzed and correlated with a single person with surprising accuracy.

June 1, 2011

VIA EMAIL AND HAND DELIVERY

The Honorable Al Franken
Chairman
Subcommittee on Privacy, Technology and the Law
United States Senate
Washington, DC 20510

Dear Chairman Franken:

I am writing in response to your letter of May 25, 2011 regarding consumer privacy disclosures from app developers. As we stated in our testimony at your May 10, 2011 hearing on Protecting Mobile Privacy, Apple is deeply committed to protecting the privacy of our customers who use Apple mobile devices, including iPhone, iPad and iPod touch. We have adopted a single comprehensive privacy policy that covers all our businesses and products, including the iTunes Store and the App Store. We do not share personally identifiable information with third parties for their marketing purposes without consent. Of equal importance, we require third-party application developers to agree to specific restrictions protecting our customers' privacy, which I will describe in more detail below.

Apple launched the App Store in July 2008 where customers may shop and acquire applications offered by third-party developers for the iPhone, iPad and iPod touch. Currently, the App Store includes more than 350,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation and socials. Because the overwhelming majority of these apps do not collect any information whatsoever from any user at any time, Apple has not mandated that its third-party developers incur both the legal expense and the burdensome administrative costs associated with issuing and maintaining a privacy policy unnecessarily – an expense that could well be prohibitive for a small struggling software developer or a teenager in his bedroom with only a MacBook and an idea.

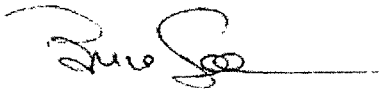
For those apps that do collect information, however, our licensing agreement with developers prohibits any application from collecting user or device data without prior user consent. We also make it abundantly clear in our licensing agreement that developers, irrespective of size of business or age, must provide clear and complete information to users regarding their apps' collection, use and disclosure of user or device data. While many developers comply simply by adding a link to their online privacy policy, others have chosen to disclose this information by adding a pop-up dialogue box for the user to see when launching the app for the first time. We strictly prohibit the use of any analytics software in an application that collects and sends device data to a third party. Our licensing agreement also requires that apps comply with all applicable privacy and data collection laws and regulations regarding the use or transmission of user and device data, including location-based information. Apple's requirements are intended to provide the user with the most useful information that meets our strict transparency and disclosure requirements, but we also have chosen not to dictate the means by which that information is delivered to the user.

Because location information can be particularly sensitive, in addition to all the developer privacy and collection disclosure requirements described above, Apple requires

explicit customer consent when any application requests location-based information for the first time. When an application requests the information, a dialog box appears stating: "[Application] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be provided to the application. This dialogue box is mandatory – neither Apple's applications nor those of third parties are permitted to override it. Again, as we stated in our recent testimony before your Subcommittee, this consent for location services by an app can be given and rescinded on an app-by-app basis quite easily, and very transparently.

Let me restate Apple's unwavering commitment to giving our customers clear and transparent notice, choice and control over their personal information. We believe our products do this in a simple and elegant way. We also strongly agree that any third-party app developer with access to customers' personal information should give its customers clear and transparent notice, choice and control over their information. We have made this a strict licensing requirement for all of our app developers. We share your concerns about the potential misuse of all customer data, and we believe that we have instituted policies and procedures that encourage third-party app developers to go well beyond disclosures written, and often unread, in an online privacy policy. We appreciate this opportunity to explain our policies and procedures to you.

Sincerely,



Bruce Sewell
General Counsel and Senior Vice
President of Legal and Government
Affairs

Apple App Store Review Guidelines

Introduction

We're pleased that you want to invest your talents and time to develop applications for iOS. It has been a rewarding experience - both professionally and financially – for tens of thousands of developers and we want to help you join this successful group. We have published our App Store Review Guidelines in the hope that they will help you steer clear of issues as you develop your app and speed you through the approval process when you submit it.

We view Apps different than books or songs, which we do not curate. If you want to criticize a religion, write a book. If you want to describe sex, write a book or a song, or create a medical app. It can get complicated, but we have decided to not allow certain kinds of content in the App Store. It may help to keep some of our broader themes in mind:

- We have lots of kids downloading lots of apps, and parental controls don't work unless the parents set them up (many don't). So know that we're keeping an eye out for the kids.
- We have over 350,000 apps in the App Store. We don't need any more Fart apps. If your app doesn't do something useful or provide some form of lasting entertainment, it may not be accepted.
- If your App looks like it was cobbled together in a few days, or you're trying to get your first practice App into the store to impress your friends, please brace yourself for rejection. We have lots of serious developers who don't want their quality Apps to be surrounded by amateur hour.
- We will reject Apps for any content or behavior that we believe is over the line. What line, you ask? Well, as a Supreme Court Justice once said, "I'll know it when I see it". And we think that you will also know it when you cross it.
- If your app is rejected, we have a Review Board that you can appeal to. If you run to the press and trash us, it never helps.
- If you attempt to cheat the system (for example, by trying to trick the review process, steal data from users, copy another developer's work, or manipulate the ratings) your apps will be removed from the store and you will be expelled from the developer program.
- This is a living document, and new apps presenting new questions may result in new rules at any time. Perhaps your app will trigger this.

Lastly, we love this stuff too, and honor what you do. We're really trying our best to create the best platform in the world for you to express your talents and make a living too. If it sounds like we're control freaks, well, maybe it's because we're so committed to our users and making sure they have a quality experience with our products. Just like almost all of you are too.

Table of Contents

1. Terms and conditions
2. Functionality
3. Metadata, ratings and rankings
4. Location

5. Push notifications
6. Game Center
7. iAds
8. Trademarks and trade dress
9. Media content
10. User interface
11. Purchasing and currencies
12. Scraping and aggregation
13. Damage to device
14. Personal attacks
15. Violence
16. Objectionable content
17. Privacy
18. Pornography
19. Religion, culture, and ethnicity
20. Contests, sweepstakes, lotteries, and raffles
21. Charities and contributions
22. Legal requirements

1. Terms and conditions

- **1.1**
  As a developer of applications for the App Store you are bound by the terms of the Program License Agreement (PLA), Human Interface Guidelines (HIG), and any other licenses or contracts between you and Apple. The following rules and examples are intended to assist you in gaining acceptance for your app in the App Store, not to amend or remove provisions from any other agreement.

2. Functionality

- **2.1**
  Apps that crash will be rejected

- **2.2**
  Apps that exhibit bugs will be rejected

- **2.3**
  Apps that do not perform as advertised by the developer will be rejected

- **2.4**
  Apps that include undocumented or hidden features inconsistent with the description of the app will be rejected

- **2.5**
  Apps that use non-public APIs will be rejected

- **2.6**
  Apps that read or write data outside its designated container area will be rejected

- **2.7**
  Apps that download code in any way or form will be rejected

- **2.8**
  Apps that install or launch other executable code will be rejected

- **2.9**
  Apps that are "beta", "demo", "trial", or "test" versions will be rejected

- **2.10**
  iPhone apps must also run on iPad without modification, at iPhone resolution, and at 2X iPhone 3GS resolution

- **2.11**
  Apps that duplicate apps already in the App Store may be rejected, particularly if there are many of them, such as fart, burp, flashlight, and Kama Sutra apps.

- **2.12**
  Apps that are not very useful or do not provide any lasting entertainment value may be rejected

- **2.13**
  Apps that are not very useful, are simply web sites bundled as apps, or do not provide any lasting entertainment value may be rejected

- **2.14**
  Apps that are intended to provide trick or fake functionality that are not clearly marked as such will be rejected

- **2.15**
  Apps larger than 20MB in size will not download over cellular networks (this is automatically prohibited by the App Store)

- **2.16**
  Multitasking apps may only use background services for their intended purposes: VoIP, audio playback, location, task completion, local notifications, etc

- **2.17**
  Apps that browse the web must use the iOS WebKit framework and WebKit Javascript

- **2.18**
  Apps that encourage excessive consumption of alcohol or illegal substances, or encourage minors to consume alcohol or smoke cigarettes, will be rejected

- **2.19**
  Apps that provide incorrect diagnostic or other inaccurate device data will be rejected

- **2.20**
  Developers "spamming" the App Store with many versions of similar apps will be removed from the iOS Developer Program

- **2.21**
  Apps that are simply a song or movie should be submitted to the iTunes store. Apps that are simply a book should be submitted to the iBookstore.

- **2.22**
  Apps that arbitrarily restrict which users may use the app, such as by location or carrier, may be rejected

3. Metadata (name, descriptions, ratings, rankings, etc)

- **3.1**
  Apps or metadata that mentions the name of any other mobile platform will be rejected

- **3.2**
  Apps with placeholder text will be rejected

- **3.3**
  Apps with descriptions not relevant to the application content and functionality will be rejected

- **3.4**
  App names in iTunes Connect and as displayed on a device should be similar, so as not to cause confusion

- **3.5**
  Small and large app icons should be similar, so as to not to cause confusion

- **3.6**
  Apps with app icons and screenshots that do not adhere to the 4+ age rating will be rejected

- **3.7**
  Apps with Category and Genre selections that are not appropriate for the app content will be rejected

- **3.8**
  Developers are responsible for assigning appropriate ratings to their apps. Inappropriate ratings may be changed by Apple

- **3.9**
  Developers are responsible for assigning appropriate keywords for their apps. Inappropriate keywords may be changed/deleted by Apple

- **3.10**
  Developers who attempt to manipulate or cheat the user reviews or chart ranking in the App Store with fake or paid reviews, or any other inappropriate methods will be removed from the iOS Developer Program

- **3.11**
  Apps which recommend that users restart their iOS device prior to installation or launch may be rejected

- **3.12**
  Apps should have all included URLs fully functional when you submit it for review, such as support and privacy policy URLs

4. Location

- **4.1**
  Apps that do not notify and obtain user consent before collecting, transmitting, or using location data will be rejected

- **4.2**
  Apps that use location-based APIs for automatic or autonomous control of vehicles, aircraft, or other devices will be rejected

- **4.3**
  Apps that use location-based APIs for dispatch, fleet management, or emergency services will be rejected

- **4.4**
  Location data can only be used when directly relevant to the features and services provided by the app to the user or to support approved advertising uses

5. Push notifications

- **5.1**
  Apps that provide Push Notifications without using the Apple Push Notification (APN) API will be rejected

- **5.2**
  Apps that use the APN service without obtaining a Push Application ID from Apple will be rejected

- **5.3**
  Apps that send Push Notifications without first obtaining user consent will be rejected

- **5.4**
  Apps that send sensitive personal or confidential information using Push Notifications will be rejected

- **5.5**
  Apps that use Push Notifications to send unsolicited messages, or for the purpose of phishing or spamming will be rejected

- **5.6**
  Apps cannot use Push Notifications to send advertising, promotions, or direct marketing of any kind

- **5.7**
  Apps cannot charge users for use of Push Notifications

- **5.8**
  Apps that excessively use the network capacity or bandwidth of the APN service or unduly burden a device with Push Notifications will be rejected

- **5.9**
  Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the APN service will be rejected

6. Game Center

- **6.1**
  Apps that display any Player ID to end users or any third party will be rejected

- **6.2**
  Apps that use Player IDs for any use other than as approved by the Game Center terms will be rejected

- **6.3**
  Developers that attempt to reverse lookup, trace, relate, associate, mine, harvest, or otherwise exploit Player IDs, alias, or other information obtained through the Game Center will be removed from the iOS Developer Program

- **6.4**
  Game Center information, such as Leaderboard scores, may only be used in apps approved for use with the Game Center

- **6.5**
  Apps that use Game Center service to send unsolicited messages, or for the purpose of phishing or spamming will be rejected

- **6.6**
  Apps that excessively use the network capacity or bandwidth of the Game Center will be rejected

- **6.7**
  Apps that transmit viruses, files, computer code, or programs that may harm or disrupt the normal operation of the Game Center service will be rejected

7. iAds

- **7.1**
  Apps that artificially increase the number of impressions or click-throughs of ads will be rejected

- **7.2**
  Apps that contain empty iAd banners will be rejected

- **7.3**
  Apps that are designed predominantly for the display of ads will be rejected

8. Trademarks and trade dress

- **8.1**
  Apps must comply with all terms and conditions explained in the Guidelines for using Apple Trademark and Copyrights and the Apple Trademark List

- **8.2**
  Apps that suggest or infer that Apple is a source or supplier of the app, or that Apple endorses any particular representation regarding quality or functionality will be rejected

- **8.3**
  Apps which appear confusingly similar to an existing Apple product or advertising theme will be rejected

- **8.4**
  Apps that misspell Apple product names in their app name (i.e., GPS for Iphone, iTunz) will be rejected

- **8.5**
  Use of protected 3rd party material (trademarks, copyrights, trade secrets, otherwise proprietary content) requires a documented rights check which must be provided upon request

- **8.6**
  Google Maps and Google Earth images obtained via the Google Maps API can be used within an application if all brand features of the original content remain unaltered and fully visible. Apps that cover up or modify the Google logo or copyright holders identification will be rejected

9. Media content

- **9.1**
  Apps that do not use the MediaPlayer framework to access media in the Music Library will be rejected

- **9.2**
  App user interfaces that mimic any iPod interface will be rejected

- **9.3**
  Audio streaming content over a cellular network may not use more than 5MB over 5 minutes

- **9.4**
  Video streaming content over a cellular network longer than 10 minutes must use HTTP Live Streaming and include a baseline 64 kbps audio-only HTTP Live stream

10. User interface

- **10.1**
  Apps must comply with all terms and conditions explained in the Apple iOS Human Interface Guidelines

- **10.2**
  Apps that look similar to apps bundled on the iPhone, including the App Store, iTunes Store, and iBookstore, will be rejected

- **10.3**
  Apps that do not use system provided items, such as buttons and icons, correctly and as described in the Apple iOS Human Interface Guidelines may be rejected

- **10.4**
  Apps that create alternate desktop/home screen environments or simulate multi-app widget experiences will be rejected

- **10.5**
  Apps that alter the functions of standard switches, such as the Volume Up/Down and Ring/Silent switches, will be rejected

- **10.6**
  Apple and our customers place a high value on simple, refined, creative, well thought through interfaces. They take more work but are worth it. Apple sets a high bar. If your user interface is complex or less than very good it may be rejected

11. Purchasing and currencies

- **11.1**
  Apps that unlock or enable additional features or functionality with mechanisms other than the App Store, except as approved in section 11.13, will be rejected

- **11.2**
  Apps utilizing a system other than the In App Purchase API (IAP) to purchase content, functionality, or services in an app will be rejected

- **11.3**
  Apps using IAP to purchase physical goods or goods and services used outside of the application will be rejected

- **11.4**
  Apps that use IAP to purchase credits or other currencies must consume those credits within the application

- **11.5**
  Apps that use IAP to purchase credits or other currencies that expire will be rejected

- **11.6**
  Content subscriptions using IAP must last a minimum of 7 days and be available to the user from all of their iOS devices

- **11.7**
  Apps that use IAP to purchase items must assign the correct Purchasability type

- **11.8**
  Apps that use IAP to purchase access to built-in capabilities provided by iOS, such as the camera or the gyroscope, will be rejected

- **11.9**
  Apps containing "rental" content or services that expire after a limited time will be rejected

- **11.10**
  Insurance applications must be free, in legal-compliance in the regions distributed, and cannot use IAP

- **11.11**
  In general, the more expensive your app, the more thoroughly we will review it

- **11.12**
  Apps offering subscriptions must do so using IAP, Apple will share the same 70/30 revenue split with developers for these purchases, as set forth in the Developer Program License Agreement.

- **11.13**
  Apps can read or play approved content (magazines, newspapers, books, audio, music, video) that is sold outside of the app, for which Apple will not receive any portion of the revenues, provided that the same content is also offered in the app using IAP at the same

price or less than it is offered outside the app. This applies to both purchased content and subscriptions.

- **11.14**
  Apps that link to external mechanisms for purchasing content to be used in the app, such as a "buy" button that goes to a web site to purchase a digital book, will be rejected

12. Scraping and aggregation

- **12.1**
  Applications that scrape any information from Apple sites (for example from apple.com, iTunes Store, App Store, iTunes Connect, Apple Developer Programs, etc) or create rankings using content from Apple sites and services will be rejected

- **12.2**
  Applications may use approved Apple RSS feeds such as the iTunes Store RSS feed

- **12.3**
  Apps that are simply web clippings, content aggregators, or a collection of links, may be rejected

13. Damage to device

- **13.1**
  Apps that encourage users to use an Apple Device in a way that may cause damage to the device will be rejected

- **13.2**
  Apps that rapidly drain the device's battery or generate excessive heat will be rejected

14. Personal attacks

- **14.1**
  Any app that is defamatory, offensive, mean-spirited, or likely to place the targeted individual or group in harms way will be rejected

- **14.2**
  Professional political satirists and humorists are exempt from the ban on offensive or mean-spirited commentary

15. Violence

- **15.1**
  Apps portraying realistic images of people or animals being killed or maimed, shot, stabbed, tortured or injured will be rejected

- **15.2**
  Apps that depict violence or abuse of children will be rejected

- **15.3**
  "Enemies" within the context of a game cannot solely target a specific race, culture, a real government or corporation, or any other real entity

- **15.4**
  Apps involving realistic depictions of weapons in such a way as to encourage illegal or reckless use of such weapons will be rejected

- **15.5**
  Apps that include games of Russian roulette will be rejected

16. Objectionable content

- **16.1**
  Apps that present excessively objectionable or crude content will be rejected

- **16.2**
  Apps that are primarily designed to upset or disgust users will be rejected

17. Privacy

- **17.1**
  Apps cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used

- **17.2**
  Apps that require users to share personal information, such as email address and date of birth, in order to function will be rejected

- **17.3**
  Apps that target minors for data collection will be rejected

18. Pornography

- **18.1**
  Apps containing pornographic material, defined by Webster's Dictionary as "explicit descriptions or displays of sexual organs or activities intended to stimulate erotic rather than aesthetic or emotional feelings", will be rejected

- **18.2**
  Apps that contain user generated content that is frequently pornographic (ex "Chat Roulette" apps) will be rejected

19. Religion, culture, and ethnicity

- **19.1**
  Apps containing references or commentary about a religious, cultural or ethnic group that are defamatory, offensive, mean-spirited or likely to expose the targeted group to harm or violence will be rejected

- **19.2**
  Apps may contain or quote religious text provided the quotes or translations are accurate and not misleading. Commentary should be educational or informative rather than inflammatory

20. Contests, sweepstakes, lotteries, and raffles

- **20.1**
  Sweepstakes and contests must be sponsored by the developer/company of the app

- **20.2**
  Official rules for sweepstakes and contests, must be presented in the app and make it clear that Apple is not a sponsor or involved in the activity in any manner

- **20.3**
  It must be permissible by law for the developer to run a lottery app, and a lottery app must have all of the following characteristics: consideration, chance, and a prize

- **20.4**
  Apps that allow a user to directly purchase a lottery or raffle ticket in the app will be rejected

21. Charities and contributions

- **21.1**
  Apps that include the ability to make donations to recognized charitable organizations must be free

- **21.2**
  The collection of donations must be done via a web site in Safari or an SMS

22. Legal requirements

- **22.1**
  Apps must comply with all legal requirements in any location where they are made available to users. It is the developer's obligation to understand and conform to all local laws

- **22.2**
  Apps that contain false, fraudulent or misleading representations will be rejected

- **22.3**
  Apps that solicit, promote, or encourage criminal or clearly reckless behavior will be rejected

- **22.4**
  Apps that enable illegal file sharing will be rejected

- **22.5**
  Apps that are designed for use as illegal gambling aids, including card counters, will be rejected

- **22.6**
  Apps that enable anonymous or prank phone calls or SMS/MMS messaging will be rejected

- **22.7**
  Developers who create apps that surreptitiously attempt to discover user passwords or other private user data will be removed from the iOS Developer Program

Living document

This document represents our best efforts to share how we review apps submitted to the App Store, and we hope it is a helpful guide as you develop and submit your apps. It is a living document that will evolve as we are presented with new apps and situations, and we'll update it periodically to reflect these changes.

Thank you for developing for iOS. Even though this document is a formidable list of what not to do, please also keep in mind the much shorter list of what you must do. Above all else, join us in trying to surprise and delight users. Show them their world in innovative ways, and let them interact with it like never before. In our experience, users really respond to polish, both in functionality and user interface. Go the extra mile. Give them more than they expect. And take them places where they have never been before. We are ready to help.

© Apple, 2011

Apple's July 12, 2010 Letter to the Honorable Edward J. Markey and the Honorable Joe Barton

July 12, 2010

VIA HAND DELIVERY

The Honorable Edward J. Markey
The Honorable Joe Barton
United States House of Representatives
Washington, DC 20515

Re: ***Apple Inc.'s Response to Request for Information Regarding Its Privacy Policy and Location-Based Services***

Dear Representatives Markey and Barton:

I write in response to your June 24, 2010 letter to Steve Jobs requesting information and documents about Apple's privacy policy and location-based services. I appreciate the opportunity to provide additional information about these matters, and I welcome further discussions with you.

To provide context to our responses to the questions presented in your letter, I first would like to provide some background information about Apple's privacy policy, location-based services, the iAd network, and the App Store.

I. APPLE'S PRIVACY POLICY

A. Overview

Apple is strongly committed to protecting the privacy of its customers. Apple has a single Customer Privacy Policy (the "Policy") that applies across all Apple businesses and products, including the iTunes Store and App Store.[1] The Policy, written in easy-to-read language, details what information Apple collects and how Apple and its partners and licensees may use the information. The Policy is available from a link on every page of Apple's website.[2]

As noted in your letter, the Policy was updated on June 21, 2010, to add, among other changes discussed below, the following provision regarding location-based information:

---

[1] As used in the policy and in this letter, "Apple," refers to Apple Inc. and affiliated companies.
[2] The links take customers to http://www.apple.com/legal/privacy, which may also be accessed by customers directly.

> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.
>
> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.

This provision incorporated similar language regarding location-based information that appears in Apple End User Software License Agreements ("SLAs") for products that provide location-based services. For example, the current iPhone 3GS SLA, last updated in May 2009, states:

> Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data collected by Apple is collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data to provide such products and services.** You may withdraw this consent at any time by not using the location-based features or by turning off the Location Services setting on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services.

(Emphasis in original.) Similar provisions regarding location-based information appear in the iPhone 4, iPad, iPod Touch, Mac OS X, and Safari 5 SLAs.

The Policy identifies dedicated email addresses for privacy-related inquiries and comments. Apple monitors these email addresses and responds to appropriate inquiries in a

timely manner. Customers may also address privacy concerns to TRUSTe, Apple's third-party privacy monitor. A link to TRUSTe is displayed within the Policy.

B. June 2010 Policy Update

In the past three years, Apple revised its Policy three times: June 29, 2007, early February 2008, and June 21, 2010.

The June 29, 2007 update advised customers about the necessary exchange of information between Apple and the relevant cellular carrier when an iPhone is activated. Apple also added a provision stating that it does "not knowingly collect personal information from children." The provision explained that if such information was collected inadvertently, Apple would attempt to delete it "as soon as possible."

The February 2008 Policy update revised language regarding Apple's use of "pixel tags." Pixel tags are tiny graphic images used to determine what parts of Apple's website customers visited or to measure the effectiveness of searches performed on Apple's website. The revised language stated that: "[Apple] may use this information to reduce or eliminate messages sent to a customer."

On June 21, 2010, Apple updated the Policy to incorporate the language regarding location-based services from Apple SLAs, as discussed above. Apple also added provisions regarding new Apple services, such as Apple's MobileMe "Find My iPhone" feature and the iAd network. Apple made the following, additional material changes to the Policy:

- Revised provisions regarding (i) what information Apple collects from customers and how Apple and its partners and licensees may use the information, (ii) the use of "Cookies and Other Technologies," (iii) the safeguards in place to prevent the collection of personal information from children, and (iv) the collection and use of information from international customers; and

- Added provisions (i) advising customers to review the privacy practices of third-party application providers and (ii) cautioning customers about posting personal information on an Apple forum, chat room, or social networking service.

As noted above, customers may access the updated Policy from every page on Apple's website. The updated Policy also was placed where Apple believed the largest number of customers would see it: the iTunes Store. Following the update, every customer logging onto the iTunes Store is prompted to review the iTunes Store Terms and Conditions. For customers with existing iTunes accounts, the webpage states:

> iTunes Store Terms and Conditions have changed. Apple's Privacy Policy
>
> The changes we have made to the terms and conditions include the following:

• Apple's Privacy Policy has changed in material ways. Please visit www.apple.com/legal/privacy or view below.

Customers are asked to click an unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not agree to the Terms and Conditions and the Policy will not be able to use the iTunes Store (*e.g.*, will not be able to make purchases on the iTunes Store or the App Store), but they may continue to use iTunes software.

Customers attempting to open a new iTunes account are directed to a webpage titled: "iTunes Store Terms & Conditions and Apple's Privacy Policy." They are asked to click the same unchecked agreement box stating: "I have read and agree to the iTunes Terms and Conditions and Apple's Privacy Policy." Customers who do not accept the Terms and Conditions and the Policy will not be able to open an iTunes account but may still activate and use their devices.

II. LOCATION-BASED SERVICES

A. Overview

In response to increasing customer demand, Apple began to provide location-based services in January 2008. These services enable applications that allow customers to perform a wide variety of useful tasks such as getting directions to a particular address from their current location, locating their friends or letting their friends know where they are, or identifying nearby restaurants or stores.

Apple offers location-based services on the iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard,[3] and Windows or Mac computers running Safari 5.[4]

Although Apple's customers value these services and may use them on a daily basis, Apple recognizes that some customers may not be interested in such services at all times. As discussed below, Apple provides its customers with tools to control if and when location-based information is collected from them.

B. Privacy Features

Apple has always provided its customers with the ability to control the location-based service capabilities of their devices. In fact, Apple now provides customers even greater control

[3] All of Apple's Mac computers, *e.g.*, MacBook, MacBook Pro, MacBook Air, iMac, Mac mini, and Mac Pro, run on its proprietary Mac OS operating system. Apple released the current version, Mac OS X version 10.6, known as "Snow Leopard," on August 28, 2009.
[4] Safari is Apple's proprietary Internet browser. Apple released the current version of Safari version 5, on June 7, 2010.

over such capabilities for devices running the current version of Apple's mobile operating system—iOS 4.[5]

First, customers have always had the ability to turn "Off" all location-based service capabilities with a single "On/Off" toggle switch. For mobile devices, the toggle switch is in the "General" menu under "Settings." For Mac computers running Snow Leopard, the toggle switch is in the "Security" menu under "System Preferences." And for Safari 5, the toggle switch is in the "Security" menu in Safari "Preferences." If customers toggle the switch to "Off," they may not use location-based services, and no location-based information will be collected.

Second, Apple has always required express customer consent when any application or website requests location-based information for the first time. When an application or website requests the information, a dialogue box appears stating: "[Application/Website] would like to use your current location." The customer is asked: "Don't Allow" or "OK." If the customer clicks on "Don't Allow," no location-based information will be collected or transmitted. This dialogue box is mandatory—neither Apple nor third-parties are permitted to override the notification.

Third, iOS 4 permits customers to identify individual applications that may not access location-based information, even though the global location-based service capabilities setting may be toggled to "On." The "General" menu under "Settings" provides an "On/Off" toggle switch for each application. When the switch for a particular application is toggled to "Off," no location-based information will be collected or transmitted for that application. And even if the switch for an application is toggled to "On," the "Don't Allow/OK" dialogue box will request confirmation from the customer the first time that application requests location-based information. Customers can change their individual application settings at any time.

Finally, an arrow icon ( ) alerts iOS 4 users that an application is using or has recently used location-based information. This icon will appear real-time for currently running applications and next to the "On/Off" toggle switch for any application that has used location-based information in the past twenty-four hours.

C. Location-Based Information

To provide the high quality products and services that its customers demand, Apple must have access to comprehensive location-based information. For devices running the iPhone OS versions 1.1.3 to 3.1, Apple relied on (and still relies on) databases maintained by Google and Skyhook Wireless ("Skyhook") to provide location-based services. Beginning with the iPhone OS version 3.2 released in April 2010, Apple relies on its own databases to provide location-

[5] All of Apple's mobile devices run on its proprietary mobile operating system. Apple released the current version, iOS 4, on June 21, 2010. Currently, iOS 4 may be run on the iPhone 3G, iPhone 3GS, iPhone 4, and iPod touch. The iPad Wi-Fi + 3G, iPad Wi-Fi, and older models of the iPhone run on prior versions of Apple's mobile operating system, referred to as iPhone OS. Apple has released iPhone OS versions 1.0 through 3.2.

based services and for diagnostic purposes. These databases must be updated continuously to account for, among other things, the ever-changing physical landscape, more innovative uses of mobile technology, and the increasing number of Apple's customers. Apple always has taken great care to protect the privacy of its customers.

1. Cell Tower and Wi-Fi Information

a. Collections and Transmissions from Apple Mobile Devices

To provide location-based services, Apple must be able to determine quickly and precisely where a device is located. To do this, Apple maintains a secure database containing information regarding known locations of cell towers and Wi-Fi access points. The information is stored in a database accessible only by Apple and does not reveal personal information about any customer.

Information about nearby cell towers and Wi-Fi access points is collected and sent to Apple with the GPS coordinates of the device, if available: (1) when a customer requests current location information and (2) automatically, in some cases, to update and maintain databases with known location information. In both cases, the device collects the following anonymous information:

- Cell Tower Information: Apple collects information about nearby cell towers, such as the location of the tower(s), Cell IDs, and data about the strength of the signal transmitted from the towers. A Cell ID refers to the unique number assigned by a cellular provider to a cell, a defined geographic area covered by a cell tower in a mobile network. Cell IDs do not provide any personal information about mobile phone users located in the cell. Location, Cell ID, and signal strength information is available to anyone with certain commercially available software.

- Wi-Fi Access Point Information: Apple collects information about nearby Wi-Fi access points, such as the location of the access point(s), Media Access Control (MAC) addresses, and data about the strength and speed of the signal transmitted by the access point(s). A MAC address (a term that does not refer to Apple products) is a unique number assigned by a manufacturer to a network adapter or network interface card ("NIC"). The address provides the means by which a computer or mobile device is able to connect to the Internet. MAC addresses do not provide any personal information about the owner of the network adapter or NIC. Anyone with a wireless network adapter or NIC can identify the MAC address of a Wi-Fi access point. Apple does not collect the user-assigned name of the Wi-Fi access point (known as the "SSID," or service set identifier) or data being transmitted over the Wi-Fi network (known as "payload data").

First, when a customer requests current location information, the device encrypts and transmits Cell Tower and Wi-Fi Access Point Information and the device's GPS coordinates (if available) over a secure Wi-Fi Internet connection to Apple.[6] For requests transmitted from devices running the iPhone OS version 3.2 or iOS 4, Apple will retrieve known locations for nearby cell towers and Wi-Fi access points from its proprietary database and transmit the information back to the device. For requests transmitted from devices running prior versions of the iPhone OS, Apple transmits—anonymously—the Cell Tower Information to Google[7] and Wi-Fi Access Point Information to Skyhook. These providers return to Apple known locations of nearby cell towers and Wi-Fi access points, which Apple transmits back to the device. The device uses the information, along with GPS coordinates (if available), to determine its actual location. Information about the device's actual location is not transmitted to Apple, Skyhook, or Google. Nor is it transmitted to any third-party application provider, unless the customer expressly consents.

Second, to help Apple update and maintain its database with known location information, Apple may also collect and transmit Cell Tower and Wi-Fi Access Point Information automatically. With one exception,[8] Apple automatically collects this information only (1) if the device's location-based service capabilities are toggled to "On" and (2) the customer uses an application requiring location-based information. If both conditions are met, the device intermittently and anonymously collects Cell Tower and Wi-Fi Access Point Information from the cell towers and Wi-Fi access points that it can "see," along with the device's GPS coordinates, if available. This information is batched and then encrypted and transmitted to Apple over a Wi-Fi Internet connection every twelve hours (or later if the device does not have Wi-Fi Internet access at that time).

b. Collections and Transmissions from Computers Running Snow Leopard and/or Safari 5

Apple collects Wi-Fi Access Point Information when a Mac computer running Snow Leopard makes a location-based request—for example, if a customer asks for the current time

---

[6] Requests sent from devices running older versions of the iPhone OS also include a random identification number that is generated by the device every ninety days. This number cannot be used to identify any particular user or device.

[7] For GPS-enabled devices running prior versions of the iPhone OS, Apple also sends the device's GPS coordinates, if available, anonymously to Google so that Google can update its database of known locations.

[8] For GPS-enabled devices with location-based service capabilities toggled to "On," Apple automatically collects Wi-Fi Access Point Information and GPS coordinates when a device is searching for a cellular network, such as when the device is first turned on or trying to re-establish a dropped connection. The device searches for nearby Wi-Fi access points for approximately thirty seconds. The device collects anonymous Wi-Fi Access Point Information for those that it can "see." This information and the GPS coordinates are stored (or "batched") on the device and added to the information sent to Apple. None of the information transmitted to Apple is associated with a particular user or device.

zone to be set automatically. The information is collected anonymously and is stored in a database accessible only by Apple. Snow Leopard users can prevent the collection of this information by toggling the "Location Services" setting to "Off" in the "Security" menu under "System Preferences."

Apple also provides location-based services in Safari 5. When a customer is using Safari 5 and runs an Internet application that requests location-based information (*e.g.*, Google Maps), a dialog box will appears stating: "[Website name] would like to use your computer location." If the customer selects "Don't Allow," no location-based information is transmitted by the computer. If the customer selects "OK," Wi-Fi Access Point Information is transmitted to Apple with the request, so that Apple can return information about the computer's location. Apple does not store any Wi-Fi Access Point Information sent with requests from Safari 5.

2. Diagnostic Information

To evaluate and improve the performance of its mobile hardware and operating system, Apple collects diagnostic information from randomly-selected iPhones and analyzes the collected information. For example, when an iPhone customer makes a call, Apple may determine the device's approximate location at the beginning and end of the call to analyze whether a problem like dropped calls is occurring on the same device repeatedly or by multiple devices in the same area. Apple determines the approximate location by collecting information about nearby cell towers and Wi-Fi access points and comparing that with known cell tower and Wi-Fi access point locations in Apple's database. Apple may also collect signal strength information to identify locations with reception issues.

Before any diagnostic information is collected, the customer must provide express consent to Apple. If the customer consents, the information is sent to Apple over a secure connection. The information is sent anonymously and cannot be associated with a particular user or device. The diagnostic information is stored in a database accessible only by Apple. If the customer does not consent, Apple will not collect any diagnostic information.

3. GPS Information

The iPhone 3G, iPhone 3GS, iPhone 4, and iPad Wi-Fi + 3G are equipped with GPS chips. A GPS chip attempts to determine a device's location by analyzing how long it takes for satellite signals to reach the device. Through this analysis, the GPS chip can identify the device's latitude/longitude coordinates, altitude, speed and direction of travel, and the current date and time where the device is located ("GPS Information").

Apple collects GPS Information from mobile devices running the iPhone OS 3.2 or iOS 4. GPS Information may be used, for example, to analyze traffic patterns and density in various areas. With one exception,[9] Apple collects GPS Information only if (1) the location-based

[9] GPS Information is also collected during the short period of time (approximately thirty seconds) when a GPS-enabled device with location-based service capabilities toggled to "On" is

service capabilities of the device are toggled to "On" and (2) the customer uses an application requiring GPS capabilities. The collected GPS Information is batched on the device, encrypted, and transmitted to Apple over a secure Wi-Fi Internet connection (if available) every twelve hours with a random identification number that is generated by the device every twenty-four hours. The GPS Information cannot be associated with a particular customer or device.

The collected GPS Information is stored in a database accessible only by Apple.

D. iAd Network

On July 1, 2010, Apple launched the iAd mobile advertising network for iPhone and iPod touch devices running iOS 4. The iAd network offers a dynamic way to incorporate and access advertising within applications. Customers can receive advertising that relates to their interests ("interest-based advertising") and/or their location ("location-based advertising"). For example, a customer who purchased an action movie on iTunes may receive advertising regarding a new action movie being released in the theaters or on DVD. A customer searching for nearby restaurants may receive advertising for stores in the area.

As specified in the updated Policy and the iPhone 4 and iPod touch SLAs, customers may opt out of interest-based advertising by visiting the following site from their mobile device: https://oo.apple.com. Customers also may opt out of location-based advertising by toggling the device's location-based service capabilities to "Off."[10]

For customers who do not toggle location-based service capabilities to "Off," Apple collects information about the device's location (latitude/longitude coordinates) when an ad request is made. This information is transmitted securely to the Apple iAd server via a cellular network connection or Wi-Fi Internet connection. The latitude/longitude coordinates are converted immediately by the server to a five-digit zip code. Apple does not record or store the latitude/longitude coordinates—Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer.

Apple does not share any interest-based or location-based information about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive overly repetitive and/or duplicative ads and for administrative purposes.

---

searching for a cellular network. This information is sent anonymously to Apple to assist the device with locating an available channel. Apple does not retain this GPS Information in its database.

[10] A customer who opts out of interest-based and location-based advertising may still receive ads. The ads, however, will likely be less relevant to the customer because they will not be based on either interests or location. The customer also may receive interest-based or location-based ads from networks other than the iAd network.

In some cases, an advertiser may want to provide more specific information based on a device's actual location. For example, a retailer may want its ad to include the approximate distance to nearby stores. A dialogue box will appear stating: "iAd would like to use your current location." The customer is presented with two options: "Don't Allow" or "OK." If a customer clicks "Don't Allow," no additional location information is transmitted. If the customer clicks "OK," Apple uses the latitude/longitude coordinates to provide the ad application with more specific location information—the information is not provided to the advertiser.

III. THIRD-PARTY APPLICATIONS

A. Overview

In July 2008, Apple launched the App Store where customers may shop for and acquire applications offered by third-party developers for the iPhone, iPad, and iPod touch. Currently the App Store includes more than 200,000 third-party applications covering a wide variety of areas including news, games, music, travel, health, fitness, education, business, sports, navigation, and social networking. Each application includes a description prepared by the developer regarding, among other things, what the application does, when it was posted, and, if applicable, what information the application may collect from the customer.

Any customer with an iTunes account may purchase and download applications from the App Store. Developers do not receive any personal information about customers from Apple when applications are purchased. Only Apple has access to that information.

B. Third-Party Developers

Third-party application developers must register as an "Apple Developer" by paying a fee and signing the iPhone Developer Agreement (the "IDA") and the Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit ("SDK") and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application (PLA § 3.3.9);

- Developers must provide information to their customers regarding the use and disclosure of location-based information (*e.g.*, a description on the App Store or adding a link to the applicable privacy policy) (PLA § 3.3.10);

- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access (*id.*);

- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information (PLA § 3.3.11);

- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers (PLA § 3.3.12); and

- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use (PLA § 3.3.14).

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these provisions. (PLA § 12.2.)

Apple reviews all applications before adding them to the App Store to ensure, for example, that they run properly and do not contain malicious code. Apple, however, does not monitor applications after they are listed in the App Store, unless issues or problems arise.

IV. RESPONSES

The following responses represent the current state of our knowledge based on our investigation to date. Our investigation is ongoing, however, and we may continue to discover information responsive to your letter. I will update our responses, as needed, if we locate other responsive materials or information.

1. **Which specific Apple products are being used by Apple to collect geographic location data?**

The iPhone 3G, iPhone 3GS, iPhone 4, iPad Wi-Fi + 3G, and, to a more limited extent, older models of the iPhone, the iPad Wi-Fi, iPod touch, Mac computers running Snow Leopard, and Windows or Mac computers running Safari 5.

2. **When did Apple begin collecting this location data, and how often is data collected from a given consumer?**

Apple first began offering location-based service in January of 2008 and began collecting Wi-Fi Access Point Information at that time.

As described above, collection of location data varies greatly based on the services requested by each customer. Location data will not be collected at all from those users who have location services turned off.

3. **Does Apple collect this location data from all consumers using Apple products? If the answer is no, please explain which consumers Apple is**

collecting information from and the reasons that these consumers were chosen for monitoring?

Apple collects anonymous Wi-Fi Access Point, Cell Tower and GPS Information from devices that have location services turned on, have explicitly authorized apps to use their location, and are actively running one of the apps. Anonymous Wi-Fi Access Point Information and GPS coordinates may also be collected when an iPhone is using GPS to search for a cellular network. Diagnostic location data is only collected from users who have expressly agreed to send this information to Apple. Device location data (by zip code only) is collected from users who participate in the iAd network.

4. **How many consumers are subject to this collection of location data?**

Please see our answer to question #3 above.

5. **What internal procedures are in place to ensure that any location data is stored "anonymously in a form that does not personally identify" individual consumers?**

When a customer's device sends Wi-Fi, cell tower, GPS or diagnostic location data to Apple it does not include any information identifying the particular device or user.

In the case of the iAd network, latitude and longitude coordinates are collected and immediately converted to a five-digit zip code. Latitude and longitude coordinates are not kept or otherwise associated with an individual. Apple's iAd server does associate the five-digit zip code with a device identifier for the purpose of serving a location-relevant ad. Apple does not share any location data about individual customers, including the zip code calculated by the iAd server, with advertisers. Apple retains a record of each ad sent to a particular device in a separate iAd database, accessible only by Apple, to ensure that customers do not receive duplicative ads and for administrative purposes. Apple intends to retain the zip code information it has collected for six months to administer and improve the iAd network. After six months, the information may be aggregated for administrative purposes.

6. **Please explain in detail why Apple decided to begin collecting location data at this time, and how it intends to use the data.**

Please see our answer to question #2 above regarding when we began collecting relevant information. Apple collects location data for only one purpose—to enhance and improve the services we can offer to our customers.

7. **Is Apple sharing consumer location information collected through iPhones and iPads with AT&T or other telecommunications carriers?**

No.

8. **Who are the unspecified "partners and licensees" with which Apple shares this location data, and what are the terms and conditions of such information sharing? How does this comply with the requirements of Section 222 of the Communications Act, which mandates that no consumer location information be shared without the explicit prior consent of the consumer?**

The "licensees" referred to above are our software application developers. Apple shares location data with an application developer only after a user has given express consent to the sharing.

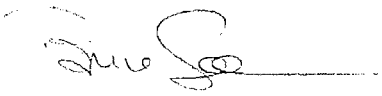
"Partners" refers to two external partners who maintain databases of known locations for cell towers and Wi-Fi access points. Earlier versions of the iPhone software rely on these databases for Wi-Fi access point and cell tower locations. For devices running that earlier software, Apple shares anonymous, non-device identifying location information with these external partners to obtain better location results for our users.

9. **Does Apple believe that legal boilerplate in a general information policy, which the consumer must agree to in order to download applications or updates, is consistent with the intent of Section 222, and sufficient to inform the consumer that the consumer's location may be disclosed to other parties? Has Apple or its legal counsel conducted an analysis of this issue? If yes, please provide a copy. If not, why not?**

While Apple is not a telecommunications carrier or service provider subject to Section 222, we believe the privacy protections described in detail in this letter are consistent with the intent of Section 222.

Apple is committed to giving our customers clear notice and control over their information, and we believe our products do this in a simple and elegant way. We share your concerns about the collection and misuse of location data, and appreciate this opportunity to explain our policies and procedures.

Sincerely,



Bruce Sewell
General Counsel and Senior Vice President of
Legal and Government Affairs

May 6, 2011

VIA EMAIL AND HAND DELIVERY

The Honorable Al Franken
United States Senate
Washington, DC 20510

Dear Chairman Franken:

Apple provides this letter in response to your letter of April 20, 2011.

On April 27, 2011, Apple issued the attached public response to questions about how Apple gathers and uses location information. That response provides much of the information requested in your letter. The following summary provides additional details regarding Apple's collection, storage, and use of location information on Apple mobile devices. After this summary, specific answers are given to each question in your letter.

At the outset, the initial point made in Apple's April 27 public response should be emphasized: Apple does not track users' locations – Apple has never done so and has no plans to ever do so. Instead, to provide the best services to meet customers' demands, Apple collects the following, limited kinds of location-related information from a device.

I. SUMMARY OF APPLE'S COLLECTION, STORAGE, AND USE OF LOCATION INFORMATION ON APPLE MOBILE DEVICES

A. Crowd-Sourced Database of Wi-Fi Hotspot and Cell Tower Location Information

Consumers are increasingly demanding accurate location information from their handheld devices. Consumers want directions from their current location to a desired destination; consumers want their devices to find the nearest coffee shop or gas station. To get this type of information, consumers want and expect their mobile devices to be able to quickly and reliably determine their current locations. If the device contains a GPS chip, the device can determine its current location using GPS satellite data. But this process can take up to several minutes. Obviously, if the device does not have a GPS chip, the GPS location data is not available at all.

To enable Apple mobile devices to respond quickly (or at all, in the case of non-GPS equipped devices or when GPS is not available, such as indoors or in basements) to a customer's request for current location information, Apple maintains a secure database containing

information regarding known locations of cell towers and Wi-Fi access points – also referred to as Wi-Fi hotspots. (For additional details, please see Apple's July 12, 2010 Letter to The Honorable Edward J. Markey and The Honorable Joe Barton (Apple's "July 12, 2010 Letter") at 6.)[1] As described in greater detail below with regard to mobile devices – and as discussed in detail with regard to both mobile devices and Mac computers in the July 12, 2010 Letter – Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of Apple devices. From this anonymous information, Apple has been able, over time, to calculate the known locations of millions of Wi-Fi hot spots and cell towers. Because the basis for this location information is the "crowd" of Apple devices, Apple refers to this as its "crowd-sourced" database. The crowd-sourced database does not reveal personal information about any customer.

An Apple mobile device running Apple's mobile device operating system, iOS, can use the crowd-sourced database to (1) provide the customer with an approximate location while waiting for the more precise GPS location, (2) find GPS satellites much more quickly, significantly reducing the wait time for the GPS location, and (3) triangulate the device location when GPS is not available (such as indoors or in basements). The device performs all of these calculations in response to a request for location information from an application on the customer's device that has been explicitly approved by the user to obtain the current location, and the device requests from Apple the crowd-sourced database information needed for these calculations.

To further improve the speed with which the device can calculate location, Apple downloads a subset of the crowd-sourced database content to a local cache on the device. This content describes the known locations of Wi-Fi hotspots[2] and cell towers that the device can "see" and/or that are nearby, as well as nearby cell location area codes,[3] some of which may be more than one hundred miles away. The presence of the local cache on the device enables the device to calculate an initial approximate location before Apple's servers can respond to a request for information from the crowd-sourced database.

As discussed in more detail below, Apple issued a free software update that changed the way in which iOS maintained its local cache. The software update reduced the size of the crowd-source Wi-Fi hotspot and cell tower database cached on the devices, ceased backing up this cache, and deleted the cache entirely when Location Services is off.

For devices that have installed this update, iOS stores this local cache in a database file called "cache.db." For devices running previous versions of iOS 4, iOS stores this local cache in the "consolidated.db" database. Except as otherwise noted, "local cache" is used herein to refer to the downloaded hotspot and cell tower location information, whether stored in consolidated.db or in cache.db.

---

[1] For your reference, a copy of Apple's July 12, 2010 Letter is attached and is also available online on Congressman Markey's website at http://markey.house.gov/docs/applemarkeybarton7-12-10.pdf.

[2] For each Wi-Fi hotspot, the location information includes that hotspot's MAC address, latitude/longitude coordinates, associated horizontal accuracy number, and a confidence value. For each cell tower, the location information includes the cell tower ID, latitude/longitude coordinates, associated horizontal accuracy number, and a confidence value.

[3] Cell base stations are grouped into "location areas" for network planning purposes, and each location area is assigned a unique "location area code." This "location area code" is broadcast by the cell base stations.

The local cache does not include a log of each time the device was near a particular hotspot or cell tower, and the local cache has never included such a log. For each Wi-Fi hotspot and cell tower, the local cache stores only that hotspot's/cell tower's most recent location information, downloaded from Apple's constantly updated crowd-sourced database. After a customer installs the free iOS software update, iOS will purge records that are older than seven days, and the cache will be deleted entirely when Location Services is turned off.

The local cache is protected with iOS security features, but it is not encrypted. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

When a customer runs certain applications, those applications request location information from iOS. Because of a bug that existed prior to the update, even when Location Services was off, the device would anonymously send the IDs of visible Wi-Fi hotspots and cell towers, without any GPS information, to Apple's servers, Apple's servers would send back the known, crowd-sourced location information for those hotspots and cell towers (and nearby hotspots and cell towers), and the device would cache that information in the consolidated.db file. None of this downloaded crowd-sourced location information – or any other location information – would be provided to or disclosed to the application.

The iOS software update fixed the bug that caused crowd-sourced location information to be downloaded to the device while Location Services was off. iOS will now delete any existing local cache from consolidated.db and, if Location Services is off, (1) Apple will not download any crowd-sourced location information to the device, regardless of whether a specific application requests that information, and (2) iOS will delete any cache of this information stored in cache.db.

B. Collecting Crowd-Sourced Wi-Fi Hotspot and Cell Tower Location Information

As mentioned above and in the July 12, 2010 Letter, Apple collects anonymous location information about Wi-Fi hotspots and cell towers from millions of devices to develop and refine Apple's database of crowd-sourced location information. The mobile devices intermittently collect information about Wi-Fi hotspots and cell towers that they can "see" and tag that information with the device's current GPS coordinates, i.e. the devices "geo-tag" hotspots and towers.

This collected Wi-Fi hotspot and cell tower information is temporarily saved in a separate table in the local cache; thereafter, that data is extracted from the database, encrypted, and transmitted – anonymously – to Apple over a Wi-Fi connection every twelve hours (or later if the device does not have Wi-Fi access at that time). Apple's servers use this information to re-

calculate and update the known locations of Wi-Fi hotspots and cell towers stored in its crowd-sourced database. As explained in Apple's April 27 public response and Apple's July 12, 2010 Letter, Apple cannot identify the source of this information, and Apple collects and uses this information only to develop and improve the Wi-Fi hotspot and cell tower location information in Apple's crowd-sourced database. After the device attempts to upload this information to Apple, even if the attempt fails, the information is deleted from the local cache database on the device. In versions of iOS 4.1 or later, moreover, the device will not attempt to collect or upload this anonymous information to Apple unless Location Services is on and the customer has explicitly consented to at least one application's request to use location information.[4]

C. Additional Location Information Collections

If Location Services is on, Apple collects location information from mobile devices under the following additional circumstances.

First, as mentioned in Apple's April 27 response, Apple is now collecting anonymous traffic data to build a crowd-sourced automobile traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years. This information is temporarily stored in the local cache on the device, anonymously uploaded to Apple, and then deleted from the device.

Second, Apple collects anonymous diagnostic information from randomly-selected devices to evaluate and improve the performance of its mobile hardware and operating system. For example, Apple may collect information about a dropped cell phone call, including the calculated location of the device when a call was dropped, to help identify and address any cell connection issues. Before any diagnostic information is collected, the customer must provide express consent to Apple. Apple cannot associate this information with a particular customer. Additional details regarding Apple's diagnostic collection practices are provided in the July 12, 2010 Letter at page 8.

Third, Apple obtains information about the device's location (the latitude/longitude coordinates) when an ad request is made. The device securely transmits this information to the Apple iAd servers, the iAd servers immediately convert the latitude/longitude coordinates to a five-digit zip code, and the iAd servers then discard the coordinates. Apple does not record or store the latitude/longitude coordinates – Apple stores only the zip code. Apple then uses the zip code to select a relevant ad for the customer. Additional details regarding Apple's advertising collection practices are provided in the July 12, 2010 Letter at pages 9-10.

Finally, if a customer has consented to an application's collection and/or use of location information, iOS will provide current location information in response to a request from that application. iOS will provide that customer-approved application with the location of the device only; iOS does not provide applications with direct access to the local cache.

---

[4] When Apple released iOS 4.1 on September 8, 2010, Apple fixed a bug that had caused iOS to send anonymous, geo-tagged information about Wi-Fi hotspots and cell towers to Apple even if the customer had turned off Location Services. For devices running iOS version 4.1 and later, the device does not send this anonymous location information to Apple.

D. Apple's May 4, 2011 iOS Software Update

As discussed above, Apple released an iOS Software Update. After a customer installs this software update on an iOS device:

- if Location Services is off, Apple will not download any crowd-sourced Wi-Fi hotspot and cell tower location information to the device, regardless of whether a specific application requests that information;
- iOS will delete from consolidated.db any cached location information described above – even if Location Services is on;
- iOS will store cached location information, as described above, in cache.db only if Location Services is on and will delete any such cached location information from cache.db if Location Services is turned off;
- iOS will purge from cache.db crowd-sourced Wi-Fi hotspot and cell tower location information records that are older than seven days; and
- iTunes will not back up cache.db.

II. RESPONSES

The following responses represent the current state of our knowledge based on our investigation to date. Our investigation is ongoing, however, and we may continue to discover information responsive to your letter. I will update our responses, as needed, if we locate other responsive materials or information.

1. Why does Apple collect and compile this location data? Why did Apple choose to initiate tracking this data in its iOS 4 operating system?

As noted above, Apple does not track users' locations. Apple collects location-based information for only one purpose – to enhance and improve the services we can offer to our customers.

Apple uses the anonymous, geo-tagged information about Wi-Fi hotspots and cell towers collected from mobile devices, along with other information (such as cellular specifications), to calculate the locations of hotspots and cell towers. Apple stores the calculated locations in Apple's crowd-sourced database. Information from this database enables Apple mobile devices to calculate location quickly (or at all, in the case of non-GPS enabled devices) to the customer's request for current location information.

Apple is using location information associated with automobile traffic data to build a crowd-sourced traffic database with the goal of providing iPhone users an improved traffic service in the next couple of years.

Apple uses location information associated with diagnostic data to evaluate and improve the performance of its mobile hardware and operating system.

Finally, Apple uses location information collected when an ad request is made to calculate a zip code that is used to select a relevant ad for the customer. As noted above, Apple discards the actual location information transmitted from the device to Apple's iAd servers when an ad request is made.

2. Does Apple collect and compile this location data for laptops?

Apple anonymously collects information about Wi-Fi hotpots, such as MAC addresses, from laptops running Mac OS X. Additional details regarding the collection of this information from Mac OS X are provided in the July 12, 2010 Letter at pages 7-8.

3. How is this data generated? (GPS, cell tower triangulation, WiFi triangulation, etc.)

Under the circumstances described above, iOS may use the information contained in the crowd-sourced location database to triangulate the device location when GPS is not available (such as indoors or in basements). If GPS information is available, iOS can determine the device location using GPS satellite data.

4. How frequently is a user's location recorded? What triggers the creation of a record of someone's location?

Following the May 4, 2011 software update, iOS does not record the device location in a file. In versions of iOS 4 prior to the update, iOS wrote a cache copy of the device's single "last known location" to a file named "cache.plist." Specifically, when the device determined its current location, iOS wrote that location to cache.plist, overwriting any previous data that may have been in the file. In other words, only one last known location was stored; previous locations, or locations over time, were not stored by iOS. The next time an application or service requested current location information, iOS used the data in cache.plist, along with other information, to determine the device's then-current location. Any previous location in cache.plist was then overwritten.

5. How precise is this location data? Can it track a user's location to 50 meters, 100 meters, etc.?

The precision with which iOS can calculate a device's location varies based on the quality and quantity of information available to the iOS. For example, if GPS satellite data is not available, iOS may attempt to calculate the device location using only the crowd-sourced locations of Wi-Fi hotspots and cell towers. Because some of those hotspots and cell towers could be more than one hundred miles away, the device location calculated by iOS will only be an approximation.

6. Why is this data not encrypted? What steps will Apple take to encrypt this data?

The local cache is protected with iOS security features. Beginning with the next major release of iOS, the operating system will encrypt any local cache of the hotspot and cell tower location information.

Prior to the update, iTunes backed up the local cache (stored in consolidated.db) as part of the normal device backup if there was a syncing relationship between the device and a computer. The iTunes backup, including consolidated.db, may or may not have been encrypted, depending on the customer's settings in iTunes. After the software update, iTunes does not back up the local cache (now stored in cache.db).

7. Why were Apple consumers never affirmatively informed of the collection and retention of their location data in this manner? Why did Apple not seek affirmative consent before doing so?

Apple has publicly disclosed in several ways the types of information it collects and how it uses that information. Through its Privacy Policy and previous disclosures to questions raised about location based data, Apple has informed its customers of the types of data collected and used by the devices. Apple provided a detailed description of its collection and use of location-based information in the July 27, 2010 Letter. In Apple's April 27, 2011 public response, Apple disclosed additional technical details, including characteristics of the local cache database file.

Apple has taken several measures to inform its customers about the use of location data. First, Apple's Privacy Policy, which is available from links on every page of Apple's website,[5] contains express disclosures regarding Apple's collection and use of location data and non-personal information:

> **Location-Based Services**
>
> To provide location-based services on Apple products, Apple and our partners and licensees may collect, use, and share precise location data, including the real-time geographic location of your Apple computer or device. This location data is collected anonymously in a form that does not personally identify you and is used by Apple and our partners and licensees to provide and improve location-based products and services. For example, we may share geographic location with application providers when you opt in to their location services.
>
> Some location-based services offered by Apple, such as the MobileMe "Find My iPhone" feature, require your personal information for the feature to work.
>
> **********
>
> **Collection and Use of Non-Personal Information**
>
> We also collect non-personal information – data in a form that does not permit direct association with any specific individual. We may collect, use, transfer, and disclose non-personal information

[5] The links take customers to http://www.apple.com/privacy, which may also be accessed by customers directly.

> for any purpose. The following are some examples of non-personal information that we collect and how we may use it:
>
> - We may collect information such as occupation, language, zip code, area code, unique device identifier, location, and the time zone where an Apple product is used so that we can better understand customer behavior and improve our products, services, and advertising.
>
> ...
>
> If we do combine non-personal information with personal information the combined information will be treated as personal information for as long as it remains combined.

Second, Apple's Software License Agreements ("SLAs") for products that provide location-based services similarly provide express disclosures regarding Apple's collection and use of location information. For example, to activate an iPhone, the customer must accept and agree to the iPhone SLA, including the following provision regarding location data:

> 4. Consent to Use of Data.
>
> ...
>
> (b) Location Data. Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide and improve these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone, and location search queries. The location data and queries collected by Apple are collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide and improve location-based products and services. **By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data and queries to provide and improve such products and services.** (emphasis exists in the SLA) You may withdraw this consent at any time by going to the Location Services setting on your iPhone and either turning off the global Location Services setting or turning off the individual location settings of each location-aware application on your iPhone. Not using these location features will not impact the non location-based functionality of your iPhone. When using third party applications

> or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services. ...
>
> At all times your information will be treated in accordance with Apple's Privacy Policy, which is incorporated by reference into this License and can be viewed at: www.apple.com/legal/privacy/.

In addition, every time a customer updates iOS on an iPhone, the customer must again accept and agree to the iPhone SLA.

Third, before any application can collect or use location information, iOS discloses to the customer that the application "would like to use [the customer's] current location" and requests the customer's express consent.

Fourth, before Apple will collect any diagnostic information from an iOS customer, that customer must explicitly agree that Apple may collect and use such information. For example, iPhone customers must click "Agree" in response to the following disclosure:

> You can help Apple improve its products by sending us anonymous diagnostic and usage information about your iPhone.
>
> By clicking "Agree" you agree that Apple may periodically collect and use this information as part of its support services and to improve its products and services. This information is collected anonymously. To learn more about Apple's Privacy Policy, see http://www.apple.com/legal/privacy.

8. Does Apple believe that this conduct is permissible under the terms of its privacy policy? *See* Apple Privacy Policy at "Location-Based Services" (accessed on April 20, 2011), *available at* www.apple.com/privacy.

Apple believes its location-based services and practices are consistent with its Privacy Policy.

9. To whom, if anyone, including Apple, has this data been disclosed? When and why were these disclosures made?

Apple has downloaded portions of the contents of the crowd-sourced database to Apple mobile devices to provide location services to Apple's customers. As discussed above, the hotspot and cell tower location information stored in Apple's crowd-sourced database and downloaded to customer devices is not the anonymous geo-tagged information collected from mobile devices – instead, it comprises the locations of hotspots and cell towers that have been derived by Apple from the anonymous crowd-sourced location data. Apple does not receive any compensation from its customers for supplying the information from the crowd-sourced database, although that service is something that Apple's customers have come to expect when they

purchase an Apple mobile device. The portions of the crowd sourced database stored on a customer's mobile device are protected as discussed above.

With the goal of providing its customers with an improved traffic service, Apple has entered into a confidential relationship with one of its development partners and has shared with this partner subsets of the anonymous location information associated with automobile traffic data collected by Apple. Contractual confidentiality and non-disclosure restrictions protect this anonymous location information, and Apple's development partner is prohibited from sharing this information with any third parties. The terms of Apple's agreement with this development partner are confidential.

As described above, iOS will provide third-party applications with a devices' current location via Apple's application programming interface if that customer consents. Third-party application developers must register as an "Apple Developer" by paying a fee and signing the Registered Apple Developer Agreement and the iOS Developer Program License Agreement (the "PLA"). Registered Apple Developers gain access to the software development kit and other technical resources necessary to develop applications for mobile devices.

The current PLA contains several provisions governing the collection and use of location-based information, including the following:

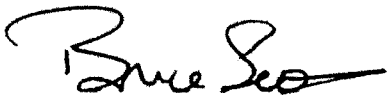
- Developers may collect, use, or disclose to a third party location-based information only with the customer's prior consent and to provide a service or function that is directly relevant to the use of the application;
- Developers must provide information to their customers regarding the use and disclosure of location-based information (*e.g.*, a description on the App Store or adding a link to the applicable privacy policy);
- Developers must take appropriate steps to protect customers' location-based information from unauthorized use or access;
- Developers must comply with applicable privacy and data collection laws and regulations regarding the use or transmission of location-based information;
- Applications must notify and obtain consent from each customer before location data is collected, transmitted, or otherwise used by developers;
- If the customer denies or withdraws consent, applications may not collect, transmit, maintain, process or utilize the customer's location data; and
- Applications must not disable, override, or otherwise interfere with Apple-implemented alerts, including those intended to notify the customer that location-based information is being collected, transmitted, maintained, processed, or used, or intended to obtain consent for such use.

Developers that do not agree to these provisions may not offer applications on the App Store. Apple has the right to terminate the PLA if a developer fails to comply with any of these

provisions. In its Privacy Policy, Apple also notifies customers that "Information collected by third parties, which may include such things as location data or contact details, is governed by their privacy practices. We encourage you to learn about the privacy practices of those third parties."

Other than as described in the prior paragraphs, Apple has not shared or given third parties access to the information collected and stored by iOS.

Sincerely,



Bruce Sewell
General Counsel and Senior Vice
President of Legal and Government
Affairs

Attachments

CNET News
CNET News

- log in
- join CNET

- Home
- Reviews
- *You are here:* News
- Downloads
- Video

Search

Go

- Latest News
- CNET River
- Latest News
- Webware
- Crave
- Business Tech
- Green Tech
- Wireless
- Security
- Blogs
- Video
- Photos
- More *Menu*

Privacy Inc.

Ad Info

Sponsored Links

Verizon Phone
Official Site. Exclusive Deals And Free Offers At Verizon.
verizonwireless.com

Official Site For Nexus S
Equipped With The New Gingerbread. Be The First To Get it. Learn More
www.google.com/nexus

Nokia Astound Now Free
Order the All-New Nokia Astound. Now Free with T-Mobile Contract!
www.NokiaUSA.com/Astound

APRIL 22, 2011 7:08 PM PDT

Android data tied to users? Some say yes

by Declan McCullagh

372 Recommend 444

Google acknowledged today that it collects location

information from Android devices, but downplayed concerns about privacy by saying the information is not "traceable to a specific user."

That claim, it turns out, depends on the definition of "traceable."

According to detailed records provided to CNET by a security researcher, Android phones regularly connect to Google.com and disgorge a miniature data dump that includes time down to the millisecond, current and recent GPS coordinates, nearby Wi-Fi network addresses, and two 16-letter strings representing a device ID that's unique to each phone.

Apple, which **came under fire this week** after reports that approximate location data is stored in perpetuity on iPhones, also collects such data through the Internet. It acknowledged (**PDF**) to Congress last year that "cell tower and Wi-Fi access point information" is "intermittently" collected and "transmitted to Apple" every 12 hours, but has refused to elaborate. (See CNET's **FAQ** on the topic.)

Assembling a database of locations **can raise privacy concerns**. While Android's device ID isn't a name or phone number, it uniquely identifies each phone and is linked to its whereabouts, which means Google might be able to trace the location of an Android phone over months or even years. Less is known about what data Apple collects, including whether a unique device ID is transmitted.

A Google representative said she would not immediately be able to respond to a list of questions posed by CNET this afternoon. The company's statement says: "We provide users with notice and control over the collection, sharing, and use of location in order to provide a better mobile experience on Android devices. Any location data that is sent back to Google location servers is anonymized and is not tied or traceable to a specific user."

Location Privacy

	Store Data	Transmit
Apple	Yes	Yes
Google	Limited	Yes
Microsoft	No	N/A*

* We're waiting for a response from Microsoft, as well as RIM and Nokia.

Source: CNET research

© 2011 CBS Interactive

(Credit: Declan McCullagh/CNET)

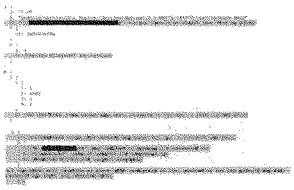
"It's not tied to a user," says **Samy Kamkar**, who provided the Android connection logs to CNET. "But it is a unique identifier to that phone that never changes unless you do a factory reset."

An Android setup screen references these ongoing location updates, saying that choosing to enable location services allows Google to "collect anonymous location data," even when "no applications are running." But that disclosure does not acknowledge that a unique device ID is transmitted. (See **a screen snapshot**.)

It's difficult to know how significant the privacy risks are. That depends in large part on whether Google anonymizes the location information and device ID that it collects from Android devices--and, especially, how long data is kept.

Marc Rotenberg, executive director of the **Electronic Privacy Information Center**, is skeptical of Google's claim that the data is not "traceable" to a specific person. "If you can link a person's address with their activity," he says, "bingo! It's personal data."

Requesting cell phone location information from wireless carriers has **become a staple of criminal investigations**, often without search warrants being sought. It's not clear how often legal requests for these records have been sent to Google and Apple, or whether the companies have required a judge's signature on a search warrant, the most privacy-protective approach, or settled for less.



Excerpts from Android connection-logging done by Samy Kamkar. CNET has redacted his device ID and Wi-Fi MAC address. Click for a larger image.

The Android device ID can be tied to a person without a minimum of number-crunching, said Kamkar, a onetime hacker with a colorful past. Google can determine that "this is probably their home address because they're there at 3 a.m. every single day," he said. And "this is probably their work address because they're there between 9 a.m. and 5 p.m. every day."

Even though police are tapping into the locations of mobile phones thousands of times a year by contacting AT&T, Verizon, and other carriers, the legal ground rules remain unclear, and federal privacy laws written a generation ago **are ambiguous at best**. The Obama Justice Department has claimed that no warrant is required for historical location information. (CNET **was the first** to report on warrantless cell tracking, in 2005.)

"I think it's important that people know what's happening" inside their phones, Kamkar said.

Like iOS devices, Android phones do collect location information in a local file. But they seem to erase it relatively quickly instead of saving it forever. Swedish programer Magnus Eriksson **has highlighted** a portion of the Android source code suggesting a maximum of 50 cell tower locations are retained, which a source close to Google indicates is correct.

Here are the questions, still unanswered, that CNET posed to Google this afternoon:

> I've been looking into this a bit more. It appears that Android phones send an HTTP POST data packet to Google, specifically this URL: http://www.google.com/loc/m/api
>
> Included in the POST packet are a series of strings, including:
> - carrier name
> - time packet was sent, down to the millisecond
> - MAC address, name, signal strength of the Wi-Fi network in use
> - MAC address, name, signal strength for other visible Wi-Fi networks
> - lat/long GPS coordinates of the phone
> - other lat/long pairs and times associated with them (showing motion)

- Two 16-byte strings that are uniquely tied to that Android device

The last field is the important one. It doesn't include a name or phone number, but it is traceable to a specific user. If I'm at a certain home address every evening, and at a certain work address every day from 9 a.m.-5 p.m., it's pretty clear who I am.

So my questions are:

- Why doesn't Google randomize those two 16-byte strings (let's call them the device ID) on an hourly or daily basis?
- Given a street address or pair of GPS coordinates, is Google able to produce the complete location logs associated with that device ID, if legally required to do so?
- Given a device ID, is Google able to produce the complete location logs associated with it, if legally required to do so?
- Given a MAC address of an access point, is Google able to produce the device IDs and location data associated with it, if legally required to do so?
- How long are these location logs and device ID logs kept?
- If they are partially anonymized after a certain time, how is that done, and can those records be restored from a backup if Google is legally required to do so?
- How many law enforcement requests or forms of compulsory process have you received for access to any portion of this database?
- Why have you assembled this location and device ID database? My current theory is that it shows traffic on Google Maps where street data would be otherwise unavailable (a very useful feature, but one that doesn't appear to require keeping fixed device IDs).
- How are the device ID strings calculated?
- Did Alma Whitten approve this form of device ID logging? If not, what internal process did you use to vet any possible privacy concerns?
- If Google knows that a Gmail user is connecting from a home network IP address every evening, it would be trivial to link that with an Android phone's device ID that also connects via that IP address. Does Google do that?
- Does Android store only a maximum of 50 cell records and 200 Wi-Fi records?

Disclosure: Declan McCullagh is married to a Google employee not involved in this issue.

Declan McCullagh

Like 210 Full Profile E-mail Declan McCullagh

Declan McCullagh is the chief political correspondent for CNET. Declan previously was a reporter for Time and the Washington bureau chief for Wired and wrote the Taking Liberties section and Other People's Money column for CBS News' Web site.

Prosecuting Computer Crimes

Computer Crime and
Intellectual Property Section
Criminal Division

Published by
Office of Legal Education
Executive Office for
United States Attorneys

The Office of Legal Education intends that this book be used by Federal prosecutors for training and law enforcement purposes, and makes no public release of it. Individuals receiving the book in training are reminded to treat it confidentially.

The contents of this book provide internal suggestions to Department of Justice attorneys. Nothing in it is intended to create any substantive or procedural rights, privileges, or benefits enforceable in any administrative, civil, or criminal matter by any prospective or actual witnesses or parties. *See United States v. Caceres*, 440 U.S. 741 (1979).

Michael Battle
Director, EOUSA

Michael W. Bailie
Director, OLE

OLE
Litigation
Series

Ed Hagen
Assistant Director,
OLE

Scott Eltringham
Computer Crime
and Intellectual
Property Section
Editor in Chief

Computer Crime & Intellectual Property Section
United States Department of Justice

Chapter 3

The Stored Communications Act

A. Introduction

- The SCA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA's classifications are summarized in the chart that appears in Section F of this chapter.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.[1] There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available "to the public" required more strict regulation than services not available to the public. (Perhaps this judgment reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy.) To protect the array of privacy interests identified by its drafters, the SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.

Agents and prosecutors must apply the various classifications devised by the SCA's drafters to the facts of each case to figure out the proper procedure for obtaining the information sought. First, they must classify the network service provider (*e.g.*, does the provider provide "electronic communication service," "remote computing service," or neither). Next, they must classify the information sought (*e.g.*, is the information content "in electronic storage," content held by a remote computing service, a non-content record pertaining

to a subscriber, or other information enumerated by the SCA). Third, they must consider whether they are seeking to compel disclosure or seeking to accept information disclosed voluntarily by the provider. If they seek compelled disclosure, they need to determine whether they need a search warrant, a 2703(d) court order, or a subpoena to compel the disclosure. If they are seeking to accept information voluntarily disclosed, they must determine whether the statute permits the disclosure. The chart contained in Section F of this chapter provides a useful way to apply these distinctions in practice.

The organization of this chapter will follow the SCA's various classifications. Section B explains the SCA's classification structure, which distinguishes between providers of "electronic communication service" and providers of "remote computing service." Section C explains the different kinds of information that providers can divulge, such as content "in electronic storage" and "records . . . pertaining to a subscriber." Section D explains the legal process that agents and prosecutors must follow to compel a provider to disclose information. Section E looks at the flip side of this problem and explains when providers may voluntarily disclose account information. A summary chart appears in Section F. Section G discusses important issues that may arise when agents obtain records from network providers: steps to preserve evidence, steps to prevent disclosure to subjects, Cable Act issues, and reimbursement to providers. Section H discusses the Fourth Amendment's application to stored electronic communications. Finally, Section I discusses the remedies that courts may impose following violations of the SCA.

B. Providers of Electronic Communication Service vs. Remote Computing Service

The SCA protects communications held by two defined classes of network service providers: providers of "electronic communication service," *see* 18 U.S.C. § 2510(15), and providers of "remote computing service," *see* 18 U.S.C. § 2711(2). Careful examination of the definitions of these two terms is necessary to understand how to apply the SCA.

1. Electronic Communication Service

An electronic communication service ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). (For a discussion of the definitions of wire and electronic communications, see Chapter 4.D.2.) For example, "telephone companies and electronic mail companies" generally act as ECS providers. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568; *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900-03 (9th Cir. 2008) (text messaging service provider is an ECS); *In re Application of United States*, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (cell phone service provider is an ECS); *Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) (host of electronic bulletin board is ECS); *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004) (AOL is an ECS).

Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city providing pager service to its police officers was a provider of ECS); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system

accessed through separate computer terminals can be a provider of ECS). In *In re Application of United States*, 349 F.3d 1132, 1138-41 (9th Cir. 2003), the Ninth Circuit held that a company operating a system that enabled drivers to communicate with designated call centers over a cellular telephone network was an ECS, though it also noted that the situation would have been entirely different "if the Company merely used wire communication as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a 'drive-thru' restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane." *Id.* at 1141 n.19.

A provider cannot provide ECS with respect to a communication if the service did not provide the ability to send or receive *that* communication. *See Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (video game manufacturer that accessed private email of users of another company's bulletin board service was not a provider of electronic communication service); *State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (financing company that used fax machines and computers but did not provide the ability to send or receive communications was not provider of electronic communication service).

Significantly, a mere user of ECS provided by another is not a provider of ECS. For example, a commercial website is not a provider of ECS, even though it may send and receive electronic communications from customers. In *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001), the plaintiff argued that Amazon.com (to whom plaintiff sent his name, credit card number, and other identification information) was an electronic communications service provider because "without recipients such as Amazon.com, users would have no ability to send electronic information." The court rejected this argument, holding that Amazon was properly characterized as a user rather than a provider of ECS. *See id. See also United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (a home computer connected to the Internet is not an ECS); *In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 309-10 (E.D.N.Y. 2005) (airline that operated website that enabled it to communicate with customers was not an ECS); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) (ECS "does not encompass businesses selling traditional products or services online"); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 508-09 (S.D.N.Y. 2001) (distinguishing ISPs that provide ECS from websites that are users of ECS). However, "an online business or retailer may be considered an electronic communication service provider if the business has a website that offers customers the ability to send messages or communications to third parties." *Becker v. Toca*, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008).

2. Remote Computing Service

The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. H.R. Rep. No. 99-647, at 23 (1986). A server that allows users to store data for future retrieval also provides an RCS. *See Steve Jackson Games, Inc. v. United States*

Secret Service, 816 F. Supp. 432, 442-43 (W.D. Tex. 1993) (provider of bulletin board services was a remote computing service), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994). Importantly, an entity that operates a website and its associated servers is not an RCS, unless of course the entity offers a storage or processing service through the website. For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS. *See In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d at 310; *see also United States v. Standefer*, 2007 WL 2301760, at *5 (S.D. Cal. Aug. 8, 2007) (holding that e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users").

Under the definition provided by § 2711(2), a service can only be a "remote computing service" if it is available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open "to the public" because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit held that a text messaging service provider was an ECS and therefore not an RCS. *See Quon*, 529 F.3d at 902-03. However, this "either/or" approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. *See* H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit's analysis in *Quon* and stated that a provider "may be deemed to provide both an ECS and an RCS to the same customer." *Flagg, v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

C. Classifying Types of Information Held by Service Providers

Network service providers can store different kinds of information relating to an individual customer or subscriber. Consider the range of information that an ISP may typically store regarding one of its customers. It may have the customer's subscriber information, such as name, address, and credit card number. It may have logs revealing when the customer logged on and off the service, the IP addresses assigned to the customer, and other more detailed logs pertaining to what the customer did while online. The ISP may also have the customer's opened, unopened, draft, and sent emails.

When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of the SCA. The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). *See* 18 U.S.C. §§ 2510(8), 2703. In addition, as described below, the SCA creates substantially different protections for contents in "electronic storage" in an ECS and contents stored by a provider of RCS.

1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2)

Section 2703(c)(2) lists the categories of basic subscriber and session information:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, "any temporarily assigned network address" includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a "temporarily assigned network address." This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

2. Records or Other Information Pertaining to a Customer or Subscriber

Section 2703(c)(1) covers a second type of information: "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." This is a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section. As one court explained, "a record means something stored or archived. The term information is synonymous with data." *In re United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511. *See also In re Application of United States*, 509 F. Supp. 76, 80 (D. Mass. 2007) (historical cell-site information fall within scope of § 2703(c)(1)); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and detailed internet address of sites accessed" by a user constituted "a record or other information pertaining to a subscriber or customer of such service" under the SCA); *Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or

customer of such service," not contents, for a telephone account); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber" rather than contents). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827, at 17, 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

3. Contents and "Electronic Storage"

The contents of a network account are the actual files (including email) stored in the account. *See* 18 U.S.C. § 2510(8) ("'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). For example, stored emails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject lines of emails are also contents. *Cf. Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages allow "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

The SCA further divides contents into two categories: contents in "electronic storage" held by a provider of electronic communication service, and contents stored by a remote computing service. (In addition, contents that fall outside of these two categories are not protected by the SCA.) Importantly, "electronic storage" is a statutorily defined term. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is " (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Moreover, the definition of "electronic storage" is important because, as explained in Section D below, contents in "electronic storage" for less than 181 days can be obtained only with a warrant.

Unfortunately, as a result of the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), there is now a split between two interpretations of "electronic storage"--a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit. Both interpretations are discussed below. As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in *Theofel*, but law enforcement elsewhere may continue to apply the traditional interpretation of "electronic storage."

As traditionally understood, "electronic storage" refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in "electronic storage." *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the communication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in "temporary, intermediate storage" and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2004) (stating that email in post-transmission storage was

not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in "electronic storage." Messages posted to an electronic "bulletin board" or similar service are also not in "electronic storage" because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc.*, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), adopted by 2005 WL 1266435 (M.D. Fla. May 27, 2005), aff'd on other grounds, 450 F.3d 1314 (11th Cir. 2006).

Furthermore, the "backup" component of the definition of "electronic storage" refers to copies made by an ISP to ensure system integrity. As one district court explained, the backup component "protects the communication in the event the system crashes before transmission is complete. The phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage.'" *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), aff'd in part on other grounds, 352 F.3d 107, 114 (3d Cir. 2004) (affirming the SCA portion of the district court's ruling on other grounds); *see also United States v. Weaver*, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (interpreting "electronic storage" to exclude previously sent email stored by web-based email service provider); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory language and legislative intent and holding that cookies fall outside of the definition of "electronic storage" because of their "long-term residence on plaintiffs' hard drives"); H.R. Rep. No. 99-647, at 65 (1986) (noting congressional intent that opened email left on a provider's system be covered by provisions of the SCA relating to remote computing services, rather than provisions relating to communications in "electronic storage").

This narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), in which the court held that email messages were in "electronic storage" regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of "electronic storage." *Id.* at 1075-77. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the "backup" portion of the definition of "electronic storage," because such a message "functions as a 'backup' for the user." *Id.* at 1075. However, CCIPS has consistently argued that the Ninth Circuit's broad interpretation of the "backup" portion of the definition of "electronic storage" should be rejected. There is no way for a service provider to determine whether a previously opened email on its servers is a backup for a copy of the email stored by a user on his computer, as the service provider simply cannot know whether the underlying email remains stored on the user's computer. Essentially, the Ninth Circuit's reasoning in *Theofel* confuses "backup protection" with ordinary storage of a file.

Although prosecutors within the Ninth Circuit are bound by *Theofel*, law enforcement elsewhere may continue to apply the traditional narrow interpretation of "electronic storage," even when the data sought is within the Ninth Circuit. Recent lower court decisions addressing the scope of "electronic storage" have split between the traditional interpretation and the *Theofel* approach. *Compare United States v. Weaver*, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (rejecting Theofel), *and Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that access to opened email in account held by non-public service provider did not violate the SCA), *with Bailey v. Bailey*, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (endorsing *Theofel*), *and Cardinal Health 414, Inc. v. Adams*, 482 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (same). Prosecutors confronted with *Theofel*-related issues should consult CCIPS at (202) 514-1026 for further assistance.

4. Illustration of the SCA's Classifications in the Email Context

An example illustrates how the SCA's categories work in practice outside the Ninth Circuit, where *Theofel* does not apply. Imagine that Joe sends an email from his account at work ("joe@goodcompany.com") to the personal account of his friend Jane ("jane@localisp.com"). The email will stream across the Internet until it reaches the servers of Jane's Internet service provider, here the fictional LocalISP. When the message first arrives at LocalISP, LocalISP is a provider of ECS with respect to that message. Before Jane accesses LocalISP and retrieves the message, Joe's email is in "electronic storage." Once Jane retrieves Joe's email, she can either delete the message from LocalISP's server or else leave the message stored there. If Jane chooses to store the email with LocalISP, LocalISP is now a provider of RCS (and not ECS) with respect to the email sent by Joe. The role of LocalISP has changed from a transmitter of Joe's email to a storage facility for a file stored remotely for Jane by a provider of RCS.

Next imagine that Jane responds to Joe's email. Jane's return email to Joe will stream across the Internet to the servers of Joe's employer, Good Company. Before Joe retrieves the email from Good Company's servers, Good Company is a provider of ECS with respect to Jane's email (just like LocalISP was with respect to Joe's original email before Jane accessed it). When Joe accesses Jane's email message and the communication reaches its destination (Joe), Good Company ceases to be a provider of ECS with respect to that email (just as LocalISP ceased to be a provider of ECS with respect to Joe's original email when Jane accessed it). Unlike LocalISP, however, Good Company does not become a provider of RCS if Joe decides to store the opened email on Good Company's server. Rather, for purposes of this specific message, Good Company is a provider of neither ECS nor RCS. Good Company does not provide RCS because it does not provide services to the public. *See* 18 U.S.C. § 2711(2) ("[T]he term 'remote computing service' means the provision *to the public* of computer storage or processing services by means of an electronic communications system." (emphasis added)); *Andersen Consulting*, 991 F. Supp. at 1043. Because Good Company provides neither ECS nor RCS with respect to the opened email in Joe's account, the SCA no longer regulates access to this email, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened email in Joe's account drops out of the SCA.

Finally, consider the status of the other copies of the emails in this scenario: Jane has downloaded a copy of Joe's email from LocalISP's server to her personal computer at home, and Joe has downloaded a copy of Jane's email from Good Company's server to his office desktop computer at work. The SCA governs neither. Although these computers contain copies of emails, these copies are not stored on the server of a third-party provider of RCS or ECS, and therefore the SCA does not apply. Access to the copies of the communications stored in Jane's personal computer at home and Joe's office computer at work is governed solely by the Fourth Amendment. *See generally* Chapters 1 and 2.

As this example indicates, a single provider can simultaneously provide ECS with regard to some communications and RCS with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others. A chart illustrating these issues appears in Section F of this chapter. Sample language that agents may use appears in Appendices B, E, and F.

D. Compelled Disclosure Under the SCA

Section 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account

records and basic subscriber and session information.

Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms are as follows:

1) Subpoena;

2) Subpoena with prior notice to the subscriber or customer;

3) § 2703(d) court order;

4) § 2703(d) court order with prior notice to the subscriber or customer; and

5) Search warrant.

One feature of the compelled disclosure provisions of the SCA is that greater process generally includes access to information that cannot be obtained with lesser process. Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified because it can authorize a broader disclosure. Note, however, the notice requirement must be considered separately under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a 2703(d) order without subscriber notice.

Two circumstances allow the government to compel disclosure of information under the SCA without a subpoena. First, when investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing. *See* 18 U.S.C. § 2703(c)(1)(D). Second, the government may compel a service provider to disclose non-content information pertaining to a customer or subscriber when the government has obtained the customer or subscriber's consent. *See* 18 U.S.C. § 2703(c)(1)(C).

1. Subpoena

The SCA permits the government to compel disclosure of the basic subscriber and session information (discussed above in Section C.1) listed in 18 U.S.C. § 2703(c)(2) using a subpoena:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

18 U.S.C. § 2703(c)(2).

Agents can also use a subpoena to obtain information that is outside the scope of the SCA. The hypothetical email exchange between Jane and Joe discussed in Section C of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened email on Good Company's server. Accordingly, § 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling Good Company to divulge the communication just as they would if the SCA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by the SCA and may be

obtained using a subpoena according to the same rationale. *Cf. Organizacion JD Ltda. v. United States Dep't of Justice*, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in the SCA).

The legal threshold for issuing a subpoena is low. *See United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950). Investigators may obtain disclosure pursuant to § 2703(c)(2) using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. *See* 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by the Inspector General Act may be used. *See* 5 U.S.C. app. 3 § 6(a)(4). Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to Fed. R. Crim. P. 6(e). At least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. *See FTC v. Netscape Commc'ns Corp.*, 196 F.R.D. 559, 561 (N.D. Cal. 2000) (holding that civil discovery subpoena did not fall within the meaning of "trial subpoena"). Sample subpoena language appears in Appendix E.

2. Subpoena with Prior Notice to the Subscriber or Customer

Agents who obtain a subpoena and *either* give prior notice to the subscriber or comply with the delayed notice provisions of § 2705(a) may obtain:

1) everything that can be obtained using a subpoena without notice;

2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and

3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2).

Outside the Ninth Circuit (which is now governed by *Theofel*), this third category will include opened and sent email. Agents outside of the Ninth Circuit can therefore obtain such email (and other stored electronic or wire communications in "electronic storage" more than 180 days) using a subpoena, provided they comply with the SCA's notice provisions. However, in light of *Theofel*, some service providers may be reluctant to produce opened or sent email less than 181 days old without a warrant. Prosecutors moving to compel compliance with a subpoena for such email should contact CCIPS at (202) 514-1026 for assistance. In the Ninth Circuit, agents can continue to subpoena communications that have been in "electronic storage" over 180 days.

The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. *See* 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) permits notice to be delayed for ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. *See* 18 U.S.C. § 2705(a)(2) (defining "adverse result"); 18 U.S.C. § 2705(a)(6) (defining "supervisory official"). This provision of the SCA provides a permissible way for the government to delay notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. The government may extend the delay of notice for additional 90-day periods through additional certifications that meet the "adverse result" standard of section 2705(b). *See* 18 U.S.C. § 2705(a)(4). Upon expiration of the delayed notice period, the statute requires the government to send a copy of the request or process along with a letter

explaining the delayed notice to the customer or subscriber. *See* 18 U.S.C. § 2705(a)(5).

3. Section 2703(d) Order

- Agents need a § 2703(d) court order to obtain most account logs and most transactional records.

Agents who obtain a court order under 18 U.S.C. § 2703(d) may obtain:

> 1) anything that can be obtained using a subpoena without notice; and
>
> 2) all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court, or equivalent state court judge. *See* 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order,

> the governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d).

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1109-10 (D. Kan. 2000) (concluding that a conclusory application for a 2703(d) order "did not meet the requirements of the statute."). As the Tenth Circuit has noted, the "specific and articulable facts" standard of 2703(d) "derives from the Supreme Court's decision in [*Terry v. Ohio*, 392 U.S. 1 (1968)]." *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008). The House Report accompanying the 1994 amendment to section 2703(d) included the following analysis:

> This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 102-827, at 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511-12 (quoted in full in *Kennedy*, 81 F. Supp. 2d at 1109 n.8). As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. A sample § 2703(d) application and order appears in Appendix B.

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. The SCA permits a judge to enter 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. *See* 18 U.S.C. § 2703(d) (stating that "*any court* that is a court of competent jurisdiction" may issue a

2703(d) order) (emphasis added); 18 U.S.C. § 2711(3) (stating that "'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographical limitation"); 18 U.S.C. § 3127(2) (defining "court of competent jurisdiction").

Section 2703(d) orders may also be issued by state courts. *See* 18 U.S.C. §§ 2711(3), 3127(2)(B) (defining "court of competent jurisdiction" to include "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device"). However, the statute provides that when a state governmental entity seeks a 2703(d) order, the order "shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Moreover, although the statute explicitly allows federal courts to issue 2703(d) orders to providers outside of the court's district, it is silent on whether state courts have such authority.

4. 2703(d) Order with Prior Notice to the Subscriber or Customer

- Investigators can obtain everything associated with an account except for unopened email or voicemail stored with a provider for 180 days or less using a 2703(d) court order that complies with the notice provisions of § 2705.

Agents who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

1) everything that can be obtained using a § 2703(d) court order without notice;

2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days," 18 U.S.C. § 2703(a); and

3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2).

As a practical matter, except in the Ninth Circuit, this means that the government can use a 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B) to obtain the full contents of a subscriber's account except unopened email and voicemail that have been in the account for 180 days or less. In the Ninth Circuit, which is governed by *Theofel*, agents can continue to use 2703(d) orders to obtain communications in "electronic storage" over 180 days. Following *Theofel*, some providers have resisted producing email content less than 181 days old in response to a 2703(d) order, even when the 2703(d) order is issued by a court outside the Ninth Circuit. Prosecutors encountering this problem should contact CCIPS at (202) 514-1026 for assistance.

As an alternative to giving prior notice, law enforcement can obtain an order delaying notice for up to ninety days when notice would seriously jeopardize the investigation. *See* 18 U.S.C. § 2705(a). In such cases, prosecutors generally will obtain this order by including an appropriate request in the 2703(d) application and proposed order; sample language appears in Appendix B. Prosecutors may also apply to the court for extensions of the delay. *See* 18 U.S.C. § 2705(a)(4). The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. *See* Section D.2., *supra*. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual;

[lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). The applicant must satisfy this standard anew in every application for an extension of the delayed notice.

5. Search Warrant

- Investigators can obtain everything associated with an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under § 2703 may obtain:

1) everything that can be obtained using a § 2703(d) court order with notice; and

2) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a).

In other words, agents can obtain any content or non-content information pertaining to an account by obtaining a search warrant "issued using the procedures described in" Fed. R. Crim. P. 41. 18 U.S.C. § 2703(a).

Search warrants issued under § 2703 have several noteworthy procedural features. First, although most search warrants obtained under Rule 41 are limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. *See United States v. Berkos*, 543 F.3d 392, 396-98 (7th Cir. 2008); *In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007); *In re Search Warrant*, 2005 WL 3844032, at *5-6 (M.D. Fla. 2006) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction"). State courts may also issue warrants under § 2703, but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. Second, obtaining a search warrant obviates the need to give notice to the subscriber. *See* 18 U.S.C. § 2703(b)(1)(A); Fed. R. Crim. P. 41(f)(1)(C).

Third, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant. *See* 18 U.S.C. § 2703(g) (stating that the presence of an officer is not required for service or execution of a § 2703 warrant); *United States v. Bach*, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment).

Fourth, a two-step process is often used to obtain the content of communications under a § 2703 warrant. First, the warrant directs the service provider to produce all email from within the specified account or accounts. Second, the warrant authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized "items to be seized" under the warrant.

Otherwise, as a practical matter, § 2703 search warrants are obtained much like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41.

E. Voluntary Disclosure

- Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. The SCA imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

The voluntary disclosure provisions of the SCA appear in 18 U.S.C. § 2702. These provisions govern when a provider of RCS or ECS can disclose contents and other information voluntarily, both to the government and non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, agents must rely on compelled disclosure provisions and obtain the appropriate legal orders.

When considering whether a provider of RCS or ECS can disclose contents or records, the first question is whether the relevant service offered by the provider is available "to the public." *See* Section B, above. If the provider does not provide the applicable service "to the public," then the SCA does not place any restrictions on disclosure. *See* 18 U.S.C. § 2702(a). For example, in *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed to the *Wall Street Journal* emails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated the SCA. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public:

> [G]iving Andersen access to [UOP's] e-mail system is not equivalent to providing e-mail to the public. Andersen was hired by UOP to do a project and as such, was given access to UOP's e-mail system similar to UOP employees. Andersen was not any member of the community at large, but a hired contractor.

Id. at 1043. Because UOP did not provide services to the public, the SCA did not prohibit disclosure of contents belonging to UOP's "subscribers." *See id.*

If the services offered by the provider *are* available to the public, then the SCA forbids both the disclosure of contents to any third party and the disclosure of other records *to any governmental entity* unless a statutory exception applies. Even a public provider may disclose customers' *non-content* records freely to any person other than a government entity. *See* 18 U.S.C. §§ 2702(a)(3), (c)(6). Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

The SCA allows the voluntary disclosure of contents when:

> 1) the disclosure is made to the intended recipient of the communication, with the consent of the sender or intended recipient, to a forwarding address, or pursuant to specified legal process, § 2702(b)(1)-(4);
>
> 2) in the case of a remote computing service, the disclosure is made with the consent of a subscriber, § 2702(b)(3);[2]
>
> 3) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(b)(5);

4) the disclosure is submitted "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A," § 2702(b)(6);

5) the disclosure is made to a law enforcement agency "if the contents . . . were inadvertently obtained by the service provider . . . [and] appear to pertain to the commission of a crime," § 2702(b)(7); or

6) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." § 2702(b)(8).

The SCA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:

1) the disclosure is made "with the lawful consent of the customer or subscriber," or "as otherwise authorized in section 2703," § 2702(c)(1)-(2);

2) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(c)(3);

3) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," § 2702(c)(4); or

4) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A." § 2702(c)(5).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and of service providers themselves outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

F. Quick Reference Guide

	Voluntary Disclosure Allowed?		How to Compel Disclosure	
	Public Provider	Non-Public	Public Provider	Non-Public
Basic subscriber, session, and billing information*	No, unless 2702(c) exception applies 2702(a)(3)	Yes 2702(a)(3)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)
Other transactional and account records	No, unless 2702(c) exception applies	Yes 2702(a)(3)	2703(d) order or search warrant	2703(d) order or search warrant

	2702(a)(3)		2703(c)(1)	2703(c)(1)
Retrieved communications and the content of other stored files†	No, unless 2702(b) exception applies 2702(a)(2)	Yes 2702(a)(2)	Subpoena with notice; 2703(d) order with notice; or search warrant* 2703(b)	Subpoena; SCA does not apply* 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)†	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)†	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Search warrant 2703(a)	Search warrant 2703(a)

* *See* 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.

† Includes the content of voice communications.

* For investigations occurring in the Ninth Circuit, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow *Theofel* even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

G. Working with Network Providers: Preservation of Evidence, Preventing Disclosure to Subjects, Cable Act Issues, and Reimbursement

Law enforcement officials who procure records under the SCA quickly learn the importance of communicating with network service providers. Communication is necessary because every network provider works differently. Some providers retain very complete records for a long period of time; others retain few records, or even none. Some providers can comply easily with law enforcement requests for information; others struggle to comply with even simple requests. These differences result from varied philosophies, resources, hardware, and software among network service providers. Because of these differences, it is often advisable for agents to

communicate with a network service provider (or review the provider's law enforcement compliance guide) to learn how the provider operates *before* obtaining a legal order that compels the provider to act.

The SCA contains two provisions designed to aid law enforcement officials working with network service providers. When used properly, these provisions help ensure that providers will not delete needed records or notify others about the investigation.

1. Preservation of Evidence under 18 U.S.C. § 2703(f)

- Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests have no prospective effect, however.

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, the SCA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Specifically, § 2703(f)(1) states:

> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should be adequate, a fax or an email is safer practice because it both provides a paper record and guards against misunderstanding. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. *See* 18 U.S.C. § 2703(f)(2). A sample § 2703(f) letter appears in Appendix C.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4.

A second limitation of § 2703(f) is that some providers may be unable to comply effectively with § 2703(f) requests, or they may be unable to comply without taking actions that potentially could alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication: agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects. Investigators with questions about a provider's practices may also contact CCIPS at (202) 514-1026 for further assistance.

2. Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order

Section § 2705(b) states:

> A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b).

This language permits agents to apply for a court order directing network service providers not to disclose the existence of legal process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a 2703(d) order or 2703 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of information using a subpoena, they must apply separately for this order.

3. The Cable Act, 47 U.S.C. § 551

- The Cable Act restricts government access to cable operator records only when the records relate to ordinary cable services. It does not restrict government access to records relating to Internet access or telephone service provided by a cable operator.

In 1984, Congress passed the Cable Communications Policy Act ("the Cable Act"), 47 U.S.C. § 521 *et seq.* Originally, 47 U.S.C. § 551 set forth a restrictive system of rules governing law enforcement access to records possessed by a cable company. Under these rules, even a search warrant was insufficient to gain access to cable company records. The government could obtain "personally identifiable information concerning a cable subscriber" only by overcoming a heavy burden of proof at an in-court adversary proceeding, as specified in 47 U.S.C. § 551(h).

After the 1984 passage of the Cable Act, cable companies began to provide Internet access and telephone service. Some cable companies asserted that the stringent disclosure restrictions of the Cable Act governed not only their provision of traditional cable programming services, but also their provision of Internet and telephone services. Congress responded by amending the Cable Act to specify that its disclosure restrictions apply only to records revealing what ordinary cable television programming a customer purchases, such as particular premium channels or "pay per view" shows. *See* USA-PATRIOT Act § 211, 115 Stat. 272, 283-84 (2001). In particular, cable operators may disclose subscriber information to the government pursuant to the SCA, Title III, and the Pen/Trap statute, except for "records revealing cable subscriber

selection of video programming." 47 U.S.C. § 551(c)(2)(D). Records revealing subscriber selection of video programming remain subject to the restrictions of 47 U.S.C. § 551(h).[3]

4. Reimbursement

- When a government entity obtains information pursuant to the SCA, the network provider may be entitled to reimbursement for its reasonable costs incurred in supplying the information.

In general, persons and entities are not entitled to reimbursement for complying with federal legal process unless there is specific federal statutory authorization. *See Blair v. United States*, 250 U.S. 273, 281 (1919) (discussing possibility of reimbursement for grand jury testimony). "It is beyond dispute that there is in fact a public obligation to provide evidence . . . and that this obligation persists no matter how financially burdensome it may be." *Hurtado v. United States*, 410 U.S. 578, 589 (1973) (stating that the Fifth Amendment does not require compensation for the performance of a public duty). However, in many (but not all) circumstances, the SCA requires government entities obtaining the contents of communications, records, or other information pursuant to the SCA to reimburse the disclosing person or entity. *See* 18 U.S.C. § 2706.

Section 2706 generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." 18 U.S.C. § 2706(a). Significantly, this section only requires reimbursement when the government actually obtains communication content, records, or other information. Thus, the government is not required to pay for costs incurred by a provider in responding to a 2703(f) preservation letter unless the government later obtains the preserved records.

The amount of the fee required under § 2706(a) "shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court." 18 U.S.C. § 2706(b). In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity. A cost accounting will help ensure that the provider is not seeking reimbursement for indirect costs or activities that were not reasonably necessary to the production.

In addition, the SCA contains a reimbursement exception that precludes reimbursement in specific circumstances. The reimbursement requirement "does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703," unless a court determines that the information sought by the government is "unusually voluminous" or "caused an undue burden on the provider." 18 U.S.C. § 2706(c).

The reimbursement exception of § 2706(c) applies only to records and other information "maintained by" a communications common carrier. In *Ameritech Corp. v. McCann*, 403 F.3d 908, 912 (7th Cir. 2005), the Seventh Circuit held that reports of who placed calls to a specified customer were not "maintained by" Ameritech. Ameritech's computer system recorded calls made by a customer, but it did not automatically keep or generate a list of the calls made to a customer. Compiling such a list required substantial computation time. According to the court, Ameritech "maintains" bills and equivalent statements, and the government can therefore get such "raw information" for free. However,

when the government requires Ameritech to create a report, the government must provide compensation. Prosecutors outside the Seventh Circuit are not bound by *Ameritech*, and there is a reasonably strong argument that its interpretation of § 2706(c) is flawed. Under this alternative interpretation, any information stored by a carrier is "maintained by" the carrier, and questions regarding the difficulty of producing information can be evaluated under the "undue burden" standard of § 2706(c).

H. Constitutional Considerations

Defendants sometimes raise constitutional challenges to compelled disclosure of information from communication service providers. They typically argue that use of a 2703(d) order or a subpoena (rather than a warrant) to compel disclosure of information violated the Fourth Amendment. These claims fail for two reasons. First, the defendant may have no reasonable expectation of privacy in the information obtained from the service provider. Second, the Fourth Amendment generally permits the government to compel a provider to disclose information in an account when the provider has access to and control over the targeted information, regardless of whether the account user has a reasonable expectation of privacy in the targeted information.

It is now well established that a customer or subscriber has no reasonable expectation of privacy in her subscriber information or transactional records. In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court held that a defendant had no reasonable expectation of privacy in his bank records because the records were not his "private papers" but were "the business records of the banks" in which the defendant could "assert neither ownership nor possession." *Id.* at 440. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id.* at 443 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). The Court relied upon the principles of *Miller* in *Smith v. Maryland*, 442 U.S. 735 (1979), in which it held that a defendant had no reasonable expectation of privacy in dialed telephone numbers obtained from the phone company. *Id.* at 745-46.

Courts have now extended this *Miller/Smith* analysis to network accounts, holding that individuals retain no Fourth Amendment privacy interest in subscriber information and transactional records. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in source or destination addresses of email or the IP addresses of websites visited); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holders' subscriber information obtained from communication service provider).

In contrast, whether a user has a reasonable expectation of privacy in the contents of communications stored in her account will depend on the facts and circumstances associated with the account. In *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 906 (9th Cir. 2008), the Ninth Circuit rejected "a monolithic view of text message users' reasonable expectation of privacy," explaining that "this is necessarily a context-sensitive inquiry." *Compare Quon*, 529 F.3d at 906-08 (finding reasonable expectation of privacy in pager messages based on an "informal policy that the text messages would not be audited"), and *Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account), aff'd, 492 F.3d 50 (1st Cir. 2007), *with Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy) and *Guest v.*

Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding that disclaimer on private bulletin board service defeated expectation of privacy in postings). *See also United States v. Young*, 350 F.3d 1302, 1307-08 (11th Cir. 2003) (Federal Express customer had no reasonable expectation of privacy in the contents of a package based on terms of service authorizing Federal Express to inspect packages).

Critically, however, even if a user has a reasonable expectation of privacy in an item, a subpoena may be used to compel the production of the item, provided the subpoena is reasonable. *See United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976). The Fourth Amendment imposes a probable cause requirement *only* on the issuance of warrants. *See* U.S. Const. amend.-IV ("and no Warrants shall issue, but upon probable cause"). A century of Supreme Court case law demonstrates that reasonable subpoenas comply with the Fourth Amendment. *See Wilson v. United States*, 221 U.S. 361, 376 (1911) ("there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced"); *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 208 (1946); *United States v. Dionisio*, 410 U.S. 1, 9-12 (1973); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984). The rule for when a subpoena is reasonable and thus complies with the Fourth Amendment is also well-established: "the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *Donovan*, 464 U.S. at 415 (quoting *See v. City of Seattle*, 387 U.S. 541, 549 (1967)). Finally, the Fourth Amendment does not require that notice be given to the target of an investigation in third-party subpoena cases. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743, 749-51 (1984).

In general, the cases indicate that the government may compel an entity to disclose any item that is within its control and that it may access. *See United States v. Barr*, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (subpoena served on private third-party mail service for the defendant's mail in the third party's possession); *Schwimmer v. United States*, 232 F.2d 855, 861-63 (8th Cir. 1956) (subpoena served on third-party storage facility for the defendant's private papers in the third party's possession); *Newfield v. Ryan*, 91 F.2d 700, 702-05 (5th Cir. 1937) (subpoena served on telegraph company for copies of defendants' telegrams in the telegraph company's possession). This rule is supported both by the rule that a party with "joint access or control for most purposes" may consent to a search, *see United States v. Matlock*, 415 U.S. 164, 171 n.7 (1974), and also by the rule that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443.

As a practical matter, there is good reason to believe that network service providers will typically have sufficient access to and control over stored communications on their networks to produce the communications in response to compulsory process. Terms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email. For example, at the time of this writing, Yahoo!'s terms of service confirm its right in its "sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Services," as well as to access and disclose email to comply with legal process. Terms of service similar to Yahoo!'s were sufficient to establish Federal Express's common authority over the contents of a package in *Young*: the Eleventh Circuit concluded that because Federal Express retained the right to inspect packages, it had authority to consent to a government request to search the package without a warrant. *Young*, 350 F.3d at 1309. *See generally Warshak v. United States*, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (noting the range of terms of service used by different providers). In addition, service providers typically exercise actual authority to access the content of communications stored on their networks. Major providers regularly screen for spam, malicious

code, and child pornography. Some, such as Gmail, screen the content of email in order to target advertising at the account holder.

CCIPS has assisted many prosecutors facing constitutional challenges to the SCA, and prosecutors confronted with such challenges are encouraged to consult with CCIPS at (202) 514-1026 for further assistance.

I. Remedies

Suppression is not a remedy for nonconstitutional SCA violations. However, the SCA does create a cause of action for civil damages.

1. Suppression

The SCA does not provide a suppression remedy. *See* 18 U.S.C. § 2708 ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Accordingly, nonconstitutional violations of the SCA do not result in suppression of the evidence. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy"); *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("[S]uppression is not a remedy contemplated under the ECPA."); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act."), aff'd, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000) (unpublished); *United States v. Reyes*, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) ("Exclusion of the evidence is not an available remedy for this violation of the ECPA. . . . The remedy for violation of [18 U.S.C. § 2701-11] lies in a civil action.").

As discussed previously in Section H, defendants occasionally have claimed that section 2703's procedures for compelled disclosure violate the Fourth Amendment. However, even if a court were to hold section 2703 unconstitutional in some circumstances, suppression would likely not be a proper remedy. In *Illinois v. Krull*, 480 U.S. 340, 349 (1987), the Supreme Court held that the exclusionary rule did not apply to evidence obtained in "objectively reasonable reliance on a statute." Reliance on section 2703 likely satisfies this standard, as the only decision thus far to have held section 2703 unconstitutional was reversed on appeal. *See Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (en banc). In addition, when a defendant moves to suppress based on a claim that the SCA's procedures are unconstitutional, the court may conclude that the government's reliance on the SCA was objectively reasonable and deny the suppression motion without ruling on the constitutionality of the SCA. *See Krull*, 480 U.S. at 357 n.13; *United States v. Vanness*, 342 F.3d 1093, 1098 (10th Cir. 2003). Courts have adopted this approach in two cases in which the defendants argued that the SCA was unconstitutional. *See United States v. Warshak*, 2007 WL 4410237, at *5 (S.D. Ohio Dec. 13, 2007); *United States v. Ferguson*, 508 F. Supp. 2d 7, 9-10 (D.D.C. 2007).

2. Civil Actions and Disclosures

Although the SCA does not provide a suppression remedy for statutory violations, it does provide for civil damages (including, in some cases, punitive damages), as well as the prospect of disciplinary actions against officers and employees of the United States who have engaged in willful violations of the

statute. *See, e.g., Freedman v. American Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. 2004) (granting summary judgment on liability under the SCA against police officers who served on AOL a purported search warrant that had not been signed by a judge). The Ninth Circuit has held that the SCA does not impose secondary liability for aiding and abetting an SCA violation or conspiring to violate the SCA. *See Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1006 (9th Cir. 2006). Thus, liability under the SCA for a violation of the voluntary disclosure provisions of section 2702 is limited to service providers. *See id.* at 1006.

Liability and discipline can result not only from violations of the rules already described in this chapter, but also from the improper disclosure of some kinds of SCA-related information. Information that is obtained pursuant to § 2703 and that qualifies as a "record" under 5 U.S.C. § 552a(a) can be disclosed by an officer or governmental entity only "in the proper performance of the official functions of the officer or governmental entity making the disclosure." 18 U.S.C. § 2707(g). Other disclosures of such information by an officer or governmental entity are unlawful unless the information has been previously and lawfully disclosed to the public. *See id.*

The SCA includes separate provisions for suits against the United States and suits against any other person or entity. Section 2707 permits a "person aggrieved" by SCA violations that result from knowing or intentional conduct to bring a civil action against the "person or entity, other than the United States, which engaged in that violation." 18 U.S.C. § 2707(a). Relief can include money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs. 18 U.S.C. § 2707(b), (c). Willful or intentional violations can also result in punitive damages, *see* § 2707(c), and employees of the United States may be subject to disciplinary action for willful or intentional violations. *See* § 2707(d). A good faith reliance on a court order or warrant, grand jury subpoena, legislative authorization, or statutory authorization provides a complete defense to any civil or criminal action brought under the SCA. *See* § 2707(e). Qualified immunity may also be available. *See* Chapter 4.E.2.

Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of the SCA, Title III, or specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* This section authorizes courts to award actual damages or $10,000, whichever is greater, and reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would adversely affect a related investigation or criminal prosecution. *See* 18 U.S.C. § 2712 (b), (e).

---

[1] The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

[2] *See also Quon*, 529 F.3d at 900-03 (holding that text messaging service

provider did not provide remote computing service and thus could not disclose users' communications to the city that subscribed to its service).

[3] The Satellite Home Viewer Extension and Reauthorization Act of 2004 (SHVERA) was based on the original Cable Act and contains nearly identical provisions governing disclosure of customer records by satellite television providers. See 47 U.S.C. § 338(i).

Computer Crime & Intellectual Property Section
United States Department of Justice

Chapter 3

The Stored Communications Act

A. Introduction

- The SCA regulates how the government can obtain stored account information from network service providers such as ISPs. Whenever agents or prosecutors seek stored email, account records, or subscriber information from a network service provider, they must comply with the SCA. The SCA's classifications are summarized in the chart that appears in Section F of this chapter.

The Stored Communications Act, 18 U.S.C. §§ 2701-2712 ("SCA"), sets forth a system of statutory privacy rights for customers and subscribers of computer network service providers.[1] There are three main substantive components to this system, which serves to protect and regulate the privacy interests of network users with respect to government, network service providers, and the world at large. First, § 2703 creates a code of criminal procedure that federal and state law enforcement officers must follow to compel disclosure of stored communications from network service providers. Second, § 2702 regulates voluntary disclosure by network service providers of customer communications and records, both to government and non-government entities. Third, § 2701 prohibits unlawful access to certain stored communications; anyone who obtains, alters, or prevents authorized access to those communications is subject to criminal penalties.

The structure of the SCA reflects a series of classifications that indicate the drafters' judgments about what kinds of information implicate greater or lesser privacy interests. For example, the drafters saw greater privacy interests in the content of stored emails than in subscriber account information. Similarly, the drafters believed that computing services available "to the public" required more strict regulation than services not available to the public. (Perhaps this judgment reflects the view that providers available to the public are not likely to have close relationships with their customers, and therefore might have less incentive to protect their customers' privacy.) To protect the array of privacy interests identified by its drafters, the SCA offers varying degrees of legal protection depending on the perceived importance of the privacy interest involved. Some information can be obtained from providers with a subpoena; other information requires a special court order; and still other information requires a search warrant. In addition, some types of legal process require notice to the subscriber, while other types do not.

Agents and prosecutors must apply the various classifications devised by the SCA's drafters to the facts of each case to figure out the proper procedure for obtaining the information sought. First, they must classify the network service provider (*e.g.*, does the provider provide "electronic communication service," "remote computing service," or neither). Next, they must classify the information sought (*e.g.*, is the information content "in electronic storage," content held by a remote computing service, a non-content record pertaining

to a subscriber, or other information enumerated by the SCA). Third, they must consider whether they are seeking to compel disclosure or seeking to accept information disclosed voluntarily by the provider. If they seek compelled disclosure, they need to determine whether they need a search warrant, a 2703(d) court order, or a subpoena to compel the disclosure. If they are seeking to accept information voluntarily disclosed, they must determine whether the statute permits the disclosure. The chart contained in Section F of this chapter provides a useful way to apply these distinctions in practice.

The organization of this chapter will follow the SCA's various classifications. Section B explains the SCA's classification structure, which distinguishes between providers of "electronic communication service" and providers of "remote computing service." Section C explains the different kinds of information that providers can divulge, such as content "in electronic storage" and "records . . . pertaining to a subscriber." Section D explains the legal process that agents and prosecutors must follow to compel a provider to disclose information. Section E looks at the flip side of this problem and explains when providers may voluntarily disclose account information. A summary chart appears in Section F. Section G discusses important issues that may arise when agents obtain records from network providers: steps to preserve evidence, steps to prevent disclosure to subjects, Cable Act issues, and reimbursement to providers. Section H discusses the Fourth Amendment's application to stored electronic communications. Finally, Section I discusses the remedies that courts may impose following violations of the SCA.

B. Providers of Electronic Communication Service vs. Remote Computing Service

The SCA protects communications held by two defined classes of network service providers: providers of "electronic communication service," *see* 18 U.S.C. § 2510(15), and providers of "remote computing service," *see* 18 U.S.C. § 2711(2). Careful examination of the definitions of these two terms is necessary to understand how to apply the SCA.

1. Electronic Communication Service

An electronic communication service ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). (For a discussion of the definitions of wire and electronic communications, see Chapter 4.D.2.) For example, "telephone companies and electronic mail companies" generally act as ECS providers. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3568; *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 900-03 (9th Cir. 2008) (text messaging service provider is an ECS); *In re Application of United States*, 509 F. Supp. 2d 76, 79 (D. Mass. 2007) (cell phone service provider is an ECS); *Kaufman v. Nest Seekers, LLC*, 2006 WL 2807177, at *5 (S.D.N.Y. Sept. 26, 2006) (host of electronic bulletin board is ECS); *Freedman v. America Online, Inc.*, 325 F. Supp. 2d 638, 643 n.4 (E.D. Va. 2004) (AOL is an ECS).

Any company or government entity that provides others with the means to communicate electronically can be a "provider of electronic communication service" relating to the communications it provides, regardless of the entity's primary business or function. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114-15 (3d Cir. 2004) (insurance company that provided email service to employees is an ECS); *Bohach v. City of Reno*, 932 F. Supp. 1232, 1236 (D. Nev. 1996) (city providing pager service to its police officers was a provider of ECS); *United States v. Mullins*, 992 F.2d 1472, 1478 (9th Cir. 1993) (airline that provides travel agents with computerized travel reservation system

accessed through separate computer terminals can be a provider of ECS). In *In re Application of United States*, 349 F.3d 1132, 1138-41 (9th Cir. 2003), the Ninth Circuit held that a company operating a system that enabled drivers to communicate with designated call centers over a cellular telephone network was an ECS, though it also noted that the situation would have been entirely different "if the Company merely used wire communication as an incident to providing some other service, as is the case with a street-front shop that requires potential customers to speak into an intercom device before permitting entry, or a 'drive-thru' restaurant that allows customers to place orders via a two-way intercom located beside the drive-up lane." *Id.* at 1141 n.19.

A provider cannot provide ECS with respect to a communication if the service did not provide the ability to send or receive *that* communication. *See Sega Enterprises Ltd. v. MAPHIA*, 948 F. Supp. 923, 930-31 (N.D. Cal. 1996) (video game manufacturer that accessed private email of users of another company's bulletin board service was not a provider of electronic communication service); *State Wide Photocopy, Corp. v. Tokai Fin. Servs., Inc.*, 909 F. Supp. 137, 145 (S.D.N.Y. 1995) (financing company that used fax machines and computers but did not provide the ability to send or receive communications was not provider of electronic communication service).

Significantly, a mere user of ECS provided by another is not a provider of ECS. For example, a commercial website is not a provider of ECS, even though it may send and receive electronic communications from customers. In *Crowley v. CyberSource Corp.*, 166 F. Supp. 2d 1263, 1270 (N.D. Cal. 2001), the plaintiff argued that Amazon.com (to whom plaintiff sent his name, credit card number, and other identification information) was an electronic communications service provider because "without recipients such as Amazon.com, users would have no ability to send electronic information." The court rejected this argument, holding that Amazon was properly characterized as a user rather than a provider of ECS. *See id. See also United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003) (a home computer connected to the Internet is not an ECS); *In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d 299, 309-10 (E.D.N.Y. 2005) (airline that operated website that enabled it to communicate with customers was not an ECS); *Dyer v. Northwest Airlines Corp.*, 334 F. Supp. 2d 1196, 1199 (D.N.D. 2004) (ECS "does not encompass businesses selling traditional products or services online"); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 508-09 (S.D.N.Y. 2001) (distinguishing ISPs that provide ECS from websites that are users of ECS). However, "an online business or retailer may be considered an electronic communication service provider if the business has a website that offers customers the ability to send messages or communications to third parties." *Becker v. Toca*, 2008 WL 4443050, at *4 (E.D. La. Sept. 26, 2008).

2. Remote Computing Service

The term "remote computing service" ("RCS") is defined by 18 U.S.C. § 2711(2) as "the provision to the public of computer storage or processing services by means of an electronic communications system." An "electronic communications system" is "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

Roughly speaking, a remote computing service is provided by an off-site computer that stores or processes data for a customer. *See* S. Rep. No. 99-541 (1986), reprinted in 1986 U.S.C.C.A.N. 3555, 3564-65. For example, a service provider that allows customers to use its computing facilities in "essentially a time-sharing arrangement" provides an RCS. H.R. Rep. No. 99-647, at 23 (1986). A server that allows users to store data for future retrieval also provides an RCS. *See Steve Jackson Games, Inc. v. United States*

Secret Service, 816 F. Supp. 432, 442-43 (W.D. Tex. 1993) (provider of bulletin board services was a remote computing service), aff'd on other grounds, 36 F.3d 457 (5th Cir. 1994). Importantly, an entity that operates a website and its associated servers is not an RCS, unless of course the entity offers a storage or processing service through the website. For example, an airline may compile and store passenger information and itineraries through its website, but these functions are incidental to providing airline reservation service, not data storage and processing service; they do not convert the airline into an RCS. *See In re Jetblue Airways Corp. Privacy Litigation*, 379 F. Supp. 2d at 310; *see also United States v. Standefer*, 2007 WL 2301760, at *5 (S.D. Cal. Aug. 8, 2007) (holding that e-gold payment website was not an RCS because e-gold customers did not use the website "to simply store electronic data" or to "outsource tasks," but instead used e-gold "to transfer gold ownership to other users").

Under the definition provided by § 2711(2), a service can only be a "remote computing service" if it is available "to the public." Services are available to the public if they are available to any member of the general population who complies with the requisite procedures and pays any requisite fees. For example, Verizon is a provider to the public: anyone can obtain a Verizon account. (It may seem odd at first that a service can charge a fee but still be considered available "to the public," but this approach mirrors commercial relationships in the physical world. For example, movie theaters are open "to the public" because anyone can buy a ticket and see a show, even though tickets are not free.) In contrast, providers whose services are available only to those with a special relationship with the provider do not provide service to the public. For example, an employer that provides email accounts to its employees will not be an RCS with respect to those employees, because such email accounts are not available to the public. *See Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041, 1043 (N.D. Ill. 1998) (interpreting the "to the public" clause in § 2702(a) to exclude an internal email system that was made available to a hired contractor but was not available to "any member of the community at large").

In *Quon v. Arch Wireless Operating Co.*, the Ninth Circuit held that a text messaging service provider was an ECS and therefore not an RCS. *See Quon*, 529 F.3d at 902-03. However, this "either/or" approach to ECS and RCS is contrary to the language of the statute and its legislative history. The definitions of ECS and RCS are independent of each other, and therefore nothing prevents a service provider from providing both forms of service to a single customer. In addition, an email service provider is certainly an ECS, but the House report on the SCA also stated that an email stored after transmission would be protected by a provision of the SCA that protects contents of communications stored by an RCS. *See* H.R. Rep. No. 99-647, at 65 (1986). One subsequent court has rejected the Ninth Circuit's analysis in *Quon* and stated that a provider "may be deemed to provide both an ECS and an RCS to the same customer." *Flagg, v. City of Detroit*, 252 F.R.D. 346, 362 (E.D. Mich. 2008). The key to determining whether the provider is an ECS or RCS is to ask what role the provider has played and is playing with respect to the communication in question.

C. Classifying Types of Information Held by Service Providers

Network service providers can store different kinds of information relating to an individual customer or subscriber. Consider the range of information that an ISP may typically store regarding one of its customers. It may have the customer's subscriber information, such as name, address, and credit card number. It may have logs revealing when the customer logged on and off the service, the IP addresses assigned to the customer, and other more detailed logs pertaining to what the customer did while online. The ISP may also have the customer's opened, unopened, draft, and sent emails.

When agents and prosecutors wish to obtain such records, they must be able to classify these types of information using the language of the SCA. The SCA breaks the information down into three categories: (1) contents; (2) non-content records and other information pertaining to a subscriber or customer; and (3) basic subscriber and session information, which is a subset of non-content records and is specifically enumerated in 18 U.S.C. § 2703(c)(2). *See* 18 U.S.C. §§ 2510(8), 2703. In addition, as described below, the SCA creates substantially different protections for contents in "electronic storage" in an ECS and contents stored by a provider of RCS.

1. Basic Subscriber and Session Information Listed in 18 U.S.C. § 2703(c)(2)

Section 2703(c)(2) lists the categories of basic subscriber and session information:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

In general, the items in this list relate to the identity of a subscriber, his relationship with his service provider, and his basic session connection records. In the Internet context, "any temporarily assigned network address" includes the IP address used by a customer for a particular session. For example, for a webmail service, the IP address used by a customer accessing her email account constitutes a "temporarily assigned network address." This list does not include other, more extensive transaction-related records, such as logging information revealing the email addresses of persons with whom a customer corresponded.

2. Records or Other Information Pertaining to a Customer or Subscriber

Section 2703(c)(1) covers a second type of information: "a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications)." This is a catch-all category that includes all records that are not contents, including basic subscriber and session information described in the previous section. As one court explained, "a record means something stored or archived. The term information is synonymous with data." *In re United States*, 509 F. Supp. 2d 76, 80 (D. Mass. 2007).

Common examples of "record[s] . . . pertaining to a subscriber" include transactional records, such as account logs that record account usage; cell-site data for cellular telephone calls; and email addresses of other individuals with whom the account holder has corresponded. *See* H.R. Rep. No. 103-827, at 10, 17, 31 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3490, 3497, 3511. *See also In re Application of United States*, 509 F. Supp. 76, 80 (D. Mass. 2007) (historical cell-site information fall within scope of § 2703(c)(1)); *United States v. Allen*, 53 M.J. 402, 409 (C.A.A.F. 2000) (concluding that "a log identifying the date, time, user, and detailed internet address of sites accessed" by a user constituted "a record or other information pertaining to a subscriber or customer of such service" under the SCA); *Hill v. MCI WorldCom Commc'ns, Inc.*, 120 F. Supp. 2d 1194, 1195-96 (S.D. Iowa 2000) (concluding that the "names, addresses, and phone numbers of parties . . . called" constituted "a record or other information pertaining to a subscriber or

customer of such service," not contents, for a telephone account); *Jessup-Morgan v. America Online, Inc.*, 20 F. Supp. 2d 1105, 1108 (E.D. Mich. 1998) (holding that a customer's identification information is a "record or other information pertaining to a subscriber" rather than contents). According to the legislative history of the 1994 amendments to § 2703(c), the purpose of separating the basic subscriber and session information from other non-content records was to distinguish basic subscriber and session information from more revealing transactional information that could contain a "person's entire on-line profile." H.R. Rep. No. 103-827, at 17, 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3497, 3511-12.

3. Contents and "Electronic Storage"

The contents of a network account are the actual files (including email) stored in the account. *See* 18 U.S.C. § 2510(8) ("'contents,' when used with respect to any wire, oral, or electronic communication, includes any information concerning the substance, purport, or meaning of that communication"). For example, stored emails or voice mails are "contents," as are word processing files stored in employee network accounts. The subject lines of emails are also contents. *Cf. Brown v. Waddell*, 50 F.3d 285, 292 (4th Cir. 1995) (noting that numerical pager messages allow "an unlimited range of number-coded substantive messages" in the course of holding that the interception of pager messages requires compliance with Title III).

The SCA further divides contents into two categories: contents in "electronic storage" held by a provider of electronic communication service, and contents stored by a remote computing service. (In addition, contents that fall outside of these two categories are not protected by the SCA.) Importantly, "electronic storage" is a statutorily defined term. It does *not* simply mean storage of information by electronic means. Instead, "electronic storage" is " (A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and (B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication." 18 U.S.C. § 2510(17). Moreover, the definition of "electronic storage" is important because, as explained in Section D below, contents in "electronic storage" for less than 181 days can be obtained only with a warrant.

Unfortunately, as a result of the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), there is now a split between two interpretations of "electronic storage"--a traditional narrow interpretation and an expansive interpretation supplied by the Ninth Circuit. Both interpretations are discussed below. As a practical matter, federal law enforcement within the Ninth Circuit is bound by the Ninth Circuit's decision in *Theofel*, but law enforcement elsewhere may continue to apply the traditional interpretation of "electronic storage."

As traditionally understood, "electronic storage" refers only to temporary storage made in the course of transmission by a service provider and to backups of such intermediate communications made by the service provider to ensure system integrity. It does not include post-transmission storage of communications. For example, email that has been received by a recipient's service provider but has not yet been accessed by the recipient is in "electronic storage." *See Steve Jackson Games, Inc. v. United States Secret Service*, 36 F.3d 457, 461 (5th Cir. 1994). At that stage, the communication is stored as a temporary and intermediate measure pending the recipient's retrieval of the communication from the service provider. Once the recipient retrieves the email, however, the communication reaches its final destination. If the recipient chooses to retain a copy of the accessed communication, the copy will not be in "temporary, intermediate storage" and is not stored incident to transmission. *See Fraser v. Nationwide Mut. Ins. Co.*, 352 F.3d 107, 114 (3d Cir. 2004) (stating that email in post-transmission storage was

not in "temporary, intermediate storage"). By the same reasoning, if the sender of an email maintains a copy of the sent email, the copy will not be in "electronic storage." Messages posted to an electronic "bulletin board" or similar service are also not in "electronic storage" because the website on which they are posted is the final destination for the information. *See Snow v. DirecTV, Inc.*, 2005 WL 1226158, at *3 (M.D. Fla. May 9, 2005), adopted by 2005 WL 1266435 (M.D. Fla. May 27, 2005), aff'd on other grounds, 450 F.3d 1314 (11th Cir. 2006).

Furthermore, the "backup" component of the definition of "electronic storage" refers to copies made by an ISP to ensure system integrity. As one district court explained, the backup component "protects the communication in the event the system crashes before transmission is complete. The phrase 'for purposes of backup protection of such communication' in the statutory definition makes clear that messages that are in post-transmission storage, after transmission is complete, are not covered by part (B) of the definition of 'electronic storage.'" *Fraser v. Nationwide Mut. Ins. Co.*, 135 F. Supp. 2d 623, 636 (E.D. Pa. 2001), aff'd in part on other grounds, 352 F.3d 107, 114 (3d Cir. 2004) (affirming the SCA portion of the district court's ruling on other grounds); *see also United States v. Weaver*, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (interpreting "electronic storage" to exclude previously sent email stored by web-based email service provider); *In re Doubleclick Inc. Privacy Litigation*, 154 F. Supp. 2d 497, 511-13 (S.D.N.Y. 2001) (emphasizing that "electronic storage" should have a narrow interpretation based on statutory language and legislative intent and holding that cookies fall outside of the definition of "electronic storage" because of their "long-term residence on plaintiffs' hard drives"); H.R. Rep. No. 99-647, at 65 (1986) (noting congressional intent that opened email left on a provider's system be covered by provisions of the SCA relating to remote computing services, rather than provisions relating to communications in "electronic storage").

This narrow interpretation of "electronic storage" was rejected by the Ninth Circuit in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), in which the court held that email messages were in "electronic storage" regardless of whether they had been previously accessed, because it concluded that retrieved email fell within the backup portion of the definition of "electronic storage." *Id.* at 1075-77. Although the Ninth Circuit did not dispute that previously accessed email was not in temporary, intermediate storage within the meaning of § 2510(17)(A), it insisted that a previously accessed email message fell within the scope of the "backup" portion of the definition of "electronic storage," because such a message "functions as a 'backup' for the user." *Id.* at 1075. However, CCIPS has consistently argued that the Ninth Circuit's broad interpretation of the "backup" portion of the definition of "electronic storage" should be rejected. There is no way for a service provider to determine whether a previously opened email on its servers is a backup for a copy of the email stored by a user on his computer, as the service provider simply cannot know whether the underlying email remains stored on the user's computer. Essentially, the Ninth Circuit's reasoning in *Theofel* confuses "backup protection" with ordinary storage of a file.

Although prosecutors within the Ninth Circuit are bound by *Theofel*, law enforcement elsewhere may continue to apply the traditional narrow interpretation of "electronic storage," even when the data sought is within the Ninth Circuit. Recent lower court decisions addressing the scope of "electronic storage" have split between the traditional interpretation and the *Theofel* approach. *Compare United States v. Weaver*, 2009 WL 2163478, at *4 (C.D. Ill. July 15, 2009) (rejecting Theofel), *and Bansal v. Russ*, 513 F. Supp. 2d 264, 276 (E.D. Pa. 2007) (holding that access to opened email in account held by non-public service provider did not violate the SCA), *with Bailey v. Bailey*, 2008 WL 324156, at *6 (E.D. Mich. Feb. 6, 2008) (endorsing *Theofel*), *and Cardinal Health 414, Inc. v. Adams*, 482 F. Supp. 2d 967, 976 n.2 (M.D. Tenn. 2008) (same). Prosecutors confronted with *Theofel*-related issues should consult CCIPS at (202) 514-1026 for further assistance.

4. Illustration of the SCA's Classifications in the Email Context

An example illustrates how the SCA's categories work in practice outside the Ninth Circuit, where *Theofel* does not apply. Imagine that Joe sends an email from his account at work ("joe@goodcompany.com") to the personal account of his friend Jane ("jane@localisp.com"). The email will stream across the Internet until it reaches the servers of Jane's Internet service provider, here the fictional LocalISP. When the message first arrives at LocalISP, LocalISP is a provider of ECS with respect to that message. Before Jane accesses LocalISP and retrieves the message, Joe's email is in "electronic storage." Once Jane retrieves Joe's email, she can either delete the message from LocalISP's server or else leave the message stored there. If Jane chooses to store the email with LocalISP, LocalISP is now a provider of RCS (and not ECS) with respect to the email sent by Joe. The role of LocalISP has changed from a transmitter of Joe's email to a storage facility for a file stored remotely for Jane by a provider of RCS.

Next imagine that Jane responds to Joe's email. Jane's return email to Joe will stream across the Internet to the servers of Joe's employer, Good Company. Before Joe retrieves the email from Good Company's servers, Good Company is a provider of ECS with respect to Jane's email (just like LocalISP was with respect to Joe's original email before Jane accessed it). When Joe accesses Jane's email message and the communication reaches its destination (Joe), Good Company ceases to be a provider of ECS with respect to that email (just as LocalISP ceased to be a provider of ECS with respect to Joe's original email when Jane accessed it). Unlike LocalISP, however, Good Company does not become a provider of RCS if Joe decides to store the opened email on Good Company's server. Rather, for purposes of this specific message, Good Company is a provider of neither ECS nor RCS. Good Company does not provide RCS because it does not provide services to the public. *See* 18 U.S.C. § 2711(2) ("[T]he term 'remote computing service' means the provision *to the public* of computer storage or processing services by means of an electronic communications system." (emphasis added)); *Andersen Consulting*, 991 F. Supp. at 1043. Because Good Company provides neither ECS nor RCS with respect to the opened email in Joe's account, the SCA no longer regulates access to this email, and such access is governed solely by the Fourth Amendment. Functionally speaking, the opened email in Joe's account drops out of the SCA.

Finally, consider the status of the other copies of the emails in this scenario: Jane has downloaded a copy of Joe's email from LocalISP's server to her personal computer at home, and Joe has downloaded a copy of Jane's email from Good Company's server to his office desktop computer at work. The SCA governs neither. Although these computers contain copies of emails, these copies are not stored on the server of a third-party provider of RCS or ECS, and therefore the SCA does not apply. Access to the copies of the communications stored in Jane's personal computer at home and Joe's office computer at work is governed solely by the Fourth Amendment. *See generally* Chapters 1 and 2.

As this example indicates, a single provider can simultaneously provide ECS with regard to some communications and RCS with regard to others, or ECS with regard to some communications and neither ECS nor RCS with regard to others. A chart illustrating these issues appears in Section F of this chapter. Sample language that agents may use appears in Appendices B, E, and F.

D. Compelled Disclosure Under the SCA

Section 2703 articulates the steps that the government must take to compel providers to disclose the contents of stored wire or electronic communications (including email and voice mail) and other information such as account

records and basic subscriber and session information.

Section 2703 offers five mechanisms that a "government entity" can use to compel a provider to disclose certain kinds of information. The five mechanisms are as follows:

1) Subpoena;

2) Subpoena with prior notice to the subscriber or customer;

3) § 2703(d) court order;

4) § 2703(d) court order with prior notice to the subscriber or customer; and

5) Search warrant.

One feature of the compelled disclosure provisions of the SCA is that greater process generally includes access to information that cannot be obtained with lesser process. Thus, a 2703(d) court order can compel everything that a subpoena can compel (plus additional information), and a search warrant can compel the production of everything that a 2703(d) order can compel (and then some). As a result, the additional work required to satisfy a higher threshold will often be justified because it can authorize a broader disclosure. Note, however, the notice requirement must be considered separately under this analysis: a subpoena with notice to the subscriber can be used to compel information not available using a 2703(d) order without subscriber notice.

Two circumstances allow the government to compel disclosure of information under the SCA without a subpoena. First, when investigating telemarketing fraud, law enforcement may submit a written request to a service provider for the name, address, and place of business of a subscriber or customer engaged in telemarketing. *See* 18 U.S.C. § 2703(c)(1)(D). Second, the government may compel a service provider to disclose non-content information pertaining to a customer or subscriber when the government has obtained the customer or subscriber's consent. *See* 18 U.S.C. § 2703(c)(1)(C).

1. Subpoena

The SCA permits the government to compel disclosure of the basic subscriber and session information (discussed above in Section C.1) listed in 18 U.S.C. § 2703(c)(2) using a subpoena:

> (A) name; (B) address; (C) local and long distance telephone connection records, or records of session times and durations; (D) length of service (including start date) and types of service utilized; (E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and (F) means and source of payment for such service (including any credit card or bank account number)[.]

18 U.S.C. § 2703(c)(2).

Agents can also use a subpoena to obtain information that is outside the scope of the SCA. The hypothetical email exchange between Jane and Joe discussed in Section C of this chapter provides a useful example: Good Company provided neither "remote computing service" nor "electronic communication service" with respect to the opened email on Good Company's server. Accordingly, § 2703 does not impose any requirements on its disclosure, and investigators can issue a subpoena compelling Good Company to divulge the communication just as they would if the SCA did not exist. Similarly, information relating or belonging to a person who is neither a "customer" nor a "subscriber" is not protected by the SCA and may be

obtained using a subpoena according to the same rationale. *Cf. Organizacion JD Ltda. v. United States Dep't of Justice*, 124 F.3d 354, 359-61 (2d Cir. 1997) (discussing the scope of the word "customer" as used in the SCA).

The legal threshold for issuing a subpoena is low. *See United States v. Morton Salt Co.*, 338 U.S. 632, 642-43 (1950). Investigators may obtain disclosure pursuant to § 2703(c)(2) using any federal or state grand jury or trial subpoena or an administrative subpoena authorized by a federal or state statute. *See* 18 U.S.C. § 2703(c)(2). For example, subpoenas authorized by the Inspector General Act may be used. *See* 5 U.S.C. app. 3 § 6(a)(4). Of course, evidence obtained in response to a federal grand jury subpoena must be protected from disclosure pursuant to Fed. R. Crim. P. 6(e). At least one court has held that a pre-trial discovery subpoena issued in a civil case pursuant to Fed. R. Civ. P. 45 is inadequate. *See FTC v. Netscape Commc'ns Corp.*, 196 F.R.D. 559, 561 (N.D. Cal. 2000) (holding that civil discovery subpoena did not fall within the meaning of "trial subpoena"). Sample subpoena language appears in Appendix E.

2. Subpoena with Prior Notice to the Subscriber or Customer

Agents who obtain a subpoena and *either* give prior notice to the subscriber *or* comply with the delayed notice provisions of § 2705(a) may obtain:

1) everything that can be obtained using a subpoena without notice;

2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days." 18 U.S.C. § 2703(a); and

3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(i), § 2703(b)(2).

Outside the Ninth Circuit (which is now governed by *Theofel*), this third category will include opened and sent email. Agents outside of the Ninth Circuit can therefore obtain such email (and other stored electronic or wire communications in "electronic storage" more than 180 days) using a subpoena, provided they comply with the SCA's notice provisions. However, in light of *Theofel*, some service providers may be reluctant to produce opened or sent email less than 181 days old without a warrant. Prosecutors moving to compel compliance with a subpoena for such email should contact CCIPS at (202) 514-1026 for assistance. In the Ninth Circuit, agents can continue to subpoena communications that have been in "electronic storage" over 180 days.

The notice provisions can be satisfied by giving the customer or subscriber "prior notice" of the disclosure. *See* 18 U.S.C. § 2703(b)(1)(B). However, 18 U.S.C. § 2705(a)(1)(B) permits notice to be delayed for ninety days "upon the execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result." 18 U.S.C. § 2705(a)(1)(B). Both "supervisory official" and "adverse result" are specifically defined terms for the purpose of delaying notice. *See* 18 U.S.C. § 2705(a)(2) (defining "adverse result"); 18 U.S.C. § 2705(a)(6) (defining "supervisory official"). This provision of the SCA provides a permissible way for the government to delay notice to the customer or subscriber when notice would jeopardize a pending investigation or endanger the life or physical safety of an individual. The government may extend the delay of notice for additional 90-day periods through additional certifications that meet the "adverse result" standard of section 2705(b). *See* 18 U.S.C. § 2705(a)(4). Upon expiration of the delayed notice period, the statute requires the government to send a copy of the request or process along with a letter

explaining the delayed notice to the customer or subscriber. *See* 18 U.S.C. § 2705(a)(5).

3. Section 2703(d) Order

- Agents need a § 2703(d) court order to obtain most account logs and most transactional records.

Agents who obtain a court order under 18 U.S.C. § 2703(d) may obtain:

> 1) anything that can be obtained using a subpoena without notice; and
>
> 2) all "record[s] or other information pertaining to a subscriber to or customer of such service (not including the contents of communications [held by providers of electronic communications service and remote computing service])." 18 U.S.C. § 2703(c)(1).

A court order authorized by 18 U.S.C. § 2703(d) may be issued by any federal magistrate, district court, or equivalent state court judge. *See* 18 U.S.C. §§ 2703(d), 2711(3). To obtain such an order,

> the governmental entity [must] offer[] specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.

18 U.S.C. § 2703(d).

This standard does not permit law enforcement merely to certify that it has specific and articulable facts that would satisfy such a showing. Rather, the government must actually offer those facts to the court in the application for the order. *See United States v. Kennedy*, 81 F. Supp. 2d 1103, 1109-10 (D. Kan. 2000) (concluding that a conclusory application for a 2703(d) order "did not meet the requirements of the statute."). As the Tenth Circuit has noted, the "specific and articulable facts" standard of 2703(d) "derives from the Supreme Court's decision in [*Terry v. Ohio*, 392 U.S. 1 (1968)]." *United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008). The House Report accompanying the 1994 amendment to section 2703(d) included the following analysis:

> This section imposes an intermediate standard to protect on-line transactional records. It is a standard higher than a subpoena, but not a probable cause warrant. The intent of raising the standard for access to transactional data is to guard against "fishing expeditions" by law enforcement. Under the intermediate standard, the court must find, based on law enforcement's showing of facts, that there are specific and articulable grounds to believe that the records are relevant and material to an ongoing criminal investigation.

H.R. Rep. No. 102-827, at 31-32 (1994), reprinted in 1994 U.S.C.C.A.N. 3489, 3511-12 (quoted in full in *Kennedy*, 81 F. Supp. 2d at 1109 n.8). As a practical matter, a short factual summary of the investigation and the role that the records will serve in advancing the investigation should satisfy this criterion. A more in-depth explanation may be necessary in particularly complex cases. A sample § 2703(d) application and order appears in Appendix B.

Section 2703(d) orders issued by federal courts have effect outside the district of the issuing court. The SCA permits a judge to enter 2703(d) orders compelling providers to disclose information even if the judge does not sit in the district in which the information is stored. *See* 18 U.S.C. § 2703(d) (stating that "*any court* that is a court of competent jurisdiction" may issue a

2703(d) order) (emphasis added); 18 U.S.C. § 2711(3) (stating that "'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographical limitation"); 18 U.S.C. § 3127(2) (defining "court of competent jurisdiction").

Section 2703(d) orders may also be issued by state courts. *See* 18 U.S.C. §§ 2711(3), 3127(2)(B) (defining "court of competent jurisdiction" to include "a court of general criminal jurisdiction of a State authorized by the law of that State to enter orders authorizing the use of a pen register or a trap and trace device"). However, the statute provides that when a state governmental entity seeks a 2703(d) order, the order "shall not issue if prohibited by the law of such State." 18 U.S.C. § 2703(d). Moreover, although the statute explicitly allows federal courts to issue 2703(d) orders to providers outside of the court's district, it is silent on whether state courts have such authority.

4. 2703(d) Order with Prior Notice to the Subscriber or Customer

- Investigators can obtain everything associated with an account except for unopened email or voicemail stored with a provider for 180 days or less using a 2703(d) court order that complies with the notice provisions of § 2705.

Agents who obtain a court order under 18 U.S.C. § 2703(d), and either give prior notice to the subscriber or else comply with the delayed notice provisions of § 2705(a), may obtain:

1) everything that can be obtained using a § 2703(d) court order without notice;

2) "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days," 18 U.S.C. § 2703(a); and

3) "the contents of any wire or electronic communication" held by a provider of remote computing service "on behalf of . . . a subscriber or customer of such remote computing service." 18 U.S.C. § 2703(b)(1)(B)(ii), § 2703(b)(2).

As a practical matter, except in the Ninth Circuit, this means that the government can use a 2703(d) order that complies with the prior notice provisions of § 2703(b)(1)(B) to obtain the full contents of a subscriber's account except unopened email and voicemail that have been in the account for 180 days or less. In the Ninth Circuit, which is governed by *Theofel*, agents can continue to use 2703(d) orders to obtain communications in "electronic storage" over 180 days. Following *Theofel*, some providers have resisted producing email content less than 181 days old in response to a 2703(d) order, even when the 2703(d) order is issued by a court outside the Ninth Circuit. Prosecutors encountering this problem should contact CCIPS at (202) 514-1026 for assistance.

As an alternative to giving prior notice, law enforcement can obtain an order delaying notice for up to ninety days when notice would seriously jeopardize the investigation. *See* 18 U.S.C. § 2705(a). In such cases, prosecutors generally will obtain this order by including an appropriate request in the 2703(d) application and proposed order; sample language appears in Appendix B. Prosecutors may also apply to the court for extensions of the delay. *See* 18 U.S.C. § 2705(a)(4). The legal standards for obtaining a court order delaying notice mirror the standards for certified delayed notice by a supervisory official. *See* Section D.2., *supra*. The applicant must satisfy the court that "there is reason to believe that notification of the existence of the court order may . . . endanger[] the life or physical safety of an individual;

[lead to] flight from prosecution; [lead to] destruction of or tampering with evidence; [lead to] intimidation of potential witnesses; or . . . otherwise seriously jeopardiz[e] an investigation or unduly delay[] a trial." 18 U.S.C. §§ 2705(a)(1)(A), 2705(a)(2). The applicant must satisfy this standard anew in every application for an extension of the delayed notice.

5. Search Warrant

- Investigators can obtain everything associated with an account with a search warrant. The SCA does not require the government to notify the customer or subscriber when it obtains information from a provider using a search warrant.

Agents who obtain a search warrant under § 2703 may obtain:

1) everything that can be obtained using a § 2703(d) court order with notice; and

2) "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." 18 U.S.C. § 2703(a).

In other words, agents can obtain any content or non-content information pertaining to an account by obtaining a search warrant "issued using the procedures described in" Fed. R. Crim. P. 41. 18 U.S.C. § 2703(a).

Search warrants issued under § 2703 have several noteworthy procedural features. First, although most search warrants obtained under Rule 41 are limited to "a search of property . . . within the district" of the authorizing magistrate judge, search warrants under § 2703 may be issued by a federal "court with jurisdiction over the offense under investigation," even for records held in another district. *See United States v. Berkos*, 543 F.3d 392, 396-98 (7th Cir. 2008); *In re Search of Yahoo, Inc.*, 2007 WL 1539971, at *6 (D. Ariz. May 21, 2007); *In re Search Warrant*, 2005 WL 3844032, at *5-6 (M.D. Fla. 2006) ("Congress intended 'jurisdiction' to mean something akin to territorial jurisdiction"). State courts may also issue warrants under § 2703, but the statute does not give these warrants effect outside the limits of the courts' territorial jurisdiction. Second, obtaining a search warrant obviates the need to give notice to the subscriber. *See* 18 U.S.C. § 2703(b)(1)(A); Fed. R. Crim. P. 41(f)(1)(C).

Third, investigators ordinarily do not themselves search through the provider's computers in search of the materials described in the warrant. Instead, investigators serve the warrant on the provider as they would a subpoena, and the provider produces the material specified in the warrant. *See* 18 U.S.C. § 2703(g) (stating that the presence of an officer is not required for service or execution of a § 2703 warrant); *United States v. Bach*, 310 F.3d 1063, 1068 (8th Cir. 2002) (finding search of email by ISP without presence of law enforcement did not violate Fourth Amendment).

Fourth, a two-step process is often used to obtain the content of communications under a § 2703 warrant. First, the warrant directs the service provider to produce all email from within the specified account or accounts. Second, the warrant authorizes law enforcement to review the information produced to identify and copy information that falls within the scope of the particularized "items to be seized" under the warrant.

Otherwise, as a practical matter, § 2703 search warrants are obtained much like Rule 41 search warrants. As with a typical Rule 41 warrant, investigators must draft an affidavit and a proposed warrant that complies with Rule 41.

E. Voluntary Disclosure

- Providers of services not available "to the public" may freely disclose both contents and other records relating to stored communications. The SCA imposes restrictions on voluntary disclosures by providers of services to the public, but it also includes exceptions to those restrictions.

The voluntary disclosure provisions of the SCA appear in 18 U.S.C. § 2702. These provisions govern when a provider of RCS or ECS can disclose contents and other information voluntarily, both to the government and non-government entities. If the provider may disclose the information to the government and is willing to do so voluntarily, law enforcement does not need to obtain a legal order to compel the disclosure. If the provider either may not or will not disclose the information, agents must rely on compelled disclosure provisions and obtain the appropriate legal orders.

When considering whether a provider of RCS or ECS can disclose contents or records, the first question is whether the relevant service offered by the provider is available "to the public." *See* Section B, above. If the provider does not provide the applicable service "to the public," then the SCA does not place any restrictions on disclosure. *See* 18 U.S.C. § 2702(a). For example, in *Andersen Consulting LLP v. UOP*, 991 F. Supp. 1041 (N.D. Ill. 1998), the petroleum company UOP hired the consulting firm Andersen Consulting and gave Andersen employees accounts on UOP's computer network. After the relationship between UOP and Andersen soured, UOP disclosed to the *Wall Street Journal* emails that Andersen employees had left on the UOP network. Andersen sued, claiming that the disclosure of its contents by the provider UOP had violated the SCA. The district court rejected the suit on the ground that UOP did not provide an electronic communication service to the public:

> [G]iving Andersen access to [UOP's] e-mail system is not equivalent to providing e-mail to the public. Andersen was hired by UOP to do a project and as such, was given access to UOP's e-mail system similar to UOP employees. Andersen was not any member of the community at large, but a hired contractor.

Id. at 1043. Because UOP did not provide services to the public, the SCA did not prohibit disclosure of contents belonging to UOP's "subscribers." *See id.*

If the services offered by the provider *are* available to the public, then the SCA forbids both the disclosure of contents to any third party and the disclosure of other records *to any governmental entity* unless a statutory exception applies. Even a public provider may disclose customers' *non-content* records freely to any person other than a government entity. *See* 18 U.S.C. §§ 2702(a)(3), (c)(6). Section 2702(b) contains exceptions for disclosure of contents, and § 2702(c) contains exceptions for disclosure of other customer records.

The SCA allows the voluntary disclosure of contents when:

> 1) the disclosure is made to the intended recipient of the communication, with the consent of the sender or intended recipient, to a forwarding address, or pursuant to specified legal process, § 2702(b)(1)-(4);
>
> 2) in the case of a remote computing service, the disclosure is made with the consent of a subscriber, § 2702(b)(3);[2]
>
> 3) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(b)(5);

4) the disclosure is submitted "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A," § 2702(b)(6);

5) the disclosure is made to a law enforcement agency "if the contents . . . were inadvertently obtained by the service provider . . . [and] appear to pertain to the commission of a crime," § 2702(b)(7); or

6) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency." § 2702(b)(8).

The SCA provides for the voluntary disclosure of non-content customer records by a provider to a governmental entity when:

1) the disclosure is made "with the lawful consent of the customer or subscriber," or "as otherwise authorized in section 2703," § 2702(c)(1)-(2);

2) the disclosure "may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service," § 2702(c)(3);

3) the disclosure is made to a governmental entity, "if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency," § 2702(c)(4); or

4) the disclosure is made "to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 2258A." § 2702(c)(5).

In general, these exceptions permit disclosure by a provider to the public when the needs of public safety and of service providers themselves outweigh privacy concerns of customers, or else when disclosure is unlikely to pose a serious threat to privacy interests.

F. Quick Reference Guide

	Voluntary Disclosure Allowed?		How to Compel Disclosure	
	Public Provider	Non-Public	Public Provider	Non-Public
Basic subscriber, session, and billing information*	No, unless 2702(c) exception applies 2702(a)(3)	Yes 2702(a)(3)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)	Subpoena; 2703(d) order; or search warrant 2703(c)(2)
Other transactional and account records	No, unless 2702(c) exception applies	Yes 2702(a)(3)	2703(d) order or search warrant	2703(d) order or search warrant

	2702(a)(3)		2703(c)(1)	2703(c)(1)
Retrieved communications and the content of other stored files†	No, unless 2702(b) exception applies 2702(a)(2)	Yes 2702(a)(2)	Subpoena with notice; 2703(d) order with notice; or search warrant* 2703(b)	Subpoena; SCA does not apply* 2711(2)
Unretrieved communications, including email and voice mail (in electronic storage more than 180 days)†	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)	Subpoena with notice; 2703(d) order with notice; or search warrant 2703(a), (b)
Unretrieved communications, including email and voice mail (in electronic storage 180 days or less)†	No, unless 2702(b) exception applies 2702(a)(1)	Yes 2702(a)(1)	Search warrant 2703(a)	Search warrant 2703(a)

* *See* 18 U.S.C. § 2703(c)(2) for listing of information covered. This information includes local and long distance telephone connection records and records of session times and durations as well as IP addresses assigned to the user during the Internet connections.

† Includes the content of voice communications.

* For investigations occurring in the Ninth Circuit, *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), requires use of a search warrant unless the communications have been in storage for more than 180 days. Some providers follow *Theofel* even outside the Ninth Circuit; contact CCIPS at (202) 514-1026 if you have an appropriate case to litigate this issue.

G. Working with Network Providers: Preservation of Evidence, Preventing Disclosure to Subjects, Cable Act Issues, and Reimbursement

Law enforcement officials who procure records under the SCA quickly learn the importance of communicating with network service providers. Communication is necessary because every network provider works differently. Some providers retain very complete records for a long period of time; others retain few records, or even none. Some providers can comply easily with law enforcement requests for information; others struggle to comply with even simple requests. These differences result from varied philosophies, resources, hardware, and software among network service providers. Because of these differences, it is often advisable for agents to

communicate with a network service provider (or review the provider's law enforcement compliance guide) to learn how the provider operates *before* obtaining a legal order that compels the provider to act.

The SCA contains two provisions designed to aid law enforcement officials working with network service providers. When used properly, these provisions help ensure that providers will not delete needed records or notify others about the investigation.

1. Preservation of Evidence under 18 U.S.C. § 2703(f)

- Agents may direct providers to preserve existing records pending the issuance of compulsory legal process. Such requests have no prospective effect, however.

In general, no law regulates how long network service providers must retain account records in the United States. Some providers retain records for months, others for hours, and others not at all. As a result, some evidence may be destroyed or lost before law enforcement can obtain the appropriate legal order compelling disclosure. For example, suppose that a crime occurs on Day 1, agents learn of the crime on Day 28, begin work on a search warrant on Day 29, and obtain the warrant on Day 32, only to learn that the network service provider deleted the records in the ordinary course of business on Day 30. To minimize the risk that evidence will be lost, the SCA permits the government to direct providers to "freeze" stored records and communications pursuant to 18 U.S.C. § 2703(f). Specifically, § 2703(f)(1) states:

> A provider of wire or electronic communication services or a remote computing service, upon the request of a governmental entity, shall take all necessary steps to preserve records and other evidence in its possession pending the issuance of a court order or other process.

There is no legally prescribed format for § 2703(f) requests. While a simple phone call should be adequate, a fax or an email is safer practice because it both provides a paper record and guards against misunderstanding. Upon receipt of the government's request, the provider must retain the records for 90 days, renewable for another 90-day period upon a government request. *See* 18 U.S.C. § 2703(f)(2). A sample § 2703(f) letter appears in Appendix C.

Agents who send § 2703(f) letters to network service providers should be aware of two limitations. First, § 2703(f) letters should not be used prospectively to order providers to preserve records not yet created. If agents want providers to record information about future electronic communications, they should comply with the electronic surveillance statutes discussed in Chapter 4.

A second limitation of § 2703(f) is that some providers may be unable to comply effectively with § 2703(f) requests, or they may be unable to comply without taking actions that potentially could alert a suspect. In such a situation, the agent must weigh the benefit of preservation against the risk of alerting the subscriber. The key here is effective communication: agents should communicate with the network service provider before ordering the provider to take steps that may have unintended adverse effects. Investigators with questions about a provider's practices may also contact CCIPS at (202) 514-1026 for further assistance.

2. Orders Not to Disclose the Existence of a Warrant, Subpoena, or Court Order

Section § 2705(b) states:

> A governmental entity acting under section 2703, when it is not required to notify the subscriber or customer under section 2703(b)(1), or to the extent that it may delay such notice pursuant to subsection (a) of this section, may apply to a court for an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena, or court order will result in--
>
> (1) endangering the life or physical safety of an individual;
>
> (2) flight from prosecution;
>
> (3) destruction of or tampering with evidence;
>
> (4) intimidation of potential witnesses; or
>
> (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

18 U.S.C. § 2705(b).

This language permits agents to apply for a court order directing network service providers not to disclose the existence of legal process whenever the government itself has no legal duty to notify the customer or subscriber of the process. If the relevant process is a 2703(d) order or 2703 warrant, agents can simply include appropriate language in the application and proposed order or warrant. If agents instead seek to compel the disclosure of information using a subpoena, they must apply separately for this order.

3. The Cable Act, 47 U.S.C. § 551

- The Cable Act restricts government access to cable operator records only when the records relate to ordinary cable services. It does not restrict government access to records relating to Internet access or telephone service provided by a cable operator.

In 1984, Congress passed the Cable Communications Policy Act ("the Cable Act"), 47 U.S.C. § 521 *et seq.* Originally, 47 U.S.C. § 551 set forth a restrictive system of rules governing law enforcement access to records possessed by a cable company. Under these rules, even a search warrant was insufficient to gain access to cable company records. The government could obtain "personally identifiable information concerning a cable subscriber" only by overcoming a heavy burden of proof at an in-court adversary proceeding, as specified in 47 U.S.C. § 551(h).

After the 1984 passage of the Cable Act, cable companies began to provide Internet access and telephone service. Some cable companies asserted that the stringent disclosure restrictions of the Cable Act governed not only their provision of traditional cable programming services, but also their provision of Internet and telephone services. Congress responded by amending the Cable Act to specify that its disclosure restrictions apply only to records revealing what ordinary cable television programming a customer purchases, such as particular premium channels or "pay per view" shows. *See* USA-PATRIOT Act § 211, 115 Stat. 272, 283-84 (2001). In particular, cable operators may disclose subscriber information to the government pursuant to the SCA, Title III, and the Pen/Trap statute, except for "records revealing cable subscriber

selection of video programming." 47 U.S.C. § 551(c)(2)(D). Records revealing subscriber selection of video programming remain subject to the restrictions of 47 U.S.C. § 551(h).[3]

4. Reimbursement

- When a government entity obtains information pursuant to the SCA, the network provider may be entitled to reimbursement for its reasonable costs incurred in supplying the information.

In general, persons and entities are not entitled to reimbursement for complying with federal legal process unless there is specific federal statutory authorization. *See Blair v. United States*, 250 U.S. 273, 281 (1919) (discussing possibility of reimbursement for grand jury testimony). "It is beyond dispute that there is in fact a public obligation to provide evidence . . . and that this obligation persists no matter how financially burdensome it may be." *Hurtado v. United States*, 410 U.S. 578, 589 (1973) (stating that the Fifth Amendment does not require compensation for the performance of a public duty). However, in many (but not all) circumstances, the SCA requires government entities obtaining the contents of communications, records, or other information pursuant to the SCA to reimburse the disclosing person or entity. *See* 18 U.S.C. § 2706.

Section 2706 generally obligates government entities "obtaining the contents of communications, records, or other information under section 2702, 2703, or 2704" to pay the service provider "a fee for reimbursement for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing, or otherwise providing such information." 18 U.S.C. § 2706(a). Significantly, this section only requires reimbursement when the government actually obtains communication content, records, or other information. Thus, the government is not required to pay for costs incurred by a provider in responding to a 2703(f) preservation letter unless the government later obtains the preserved records.

The amount of the fee required under § 2706(a) "shall be as mutually agreed by the governmental entity and the person or entity providing the information, or, in the absence of agreement, shall be as determined by the court." 18 U.S.C. § 2706(b). In practice, if the service provider seeks what appears to be unreasonably high reimbursement costs, the government should demand a detailed accounting of costs incurred by activity. A cost accounting will help ensure that the provider is not seeking reimbursement for indirect costs or activities that were not reasonably necessary to the production.

In addition, the SCA contains a reimbursement exception that precludes reimbursement in specific circumstances. The reimbursement requirement "does not apply with respect to records or other information maintained by a communications common carrier that relate to telephone toll records and telephone listings obtained under section 2703," unless a court determines that the information sought by the government is "unusually voluminous" or "caused an undue burden on the provider." 18 U.S.C. § 2706(c).

The reimbursement exception of § 2706(c) applies only to records and other information "maintained by" a communications common carrier. In *Ameritech Corp. v. McCann*, 403 F.3d 908, 912 (7th Cir. 2005), the Seventh Circuit held that reports of who placed calls to a specified customer were not "maintained by" Ameritech. Ameritech's computer system recorded calls made by a customer, but it did not automatically keep or generate a list of the calls made to a customer. Compiling such a list required substantial computation time. According to the court, Ameritech "maintains" bills and equivalent statements, and the government can therefore get such "raw information" for free. However,

when the government requires Ameritech to create a report, the government must provide compensation. Prosecutors outside the Seventh Circuit are not bound by *Ameritech*, and there is a reasonably strong argument that its interpretation of § 2706(c) is flawed. Under this alternative interpretation, any information stored by a carrier is "maintained by" the carrier, and questions regarding the difficulty of producing information can be evaluated under the "undue burden" standard of § 2706(c).

H. Constitutional Considerations

Defendants sometimes raise constitutional challenges to compelled disclosure of information from communication service providers. They typically argue that use of a 2703(d) order or a subpoena (rather than a warrant) to compel disclosure of information violated the Fourth Amendment. These claims fail for two reasons. First, the defendant may have no reasonable expectation of privacy in the information obtained from the service provider. Second, the Fourth Amendment generally permits the government to compel a provider to disclose information in an account when the provider has access to and control over the targeted information, regardless of whether the account user has a reasonable expectation of privacy in the targeted information.

It is now well established that a customer or subscriber has no reasonable expectation of privacy in her subscriber information or transactional records. In *United States v. Miller*, 425 U.S. 435 (1976), the Supreme Court held that a defendant had no reasonable expectation of privacy in his bank records because the records were not his "private papers" but were "the business records of the banks" in which the defendant could "assert neither ownership nor possession." *Id.* at 440. The Court explained that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Id.* at 443 (citing *Hoffa v. United States*, 385 U.S. 293, 302 (1966)). The Court relied upon the principles of *Miller* in *Smith v. Maryland*, 442 U.S. 735 (1979), in which it held that a defendant had no reasonable expectation of privacy in dialed telephone numbers obtained from the phone company. *Id.* at 745-46.

Courts have now extended this *Miller/Smith* analysis to network accounts, holding that individuals retain no Fourth Amendment privacy interest in subscriber information and transactional records. *See United States v. Perrine*, 518 F.3d 1196, 1204 (10th Cir. 2008) ("Every federal court to address this issue has held that subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation."); *United States v. Forrester*, 512 F.3d 500, 510 (9th Cir. 2008) (email and Internet users have no reasonable expectation of privacy in source or destination addresses of email or the IP addresses of websites visited); *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) (finding no Fourth Amendment protection for network account holders' subscriber information obtained from communication service provider).

In contrast, whether a user has a reasonable expectation of privacy in the contents of communications stored in her account will depend on the facts and circumstances associated with the account. In *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 906 (9th Cir. 2008), the Ninth Circuit rejected "a monolithic view of text message users' reasonable expectation of privacy," explaining that "this is necessarily a context-sensitive inquiry." *Compare Quon*, 529 F.3d at 906-08 (finding reasonable expectation of privacy in pager messages based on an "informal policy that the text messages would not be audited"), and *Wilson v. Moreau*, 440 F. Supp. 2d 81, 108 (D.R.I. 2006) (finding reasonable expectation of privacy in content of Yahoo! email account), aff'd, 492 F.3d 50 (1st Cir. 2007), *with Biby v. Board of Regents*, 419 F.3d 845, 850-51 (8th Cir. 2005) (university policy stating that computer files and emails may be searched in response to litigation discovery requests eliminated computer user's reasonable expectation of privacy) and *Guest v.*

Leis, 255 F.3d 325, 333 (6th Cir. 2001) (finding that disclaimer on private bulletin board service defeated expectation of privacy in postings). *See also United States v. Young*, 350 F.3d 1302, 1307-08 (11th Cir. 2003) (Federal Express customer had no reasonable expectation of privacy in the contents of a package based on terms of service authorizing Federal Express to inspect packages).

Critically, however, even if a user has a reasonable expectation of privacy in an item, a subpoena may be used to compel the production of the item, provided the subpoena is reasonable. *See United States v. Palmer*, 536 F.2d 1278, 1281-82 (9th Cir. 1976). The Fourth Amendment imposes a probable cause requirement *only* on the issuance of warrants. *See* U.S. Const. amend.-IV ("and no Warrants shall issue, but upon probable cause"). A century of Supreme Court case law demonstrates that reasonable subpoenas comply with the Fourth Amendment. *See Wilson v. United States*, 221 U.S. 361, 376 (1911) ("there is no unreasonable search and seizure when a [subpoena], suitably specific and properly limited in its scope, calls for the production of documents which, as against their lawful owner to whom the writ is directed, the party procuring its issuance is entitled to have produced"); *Oklahoma Press Publ'g Co. v. Walling*, 327 U.S. 186, 208 (1946); *United States v. Dionisio*, 410 U.S. 1, 9-12 (1973); *Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984). The rule for when a subpoena is reasonable and thus complies with the Fourth Amendment is also well-established: "the Fourth Amendment requires that the subpoena be sufficiently limited in scope, relevant in purpose, and specific in directive so that compliance will not be unreasonably burdensome." *Donovan*, 464 U.S. at 415 (quoting *See v. City of Seattle*, 387 U.S. 541, 549 (1967)). Finally, the Fourth Amendment does not require that notice be given to the target of an investigation in third-party subpoena cases. *See SEC v. Jerry T. O'Brien, Inc.*, 467 U.S. 735, 743, 749-51 (1984).

In general, the cases indicate that the government may compel an entity to disclose any item that is within its control and that it may access. *See United States v. Barr*, 605 F. Supp. 114, 119 (S.D.N.Y. 1985) (subpoena served on private third-party mail service for the defendant's mail in the third party's possession); *Schwimmer v. United States*, 232 F.2d 855, 861-63 (8th Cir. 1956) (subpoena served on third-party storage facility for the defendant's private papers in the third party's possession); *Newfield v. Ryan*, 91 F.2d 700, 702-05 (5th Cir. 1937) (subpoena served on telegraph company for copies of defendants' telegrams in the telegraph company's possession). This rule is supported both by the rule that a party with "joint access or control for most purposes" may consent to a search, *see United States v. Matlock*, 415 U.S. 164, 171 n.7 (1974), and also by the rule that "the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities." *Miller*, 425 U.S. at 443.

As a practical matter, there is good reason to believe that network service providers will typically have sufficient access to and control over stored communications on their networks to produce the communications in response to compulsory process. Terms of service used by network service providers often establish that the provider has authority to access and disclose subscriber email. For example, at the time of this writing, Yahoo!'s terms of service confirm its right in its "sole discretion to pre-screen, refuse, or remove any Content that is available via the Yahoo! Servicas," as well as to access and disclose email to comply with legal process. Terms of service similar to Yahoo!'s were sufficient to establish Federal Express's common authority over the contents of a package in *Young*: the Eleventh Circuit concluded that because Federal Express retained the right to inspect packages, it had authority to consent to a government request to search the package without a warrant. *Young*, 350 F.3d at 1309. *See generally Warshak v. United States*, 532 F.3d 521, 527 (6th Cir. 2008) (en banc) (noting the range of terms of service used by different providers). In addition, service providers typically exercise actual authority to access the content of communications stored on their networks. Major providers regularly screen for spam, malicious

code, and child pornography. Some, such as Gmail, screen the content of email in order to target advertising at the account holder.

CCIPS has assisted many prosecutors facing constitutional challenges to the SCA, and prosecutors confronted with such challenges are encouraged to consult with CCIPS at (202) 514-1026 for further assistance.

I. Remedies

Suppression is not a remedy for nonconstitutional SCA violations. However, the SCA does create a cause of action for civil damages.

1. Suppression

The SCA does not provide a suppression remedy. *See* 18 U.S.C. § 2708 ("The [damages] remedies and sanctions described in this chapter are the only judicial remedies and sanctions for nonconstitutional violations of this chapter."). Accordingly, nonconstitutional violations of the SCA do not result in suppression of the evidence. *See United States v. Perrine*, 518 F.3d 1196, 1202 (10th Cir. 2008) ("[V]iolations of the ECPA do not warrant exclusion of evidence."); *United States v. Steiger*, 318 F.3d 1039, 1049 (11th Cir. 2003); *United States v. Smith*, 155 F.3d 1051, 1056 (9th Cir. 1998) ("[T]he Stored Communications Act expressly rules out exclusion as a remedy"); *United States v. Ferguson*, 508 F. Supp. 2d 7, 10 (D.D.C. 2007); *United States v. Sherr*, 400 F. Supp. 2d 843, 848 (D. Md. 2005); *United States v. Kennedy*, 81 F. Supp. 2d 1103, 1110 (D. Kan. 2000) ("[S]uppression is not a remedy contemplated under the ECPA."); *United States v. Hambrick*, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("Congress did not provide for suppression where a party obtains stored data or transactional records in violation of the Act."), aff'd, 225 F.3d 656, 2000 WL 1062039 (4th Cir. 2000) (unpublished); *United States v. Reyes*, 922 F. Supp. 818, 837-38 (S.D.N.Y. 1996) ("Exclusion of the evidence is not an available remedy for this violation of the ECPA. . . . The remedy for violation of [18 U.S.C. § 2701-11] lies in a civil action.").

As discussed previously in Section H, defendants occasionally have claimed that section 2703's procedures for compelled disclosure violate the Fourth Amendment. However, even if a court were to hold section 2703 unconstitutional in some circumstances, suppression would likely not be a proper remedy. In *Illinois v. Krull*, 480 U.S. 340, 349 (1987), the Supreme Court held that the exclusionary rule did not apply to evidence obtained in "objectively reasonable reliance on a statute." Reliance on section 2703 likely satisfies this standard, as the only decision thus far to have held section 2703 unconstitutional was reversed on appeal. *See Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (en banc). In addition, when a defendant moves to suppress based on a claim that the SCA's procedures are unconstitutional, the court may conclude that the government's reliance on the SCA was objectively reasonable and deny the suppression motion without ruling on the constitutionality of the SCA. *See Krull*, 480 U.S. at 357 n.13; *United States v. Vanness*, 342 F.3d 1093, 1098 (10th Cir. 2003). Courts have adopted this approach in two cases in which the defendants argued that the SCA was unconstitutional. *See United States v. Warshak*, 2007 WL 4410237, at *5 (S.D. Ohio Dec. 13, 2007); *United States v. Ferguson*, 508 F. Supp. 2d 7, 9-10 (D.D.C. 2007).

2. Civil Actions and Disclosures

Although the SCA does not provide a suppression remedy for statutory violations, it does provide for civil damages (including, in some cases, punitive damages), as well as the prospect of disciplinary actions against officers and employees of the United States who have engaged in willful violations of the

statute. *See, e.g., Freedman v. American Online, Inc.*, 303 F. Supp. 2d 121 (D. Conn. 2004) (granting summary judgment on liability under the SCA against police officers who served on AOL a purported search warrant that had not been signed by a judge). The Ninth Circuit has held that the SCA does not impose secondary liability for aiding and abetting an SCA violation or conspiring to violate the SCA. *See Freeman v. DirecTV, Inc.*, 457 F.3d 1001, 1006 (9th Cir. 2006). Thus, liability under the SCA for a violation of the voluntary disclosure provisions of section 2702 is limited to service providers. *See id.* at 1006.

Liability and discipline can result not only from violations of the rules already described in this chapter, but also from the improper disclosure of some kinds of SCA-related information. Information that is obtained pursuant to § 2703 and that qualifies as a "record" under 5 U.S.C. § 552a(a) can be disclosed by an officer or governmental entity only "in the proper performance of the official functions of the officer or governmental entity making the disclosure." 18 U.S.C. § 2707(g). Other disclosures of such information by an officer or governmental entity are unlawful unless the information has been previously and lawfully disclosed to the public. *See id.*

The SCA includes separate provisions for suits against the United States and suits against any other person or entity. Section 2707 permits a "person aggrieved" by SCA violations that result from knowing or intentional conduct to bring a civil action against the "person or entity, other than the United States, which engaged in that violation." 18 U.S.C. § 2707(a). Relief can include money damages no less than $1,000 per person, equitable or declaratory relief, and a reasonable attorney's fee plus other reasonable litigation costs. 18 U.S.C. § 2707(b), (c). Willful or intentional violations can also result in punitive damages, *see* § 2707(c), and employees of the United States may be subject to disciplinary action for willful or intentional violations. *See* § 2707(d). A good faith reliance on a court order or warrant, grand jury subpoena, legislative authorization, or statutory authorization provides a complete defense to any civil or criminal action brought under the SCA. *See* § 2707(e). Qualified immunity may also be available. *See* Chapter 4.E.2.

Suits against the United States may be brought under 18 U.S.C. § 2712 for willful violations of the SCA, Title III, or specified sections of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq.* This section authorizes courts to award actual damages or $10,000, whichever is greater, and reasonable litigation costs. Section 2712 also defines procedures for suits against the United States and a process for staying proceedings when civil litigation would adversely affect a related investigation or criminal prosecution. *See* 18 U.S.C. § 2712 (b), (e).

---

[1] The SCA is sometimes referred to as the Electronic Communications Privacy Act. The SCA was included as Title II of the Electronic Communications Privacy Act of 1986 ("ECPA"), but ECPA itself also included amendments to the Wiretap Act and created the Pen Register and Trap and Trace Devices statute addressed in Chapter 4. *See* Pub. L. No. 99-508, 100 Stat. 1848 (1986). Although 18 U.S.C. § 2701-2712 is referred to as the "Stored Communications Act" here and elsewhere, the phrase "Stored Communications Act" appears nowhere in the language of the statute.

[2] *See also Quon*, 529 F.3d at 900-03 (holding that text messaging service

provider did not provide remote computing service and thus could not disclose users' communications to the city that subscribed to its service).

[3] The Satellite Home Viewer Extension and Reauthorization Act of 2004 (SHVERA) was based on the original Cable Act and contains nearly identical provisions governing disclosure of customer records by satellite television providers. *See* 47 U.S.C. § 338(i).

U.S. Department of Justice
Office of Justice Programs

Embargoed for release to the public until Tuesday, January 13, 2009, at 9:00 a.m. EST.

Bureau of Justice Statistics
Special Report

January 2009, NCJ 224527

National Crime Victimization Survey

Stalking Victimization in the United States

By Katrina Baum, Ph.D., Shannan Catalano, Ph.D., and Michael Rand
Bureau of Justice Statistics
Kristina Rose
National Institute of Justice

During a 12-month period, an estimated 3.4 million persons age 18 or older were victims of stalking. Stalking is defined as a course of conduct directed at a specific person that would cause a reasonable person to feel fear. The Supplemental Victimization Survey (SVS), which is the basis of this report, was conducted in 2006. The SVS identified seven types of harassing or unwanted behaviors consistent with a course of conduct experienced by stalking victims. The survey classified individuals as stalking victims if they responded that they experienced at least one of these behaviors on at least two separate occasions. In addition, the individuals must have feared for their safety or that of a family member as a result of the course of conduct, or have experienced additional threatening behaviors that would cause a reasonable person to feel fear.

The SVS measured the following stalking behaviors:

- making unwanted phone calls
- sending unsolicited or unwanted letters or e-mails
- following or spying on the victim
- showing up at places without a legitimate reason
- waiting at places for the victim
- leaving unwanted items, presents, or flowers
- posting information or spreading rumors about the victim on the internet, in a public place, or by word of mouth.

While individually these acts may not be criminal, collectively and repetitively these behaviors may cause a victim to fear for his or her safety or the safety of a family member. These behaviors constitute stalking for the purposes of this study. The federal government, all 50 states, the District of Columbia, and U.S. Territories have enacted laws making stalking a criminal act, although the elements defining the act of stalking differ across states (see box, Stalking laws).

The SVS also identified victims who experienced the behaviors associated with stalking but neither reported feeling fear as a result of such conduct nor experienced actions that would cause a reasonable person to feel fear. This report characterizes such individuals as harassment victims. These instances of harassment might eventually have risen to the definitional requirement for stalking. However, at the time of the interview, the offender's actions and victim's responses did not rise to the threshold of stalking victimization as measured by the SVS.

During a 12-month period an estimated 14 in every 1,000 persons age 18 or older were victims of stalking

- About half (46%) of stalking victims experienced at least one unwanted contact per week, and 11% of victims said they had been stalked for 5 years or more.
- The risk of stalking victimization was highest for individuals who were divorced or separated—34 per 1,000 individuals.
- Women were at greater risk than men for stalking victimization; however, women and men were equally likely to experience harassment.
- Male (37%) and female (41%) stalking victimizations were equally likely to be reported to the police.
- Approximately 1 in 4 stalking victims reported some form of cyberstalking such as e-mail (83%) or instant messaging (35%).
- 46% of stalking victims felt fear of not knowing what would happen next.
- Nearly 3 in 4 stalking victims knew their offender in some capacity.

Few national studies have measured the extent and nature of stalking in the United States. The Department of Justice Office on Violence Against Women funded the 2006 SVS as a supplement to the National Crime Victimization Survey (NCVS) to enhance empirical knowledge about stalking (see *Methodology*). The SVS, which represents the largest study of stalking conducted to date, incorporated elements contained in federal and state laws to construct a working definition of stalking.

This report presents information on stalking victimization. Harassment is discussed where appropriate to provide fuller context. Appendix tables focus solely on stalking victims and exclude the people who experienced what this report terms as harassment. Persons interested in viewing the SVS data in its entirety may obtain the data file from the University of Michigan's Archive of Criminal Justice Data <www.icpsr.umich.edu/NACJD>.

During a 12-month period an estimated 14 in every 1,000 persons age 18 or older were victims of stalking

An estimated 5.9 million U.S. residents age 18 or older experienced behaviors consistent with either stalking or harassment in the 12 months preceding the SVS interview (table 1).[1] Of the 5.9 million victims, more than half experienced behavior that met the definition of stalking. Approximately 14 per 1,000 persons age 18 or older experienced the repetitive behaviors associated with stalking in addition to feeling fear or experiencing behaviors that would cause a reasonable person to feel fear. Harassment victims, who experienced a course of conduct consistent with stalking but who did not report feeling fear, experienced these behaviors at a rate of 10 victimizations per 1,000 persons age 18 or older.

About half (46%) of all stalking victims experienced at least one unwanted contact per week (appendix table 6). Many victims of stalking reported being stalked over a period of months or years, and 11% of victims said they had been stalked for 5 years or more (figure 1). The fears and emotional distress that stalking engenders are many and varied. About 1 in 5 victims feared bodily harm to themselves, and 1 in 6 feared for the safety of a child or other family member.[2] One in 20 stalking victims feared being killed by the stalker. About 4 in 10 stalkers threatened the victim or the victim's family, friends, co-workers, or family pet.[3]

[1]To place this estimate in perspective, there were about 5.2 million violent crimes—rape/sexual assault, robbery, aggravated assault, and simple assault—committed in 2005.

[2]Table 10 lists the range of fearful reactions about which victims were surveyed.

[3]Table 13 lists various threats stalkers made to victims.

The most common type of stalking behavior victims experienced was unwanted phone calls and messages

With the exception of receiving unwanted letters, e-mails, or other correspondence, stalking victims were more likely than harassment victims to experience all forms of unwanted behaviors (table 2). In particular, victims of stalking experienced higher levels of three unwanted behaviors most commonly associated with stalking. These included an offender following or spying on the victim, showing up at places without a legitimate reason, or waiting outside (or inside) places for the victim. Stalking victims were about 3 times more likely to report experiencing these three behaviors than individuals who were harassed. For example, 34% of stalking victims reported that the offender followed or spied on them compared with 11% of harassment

Table 1. Prevalence of stalking and harassment over the 12 months prior to interview

	Number	Rate
All victims	5,857,030	23.8
Stalking victims	3,424,100	13.9
Harassment victims	2,432,930	9.9

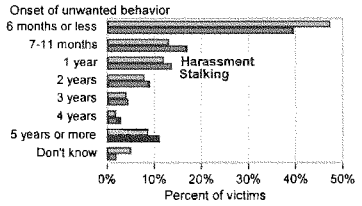
Note: The total population age 18 or older was 246,500,200 in 2006. Victimization rates are per 1,000 persons age 18 or older.

Table 2. Nature of stalking and harassment behaviors experienced by victims

	Percent of victims		
	All	Stalking	Harassment
Unwanted phone calls and messages	62.5%	66.2%	57.2%
Unwanted letters and e-mail	30.1	30.6	29.4
Spreading rumors	29.1	35.7	19.9
Following or spying	24.5	34.3	10.6
Showing up at places	22.4	31.1	10.2
Waiting for victim	20.4	29.0	8.3
Leaving unwanted presents	9.1	12.2	4.8
Number of victims	5,857,030	3,424,100	2,432,930

Note: Details sum to more than 100% because multiple responses were permitted.

About 10% of victims were stalked for 5 years or more



Note: Estimates exclude 1.2% of stalking and 10.2% of harassment victims due to missing data. All victims experience at least one unwanted behavior in the year before the interview.

Figure 1

victims who reported experiencing this behavior. Thirty-one percent of stalking victims reported that the offenders showed up in places where they had no legitimate purpose being; approximately 10% of harassment victims reported this type of unwanted behavior. Also, 29% of stalking victims stated that the offender waited in places for them, while 8% of harassment victims reported this type of behavior.

Risk of victimization varies more for stalking than for harassment

Females were at higher risk of stalking victimization than males (table 3). During the study period, females experienced 20 stalking victimizations per 1,000 females age 18 or older. The rate of stalking victimization for males was approximately 7 per 1,000 males age 18 or older. Males and females were equally likely to experience harassment.

Age

As with victimization risk more generally, risk of being stalked diminished with age. Persons age 18 to 19 and 20 to 24 experienced the highest rates of stalking victimization. About 30 per 1,000 persons age 18 to 19 and 28 per 1,000 persons age 20 to 24 were stalked during 2006.

Race and Hispanic origin of victim

Asians and Pacific Islanders (7 per 1,000 persons age 18 and older) were less likely to experience stalking than whites (14 per 1,000), blacks (12 per 1,000), and persons of two or more races (32 per 1,000). Despite apparent racial differences, no other consistent patterns of risk for stalking victimization emerged. Non-Hispanics were more likely than Hispanics to experience stalking. During the study period, non-Hispanics experienced about 14 stalking victimizations per 1,000 individuals age 18 and older. The rate for Hispanics during this period was 11 stalking victimizations per 1,000 persons age 18 or older.

Stalking laws

While the federal government, all 50 states, the District of Columbia, and U.S. Territories have enacted criminal laws to address stalking, the legal definition for stalking varies across jurisdictions. State laws vary regarding the element of victim fear and emotional distress, as well as the requisite intent of the stalker. Some state laws specify that the victim must have been frightened by the stalking, while others require only that the stalking behavior would have caused a reasonable person to experience fear. In addition states vary regarding what level of fear is required. Some state laws require prosecutors to establish fear of death or serious bodily harm, while others require only that prosecutors establish that the victim suffered emotional distress. Interstate stalking is defined by federal law 18 U.S.C. § 2261A.

Marital status

The rate of stalking victimization for individuals who were divorced or separated was 34 per 1,000 individuals age 18 or older—a higher rate of victimization than for persons of other marital status. Individuals who had never been married (17 per 1,000 individuals) were at a lower risk of stalking victimization than divorced or separated persons, but were at a higher risk of stalking victimization than persons who were married (9 per 1,000) or widowed (8 per 1,000).

Income

As with crime more generally, a pattern of decreasing risk for stalking victimization existed for persons residing in households with higher incomes. Individuals in households with an annual income under $7,500 and $7,500 to $14,999 were equally likely to be stalked but more likely to be victimized than were persons in households with an annual income at or above $25,000.

Table 3. Characteristics of stalking and harassment victims

		Rate per 1,000 victims[a]		
	Population	All	Stalking	Harassment
Gender				
Male	120,068,420	16.9	7.4	9.5
Female	126,431,780	30.3	20.0	10.2
Age				
18-19	8,047,540	47.2	29.7	17.5
20-24	20,346,940	45.7	28.4	17.3
25-34	39,835,680	30.1	20.2	9.9
35-49	65,886,490	29.9	17.3	12.6
50-64	51,400,990	20.4	10.4	10.0
65 or older	35,515,670	9.3	3.6	5.7
Race				
White	200,874,080	24.1	14.2	9.8
Black	29,853,700	22.7	12.2	10.5
American Indian/ Alaska Native	1,695,400	33.0	19.6*	13.4*
Asian/Pacific Islander	11,317,780	13.4	7.0	6.4
More than one race[b]	2,759,240	49.3	31.6	17.7
Hispanic origin				
Hispanic	29,522,670	16.5	10.6	5.9
Non-Hispanic	215,025,170	24.7	14.4	10.3
Marital status				
Never married	79,715,080	26.9	16.6	10.3
Married	123,633,560	16.8	8.7	8.1
Divorced or separated	26,334,200	51.8	34.0	17.8
Widowed	14,318,190	16.0	7.5	8.5
Household income				
Less than $7,500	8,418,570	47.0	31.7	15.3
$7,500 - $14,999	14,562,850	40.1	27.4	12.6
$15,000 - $24,999	22,428,240	32.3	21.1	11.1
$25,000 - $34,999	22,862,680	27.4	15.8	11.5
$35,000 - $49,999	30,345,140	25.2	15.8	9.4
$50,000 - $74,999	37,956,910	23.1	12.6	10.6
$75,000 or more	56,633,800	18.8	9.6	9.2

Note: Table excludes missing data.
*Based on 10 or fewer sample cases.
[a]Victimization rates are per 1,000 persons age 18 or older.
[b]Includes all persons of any race, including persons who identify two or more races.

Victims were more likely to be stalked by an offender of the same age and race

Offender age

Individuals were more likely to be stalked by offenders of similar age (appendix table 1). Nearly half of victims age 21 to 29 were stalked by offenders perceived to also be in their twenties, and 38% of victims age 30 to 39 perceived the offender to also be in their thirties.

Race

Similar to other types of victimization, stalking is primarily intraracial in nature (appendix table 2). Most (83%) of white stalking victims perceived the offender to be white compared to 66% of black stalking victims who perceived the offender to be black. This pattern of intraracial victimization changes for persons of other races. Despite apparent differences, persons of other races were equally likely to be stalked by an offender who was black, white, or of another race.[4]

Offender gender

Males were as likely to report being stalked by a male as a female offender (table 4). Forty-three percent of male stalking victims stated that the offender was female, while 41% of male victims stated that the offender was another male. Female victims of stalking were significantly more likely to be stalked by a male (67%) rather than a female (24%) offender.

Stalking is unlike most crimes because a course of conduct designed to create fear in another person does not necessarily require that the victim come into contact with the offender. For example, a victim may receive repeated threatening correspondence without knowing the source of the communication. Sixteen percent of male stalking victims and approximately 10% of female stalking victims were not able to identify the gender of the offender.

[4]Other races include American Indians, Alaska Natives, Asians, Native Hawaiians, other Pacific Islanders, and persons identifying two or more races.

Number of offenders

About 6 in 10 stalking victims stated that the perpetrator was a single offender (appendix table 3). A much lower percentage of victims reported being stalked by two (18%) or three (13%) offenders.

Relationship

About a tenth of all victims were stalked by a stranger, and nearly 3 in 4 of all victims knew their offender in some capacity (table 5). Stalking victims most often identified the stalker as a former intimate (21.5%) or a friend, roommate, or neighbor (16.4%).

Table 5. Victim-offender relationship in stalking and harassment

	Percent of victims		
	All	Stalking	Harassment
Total**	100%	100%	100%
Known, intimate	27.6%	30.3%	22.5%
Current intimate			
Spouse	4.3	5.6	1.8*
Boy/girlfriend	3.8	3.2	5.1
Former intimate			
Ex-spouse	7.1%	8.4%	4.6%
Ex-boy/girlfriend	12.4	13.1	11.0
Known, other	44.7%	45.1%	44.4%
Friend/roommate/ neighbor	16.7	16.4	17.4
Known from work or school	10.1	9.9	10.6
Acquaintance	9.4	9.8	8.8
Relative	8.5	9.0	7.6
Stranger	10.6%	9.7%	12.5%
Unknown	16.9%	15.0%	20.6%
Number of victims	4,619,430	3,064,950	1,554,480

Note: Table excludes 0.5% of all victims, 0.3% of stalking victims, and 0.7% of harassment victims due to missing data. Detail may not sum to 100% due to rounding.
*Estimate based on 10 or fewer cases.
**Includes victims who could identify a single offender who was most responsible.

Table 4. Perceived gender of the stalking or harassment offender, by victim gender

	Gender of victim					
	All		Stalking		Harassment	
Gender of offender	Male	Female	Male	Female	Male	Female
Total	100%	100%	100%	100%	100%	100%
Male	31.7	58.3	41.3	66.9	24.2	41.3
Female	37.9	22.4	42.5	23.5	34.3	20.3
Don't know	30.4	19.3	16.1	9.6	41.5	38.4
Number of victims	2,028,800	3,821,140	888,680	2,531,770	1,140,120	1,289,370

Note: Table excludes missing data about offenders from 0.2% of all male victims, 0.1% of all female victims, 0.4% of female stalking victims, and 0.3% of female harassment victims. Detail may not sum to 100% due to rounding.

Employment status of the offender

Forty-two percent of stalking victims stated that the offender was employed during the time stalking occurred (appendix table 4). Victims were equally likely to report that the offender was unemployed or that the victim was unable to ascertain the employment status of the offender.

Problems with the law

Thirty-six percent of stalking victims stated that the offender had some previous interaction with law enforcement (appendix table 5). A similar percentage of victims (38%) were unable to identify whether the offender had problems with the law prior to the stalking victimization.

One in 10 victims reported that the stalking started 5 years or more before the survey

Over half of all victims reported that the stalking or harassment began "less than a year ago" (figure 1). Harassment victims had characteristically experienced the harassing behavior for a shorter period leading up to the interview (6 months or less). Stalking victims were most likely to be stalked once or twice a week or with no set pattern (appendix table 6). Nearly a quarter of all victims reported that they were stalked almost every day (16.9%) or at least once a day (6%).

Victim perception of why stalking began

The most common reasons victims perceived for the stalking were retaliation, anger, spite (37%), or desire to control the victim (33%) (table 6). About 1 in 6 victims believed the stalking started to keep him or her in the relationship with the offender, and 1 in 10 reported the stalking began while living with the offender (not referenced in a table). About a tenth of victims did not know why the stalking began.

Cyberstalking and electronic monitoring

More than 1 in 4 stalking victims reported some form of cyberstalking was used, such as e-mail (83%) or instant messaging (35%) (table 7). Electronic monitoring was used to stalk 1 in 13 victims. Video or digital cameras were equally likely as listening devices or bugs to be used to electronically monitor victims (46% and 42%). Global positioning system (GPS) technology comprised about a tenth of the electronic monitoring of stalking victims.

Table 6. Victim perception of reasons stalking or harassment began

	Percent of all victims		
	All	Stalking	Harassment
Retaliation/anger/spite	30.0%	36.6%	20.0%
Control	25.2	32.9	13.4
Mentally ill/emotionally unstable	16.7	23.4	6.6
Liked me/found me attractive/ had crush	13.7	16.8	9.0
Keep in relationship	12.9	16.2	7.9
Substance abuser	10.3	14.4	4.1
Stalker liked attention	7.7	9.1	5.7
Proximity/convenience/ I was alone	4.8	6.6	2.2
Catch me doing something	3.3	4.3	1.9
Different cultural beliefs/background	3.2	4.0	1.8
Thought I liked attention	2.5	2.4	2.6
Other reasons	23.8	19.3	30.7
Don't know why	16.6	10.6	25.7
Number of victims	5,644,500	3,416,460	2,228,050

Note: Table excludes 3.6% of all victims, 0.2% of stalking victims, and 8.4% of harassment victims due to missing data. Details sum to more than 100% because multiple responses were permitted.

Table 7. Involvement of cyberstalking or electronic monitoring in stalking and harassment

	Percent of victims		
	All	Stalking	Harassment
Total	100%	100%	100%
No cyberstalking or electronic monitoring involved	72.7%	73.2%	72.1%
Any type of cyberstalking or electronic monitoring	26.6%	26.1%	27.4%
Cyberstalking	23.4	21.5	26.4
Electronic monitoring	6.0	7.8	3.4
Don't know	0.6	0.7	0.6
Percent of cyberstalking involving —[a]			
E-mail	82.6%	82.5%	82.7%
Instant messenger	28.7	35.1	20.7
Blogs or bulletin boards	12.5	12.3	12.8
Internet sites about victim	8.8	9.4	8.1
Chat rooms	4.0	4.4*	3.4*
Percent of electronic monitoring involving —[b]			
Computer spyware	44.1%	33.6%	81.0%*
Video/digital cameras	40.3	46.3	19.3*
Listening devices/bugs	35.8	41.8	14.8
GPS	9.7*	10.9*	5.2*
Number	5,200,410	3,158,340	2,042,070

Note: Table excludes 8.8% of all victims, 7.8% of stalking victims, and 10.2% of harassment victims due to missing data. Details sum to more than 100% because multiple responses were permitted.

*Estimate based on 10 or fewer samples.

[a]Based on 1,217,680 total victims, 677,870 stalking victims, and 539,820 harassment victims who experienced cyberstalking.

[b]Based on 314,400 total victims, 244,880 stalking victims, and 69,530 harassment victims who experienced electronic monitoring.

One in 7 victims reported they moved as a result of the stalking

The most common types of actions victims took to stop the stalking from continuing were to change usual activities outside of work or school, stay with family, or install caller ID or call blocking (table 8). The least frequent actions taken were to alter one's appearance or get pepper spray, a gun, or some other kind of weapon. Forty percent of stalking victims did not change their usual activities outside of work or school, take protective actions, or change their personal information.

Help from others

Seven in 10 victims of stalking sought help to protect themselves or to stop the stalking (table 9). Victims were most likely to enlist the help of family or friends, followed by asking people not to release information about him or her (43% versus 33%). About 7% of victims contacted victim services, a shelter, or a helpline.

Table 8. Whether stalking or harassment victims took actions to protect themselves or stop unwanted behaviors

	Percent of victims		
	All	Stalking	Harassment
Changed usual activities outside work or school			
Changed day-to-day activities	14.3%	21.6%	4.1%
Stayed with family	11.6	18.1	2.6
Took time off work or school	10.8	16.7	2.6
Avoided family/friends	10.3	14.9	3.7
Changed route to work or school	9.2	13.4	3.3
Changed or quit job or school	6.7	9.5	2.9
Altered appearance	1.5	2.3	0.4*
Took protective actions			
Installed caller ID/call blocking	13.4%	18.1%	6.7%
Changed telephone number	12.6	17.3	5.8
Changed locks/got security system	8.7	13.2	2.4
Got pepper spray	4.0	6.3	0.8*
Got a gun	1.9	2.9	0.5*
Got another kind of weapon	1.8	2.1	1.4*
Took self-defense classes	0.9	1.1	0.5*
Changed personal information			
Changed email address	5.9%	6.9%	4.4%
Changed social security number	0.3	0.2*	0.3*
Did not change behaviors listed	55.1%	39.7%	76.9%
Number	5,857,030	3,424,100	2,432,930

Note: Details sum to more than 100% because multiple responses were permitted.
*Estimate based on 10 or fewer sample cases.

Reasons stalking stopped

At the time of the interview, 3 in 5 of the victims reported the stalking had stopped, while about 2 in 5 reported it was ongoing (appendix table 7). The most common victim perceptions for why the unwanted contacts stopped were that the police warned the stalker (15.6%), the victim talked to the stalker (13.3%), or a friend or relative intervened (12.2%). About a tenth of victims attributed the cessation of the unwanted behavior to obtaining a restraining, protection, or stay away order.

Emotional impact

For stalking victims, the most common fear cited was not knowing what would happen next (table 10). Nine percent of stalking victims reported their worst fear was death. Twenty-nine percent of stalking victims feared the behavior would never stop. More than half of the stalking victims feared bodily harm to themselves, their child, or another family member.

More than 7 in 10 of all victims felt angry or annoyed at the beginning of the unwanted contacts or as they progressed (table 11). Stalking victims were about twice as likely as harassment victims to feel anxious or concerned at the

Table 9. Types of help sought by stalking or harassment victims

	Percent of victims		
	All	Stalking	Harassment
Total	100%	100%	100%
Enlisted help of friends/family	30.0	42.6	12.2
Asked people not to release information	24.0	32.9	11.6
Talked to boss/employer	16.2	21.6	8.6
Talked to an attorney	13.5	19.9	4.4
Obtained a restraining/protection/stay away order	9.4	15.6	0.6
Talked to a mental health professional	8.3	12.4	2.6
Contacted building/office security	6.4	9.2	2.5
Talked to clergy/faith leader	6.1	9.0	2.0
Talked to a doctor or nurse	6.0	9.1	1.5
Contacted victim services/shelter/help line	4.5	7.3	0.5*
Hired a private investigator	0.7	1.1	0.1*
Did not seek help**	47.3	30.3	71.2
Number of victims	5,857,030	3,424,100	2,432,930

Note: Details sum to more than 100% because multiple responses were permitted.
*Estimate based on 10 or fewer sample cases.
**Victims might have sought help from someone other than those listed above.

beginning of the unwanted contacts (52.7% versus 25.4%). As the unwanted contacts progressed, about 15% of stalking victims felt depressed or sick, and 1% reported feeling suicidal.

Workplace impact

Of the 79% of stalking victims who had a job during the 12 months preceding the interview, about 1 in 8 lost time from work because of fear for their safety or to pursue activities such as obtaining a restraining order or testifying in court (appendix table 8). Seven percent of victims lost time from work for activities such as changing a phone number, moving, or fixing or replacing damaged property. For 1 in 7 of these victims, a day or less was lost from work (appendix table 9). More than half of victims lost 5 or more days from work. About 130,000 victims reported that they had been fired from or asked to leave their jobs because of the stalking (not referenced in table).

Table 10. Victims' worst fears resulting from stalking

	Percent of victim
Not knowing what would happen next	46.1%
Behavior would never stop	29.1
Bodily harm	30.4
Harm or kidnap child	12.9
Harm other family member	12.2
Loss of freedom	10.3
Death	8.9
Loss of job	6.3
Harm current partner	6.0
Losing one's mind	4.3
Other	16.6
Don't know	5.3
Number of victims	3,416,900

Note: Table excludes 0.2% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.
*Estimate based on 10 or fewer sample cases.

Financial impact of stalking on victim

About 3 in 10 of stalking victims accrued out-of-pocket costs for things such as attorney fees, damage to property, child care costs, moving expenses, or changing phone numbers (appendix table 10). About a tenth of victims spent less than $250, while 13% spent $1,000 or more. About 296,000 stalking victims lost pay from work (appendix table 11). Over half of the victims lost less than $1,000 of pay, and 8% of victims lost $5,000 in pay or more.

Stalkers commit various types of crimes against their victims

Stalking offenders committed identity theft against about 204,000 victims. Over half of these victims had financial accounts opened or closed in their names or money taken from their accounts, and 3 in 10 of these victims had items charged to their credit cards without their consent.

Any identity theft	204,230	100%
Opened/closed accounts	110,850	54.3
Took money from accounts	105,130	51.5
Charged items to credit card	60,790	29.8

Note: Estimates exclude 0.1% of missing data. Details sum to more than 100% because multiple responses were permitted.

Table 11. How the victim felt when the stalking or harassment began and progressed

	Percent of victims					
	All		Stalking		Harassment	
	Beginning	Progressed	Beginning	Progressed	Beginning	Progressed
Annoyed/angry	72.5%	74.2%	68.9%	69.6%	78.1%	81.4%
Anxious/concerned	42.2	36.2	52.7	46.7	25.4	19.4
Frightened	26.8	25.7	41.7	41.7	3.2*	~[a]
Helpless	15.6	16.4	22.4	23.4	4.8	5.1
Depressed	10.8	10.2	15.9	15.2	2.8	2.3
Sick	10.0	9.8	14.8	14.7	2.2*	1.8
Suicidal	0.9	0.9	1.4	1.4	~	~[b]
Other way	9.7	10.1	7.9	8.9	12.4	11.9
Number of victims	5,574,400	5,530,940	3,416,430	3,406,220	2,157,960	2,124,720

Note: Table excludes 4.8% of all victims, 5.6% of all stalking victims, and 0.2% of harassment victims at the beginning of the behaviors and 0.5% of all victims, 11.3% of all stalking victims, and 12.7% of harassment victims as the behaviors progressed due to missing data. Details sum to more than 100% because multiple responses were permitted.
*Estimate based on 10 or fewer sample cases.
~Not applicable.
[a]Harassment victims, by definition, were not frightened as the unwanted behaviors progressed.
[b]Harassment victims, by definition, did not report feeling suicidal as a result of the unwanted behaviors.

About 16% of all victims suffered property damage in conjunction with the stalking (table 12). Among stalking victims, the most common type of violent crime experienced in conjunction with stalking was to be hit, slapped, or knocked down (12.3%). About 6% of the stalking victims had a family member, friend, or co-worker who was attacked.

Weapon involvement and injuries

About 139,000 stalking victims were attacked with a weapon. Stalkers were equally likely to use a knife, blunt instrument, or other object, and 23% of the weapons used were handguns. Of the 279,000 victims who were injured in an attack, nearly all (99%) of these victims sustained minor bruises and other injuries. About a fifth sustained serious injuries, including gunshot or knife wounds, internal injuries, or broken bones.

Weapon used in attack	138,630	100%
Knife/other sharp object	58,850	42.4
Handgun	31,610	22.8*
Blunt or other object	52,670	38.0

*Estimate based on 10 or fewer sample cases.

Injuries sustained in attacks	278,580	100%
Rape/sexual assault	38,590	13.9*
Serious injuries	52,080	18.7
Minor or other injuries	276,440	99.2

Note: Details sum to more than 100% because multiple responses were permitted.
*Estimate based on 10 or fewer sample cases.

Threats

Stalkers made one or more threats to 43% of victims (table 13). Stalking offenders were most likely to threaten to hit, slap, or otherwise harm the victim (13.6%) or to kill the victim (12.1%). Somewhat less likely was the stalker threatening to kill himself or herself (9.2%). Less than 5% of the threats involved harm to a child, friend, co-worker, pet, or the threat of rape or sexual assault.

Stalking victimization was equally likely to be reported to police whether the victim was male or female

For violent crime more generally, victimizations experienced by females are more likely to be reported to the police than those experienced by males. However, this pattern of reporting by gender is not observed for the crime of stalking. Male and female stalking victimizations were equally likely to be reported to the police (table 14). Thirty-seven percent of male and 41% of female victimizations were reported to the police by the victim or another person aware of the crime.

The most common reasons for not reporting stalking victimization to the police were that it was a private or personal matter or that it was a minor incident (appendix table 12).

About 40% of victims stated that police were contacted once regarding the stalking, while 3% of victims stated that police were contacted in excess of 15 times (appendix table 13). Stalking victimization was most often reported to the police by the victim (83%), the victim's family (26%), or a friend or neighbor (12%) (appendix table 14).

Table 12. Other crimes perpetrated by the offender against the stalking or harassment victim

	Percent of victims		
	All	Stalking	Harassment
Property damage	15.9%	24.4%	4.0%
Damaged property of victim or someone in victim's household	9.5	15.0	1.8
Illegally entered house/apartment	8.6	13.2	2.2
Illegally entered car	3.8	6.3	0.5*
Attacked victim	12.3%	21.0%	0.0%
Hit/slapped/knocked down	7.2	12.3	~
Choked or strangled victim	2.4	4.2	~
Attacked victim with a weapon	2.4	4.0	~
Chased or dragged with a car	2.1	3.5	~
Raped/sexually assaulted victim	0.9	1.6	~
Attacked or attempted to attack in some other way	4.3	7.3	~
Attacked person/pet other than victim	8.8%	15.0	4.0%
Attack or attempt to attack a family member	3.5	6.0	~
Attack or attempt to attack a friend or co-worker	3.4	5.8	~
Attack or attempt to attack a pet	2.2	3.7	~
Attack or attempt to attack a child	2.2	3.7	~
Number of victims	5,857,030	3,424,100	2,432,930

*Based on 10 or fewer sample cases.
~Not applicable. Harassment victims by definition were not attacked, nor were their friends, co-workers, family members, or pets.

Table 13. Threats offenders made against stalking victims

	Percent of victims	
	Number	Percent
Total	3,392,520	100%
No threats made	1,927,020	56.8%
Threatened to—	1,465,510	43.2%
Hit/slap/harm	462,610	13.6
Kill victim	411,830	12.1
Harm or kill self	313,580	9.2
Harm with a weapon	242,420	7.1
Harm another family member	209,770	6.2
Harm or kidnap child	166,230	4.9
Harm friend or co-worker	151,460	4.5
Harm a pet	87,020	2.6
Rape/sexually assault	56,050	1.7
Other way	511,530	15.1

Note: Table excludes 0.9% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.

Stalking victims report differing experiences with the criminal justice system

When contacted about a stalking victimization, the most common police response was to take a report. More than half of police officers took a report when contacted regarding the stalking (appendix table 15). Seventeen percent of responding officers gave the victim self-protection advice, while 8% of the officers arrested the perpetrator.

Nearly 20% of victims stated the police took no action when contacted. Of this 20%, victims were equally likely to perceive that no action was taken by law enforcement because police did not want to get involved (29%), had no legal authority (18%), or were inefficient or ineffective (16%) (appendix table 16). About 50% of victims perceived the stalking situation stayed the same after contacting the police (appendix table 17). Victims were equally likely to perceive the situation "improved" or "worsened" following a report to the police. For victims who had contacted police on more than one occasion, the survey recorded only the police action taken in response to the latest call.

A fifth of victims filed charges against the stalking perpetrator (appendix table 18). Of those individuals filing charges, 3 out of 10 victims stated the outcome was still pending or that a restraining, protection, or stay away order was issued to deal with the offender. Victims were equally likely to report being satisfied (46%) or dissatisfied (49%) with the criminal justice system's responses to their stalking incident (appendix table 19) and were generally split on the helpfulness or lack of helpfulness of criminal justice representatives, with one exception: some victims said that victim advocates were helpful (6%) during the criminal justice process (appendix table 20).

Table 14. Percent of stalking and harassment victimizations reported to the police, by victim gender

	Percent of victims					
	All		Stalking		Harassment	
	Male	Female	Male	Female	Male	Female
Total	100%	100%	100%	100%	100%	100%
Reported	20.6	32.8	36.8	41.0	6.8	13.9
Not reported	79.4	67.2	63.2	59.0	93.2	86.1
Number of victims	1,941,650	3,637,570	892,340	2,528,990	1,049,320	1,108,580

Note: Table excludes 4.5% of all male victims, 4.9% of all female victims, 0.1% of female stalking victims, 8% of male harassment victims, and 14.2% of female harassment victims due to missing data.

Methodology

The Supplemental Victimization Survey (SVS) was administered as a supplement to the National Crime Victimization Survey (NCVS) during January through June, 2006. All NCVS respondents age 18 and older were eligible for the supplement. About 65,270 persons participated in the supplemental survey. The response rate for eligible individuals was 83%.

The estimates presented in this report are annual prevalence estimates for persons age 18 or older victimized by stalking or other harassing behaviors during the 12 months prior to the interview. Since the interviews were conducted during the first 6 months of 2006, the majority of the stalking behaviors occurred during 2005.

The Office on Violence Against Women (OVW) and the Bureau of Justice Statistics (BJS) convened a 1-day forum with experts in the area of stalking and violence against women. Researchers, law enforcement officials, prosecutors, and victim advocates comprised the expert group. Also included in the group were representatives from the Census Bureau, the federal agency that carries out survey development and data collection for BJS. The purpose of the 1-day forum was to discuss definitional and methodological issues surrounding the crime of stalking, determine where gaps in current information on stalking existed, and determine how the SVS could further research and knowledge regarding this crime.

Following this meeting, a small federal working group was formed with representatives from OVW, BJS, and the Census Bureau. The working group met weekly for approximately 12 months until a satisfactory survey instrument was completed and approved. During the last phase of the survey development, the Census Bureau conducted cognitive interviews with stalking victims around the United States to test the reliability and validity of the instrument. Changes to the instrument were made to incorporate findings from these interviews.

The name of the SVS intentionally does not indicate that the focus of the supplemental survey is stalking. This decision was made to avoid biasing the responses of individuals and the subsequent estimates. The respondents had to state that they experienced all of the following in order for a course of behavior to be counted as stalking victimization:

- at least one of the harassing behaviors in the stalking screener
- harassing behavior more than one time on separate days
- at least one of the harassing contacts occurred during the 12 months prior to the interview
- they feared for their own or a family member's safety or experienced another crime committed by the offender that would make a reasonable person fearful (see the survey screen questions on the next page).

Victim perception of whether behavior was stalking

The SVS screened victims to determine whether they met the behavioral criteria of having unwanted or harassing contacts on more than one occasion during the past year that made them feel annoyed, fearful, anxious, or concerned. Researchers specifically avoided using the term "stalked" throughout the questionnaire so as not to bias findings based on the victim's perception of what was occurring. The final question in the supplement asked whether the victim perceived the unwanted contacts or harassing behaviors to be stalking. Stalking victims were more than twice as likely as harassment victims to label the unwanted behavior as stalking (54% versus 21%).

Victim perception of whether behavior was stalking	Percent of victims		
	All	Stalking	Harassment
Total	100%	100%	100%
Considered to be—			
Stalking	40.3%	53.6%	20.7%
Not stalking	59.7	46.4	79.3
Number of victims	5,588,150	3,325,220	2,262,940

Note: Table excludes 4.6% of all victims, 2.9% of stalking victims, and 7.0% of harassment victims due to missing data.

The final question on the survey asked, "Do you consider the series of unwanted contacts or harassing behavior you told me about to be stalking?"

Victims of harassment met all the requirements for stalking victimization except those associated with induced fear or the commission of additional associated crimes. Harassing acts by bill collectors, telephone solicitors, or other sales people were excluded from the estimates of stalking and harassment.

Standard error computations

Comparisons of percentages and rates made in this report were tested to determine if observed differences were statistically significant. Differences described as higher, lower, or different passed a test at the 0.05 level of statistical significance (95% confidence level). Differences described as somewhat, lightly, marginally, or some indication passed a test at the 0.10 level of statistical significance (90% confidence level). Caution is required when comparing estimates not explicitly discussed in the report.

Screener questions for stalking behaviors

Now, I would like to ask you some questions about any unwanted contacts or harassing behavior you may have experienced that frightened, concerned, angered, or annoyed you. Please include acts committed by strangers, casual acquaintances, friends, relatives, and even spouses and partners. I want to remind you that the information you provide is confidential.

1. Not including bill collectors, telephone solicitors, or other sales people, has anyone, male or female, EVER – frightened, concerned, angered or annoyed you by ...

a. Making unwanted phone calls to you or leaving messages?
b. Sending unsolicited or unwanted letters, e-mails, or other forms of written correspondence or communication?
c. Following you or spying on you?
d. Waiting outside or inside places for you such as your home, school, workplace, or recreation place?
e. Showing up at places where you were even though he or she had no business being there?
f. Leaving unwanted items, presents, or flowers?
g. Posting information or spreading rumors about you on the Internet, in a public place, or by word of mouth?
f. None

Questions used to identify actions that would cause a reasonable person to feel fear

1. In order to frighten or intimidate you, did this person attack or attempt to attack

a. a child
b. another family member
c. a friend or co-worker
d. a pet

2. During the last twelve months, did this person attack or attempt to attack you by...

a. hitting, slapping, or knocking you down
b. choking or strangling you
c. raping or sexually assaulting you
d. attacking you with a weapon
e. chasing or dragging with a car
f. attacking you in some other way

3. Other than the attacks or attempted attacks you just told me about, during the last 12 months, did this person threaten to...

a. kill you
b. rape or sexually assault you
c. harm you with a weapon
d. hit, slap, or harm you in some other way
e. harm or kidnap a child
f. harm another family member
g. harm a friend or co-worker
h. harm a pet
i. harm or kill himself/herself

4. What were you most afraid of happening as these unwanted contacts or behaviors were occurring?

a. death
b. physical/bodily harm
c. harm or kidnap respondent's child
d. harm current partner/boyfriend/girlfriend
e. harm other family members
f. don't know what would happen

Questions used to measure fear

1. How did the behavior of (this person/these persons) make you feel when it FIRST started? Anything else?

a. anxious/concerned
b. annoyed/angry
c. frightened
d. depressed
e. helpless
f. sick
g. suicidal
h. some other way – *specify*

2. How did you feel as the behavior progressed? Anything else?

a. no change in feelings
b. anxious/concerned
c. annoyed/angry
d. frightened
e. depressed
f. helpless
g. sick
h. suicidal
i. some other way - *specify*

Appendix table 1. Perceived age of the stalking offender, by age of the victim

Offender age	Age of the victim				
	18-20	21-29	30-39	40-49	50 or older
Total	100%	100%	100%	100%	100%
Under 18	10.9*	0.7*	1.8*	2.1*	2.0*
18-20	41.6	5.7	2.3*	2.9*	1.0*
21-29	23.3	48.2	13.8	8.8	3.8*
30-39	5.1*	23.0	37.6	16.7	16.3
40-49	6.7*	7.7	20.8	34.2	18.7
50 or older	2.4*	5.9	9.9	21.6	34.6
Age of offender unknown	10.0*	8.8	13.9	13.7	23.6
Number of victims	349,490	929,080	752,690	722,890	663,660

Note: Table excludes missing data about offenders from 0.8% of stalking victims age 30 to 39.
*Based on 10 or fewer sample cases.

Appendix table 2. Perceived race of the stalking offender, by race of the victim

Offender race	Victim race		
	White	Black	Some other race
Total	100%	100%	100%
White	82.8	12.5*	45.4
Black	5.2	65.6	16.0*
Some other race	7.6	11.8*	29.8
Race of offender unknown	4.3	10.1*	8.8*
Number of victims	2,582,360	328,900	160,400

*Based on 10 or fewer sample cases.

Appendix table 3. Number of stalking offenders perceived by victim

	Percent of victims
Total	100%
One	62.1
Two	18.2
Three or more	13.1
Number unknown	6.5
Number of victims	3,398,630

Note: Table excludes 0.7% of stalking victims due to missing data.

Appendix table 4. Employment status of the stalking offenders, as perceived by victims

	Percent of victims
Total	100%
Employed	42.1
Unemployed	24.9
Sometimes employed/unemployed	6.4
Victim unable to determine employment status	26.6
Number of victims	3,420,450

Note: Table excludes 0.1% of stalking victims due to missing data.

Appendix table 5. Stalking victims' perceptions of offenders' previous problems with the law

	Percent of victims
Total	100%
Offender had problems with the law	35.9
Offender did not have problems with the law	26.3
Victim unable to determine if offender had problems with the law	37.8
Number of victims	3,410,710

Note: Table excludes data about offenders from 0.4% of stalking victimizations.

Appendix table 6. Frequency of stalking during the 12 months prior to the interview

	Number	Percent of victims
Total	3,416,100	100%
1-2 times/year	381,540	11.2
1-2 times/month	565,790	16.6
1-2 times/week	770,380	22.6
Almost every day	576,960	16.9
At least once a day	204,860	6.0
No set pattern	864,920	25.3
Don't know	51,650	1.5

Note: Table excludes 0.2% of stalking victims due to missing data.

Appendix table 7. Victims' perceptions of whether stalking had stopped and reasons it stopped

	Number	Percent of victims
Total	3,404,110	100%
Stalking ongoing	1,234,330	36.3%
Stalking stopped	1,976,050	58.0%
Respondent took measures		
Victim talked to stalker	263,790	13.3%
Victim moved	214,150	10.8
Victim changed phone or email	210,910	10.7
Restraining/protection/stay away order	187,220	9.5
Victim got married or started new relationship	40,390	2.0
Perpetrator stopped behavior		
Stalker moved	172,220	8.7%
Stalker was arrested or incarcerated	129,470	6.6
Stalker started a new relationship	80,580	4.1
Stalker got help/counseling	48,130	2.4
Stalker died	9,320	0.5*
Others intervened		
Police warned stalker	309,060	15.6%
Friend or relative intervened	240,350	12.2
Others intervened	163,020	8.2
Employer intervened	105,490	5.3
School staff intervened	42,230	2.1
Other reason	501,730	25.4%
Don't know why stalking stopped	297,230	15.0%
Don't know whether stalking stopped	208,940	10.6%

Note: Table excludes 0.6% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.

Appendix table 8. Time lost from work for any reason as a result of stalking victimization

	Number	Percent of victims
Total	3,388,550	100%
Not working	708,070	20.9
Working	2,680,470	79.1
Reason for time lost from work		
Fear or concern for safety	350,940	13.1%
Getting a restraining/protection order or testifying in court	320,450	12.0
Changing phone number/moving/fixing damaged property	183,120	6.8

Note: Table excludes 1% of cases due to missing data. Details sum to more than 100% because multiple responses were permitted.

Appendix table 9. Amount of time victims lost from work for any reason as a result of stalking

	Number	Percent of victims
Total	540,360	100%
Less than a day	76,060	14.1
1 day	51,920	9.6
2 days	57,540	10.6
3 days	42,830	7.9
4 days	24,900	4.6*
5-9 days	77,350	14.3
10-24 days	60,690	11.2
25 or more days	78,420	14.5
Don't know	70,650	13.1

Note: Table excludes 2.5% of stalking victims due to missing data. Total based on victims who had a job and lost time from work. Detail may not sum to 100% due to rounding.
*Estimate based on 10 or fewer sample cases.

Appendix table 10. Out-of-pocket costs to victims as a result of stalking

	Number	Percent of victims
Total	3,358,800	100%
$0	2,080,230	61.9
$1-99	193,060	5.7
$100-249	151,460	4.5
$250-499	90,420	2.7
$500-999	89,730	2.7
$1,000-2,499	155,010	4.6
$2,500-4,999	91,350	2.7
$5,000 or more	188,110	5.6
Don't know	319,430	9.5

Note: Table excludes 1.9% of stalking victims due to missing data. Detail may not sum to 100% due to rounding.

Appendix table 11. Amount of employment income lost as a result of stalking victimization

	Number	Percent of victims
Total	296,450	100%
$1-99	44,340	15.0
$100-999	110,430	37.2
$1,000-2,499	40,620	13.7
$2,500-4,999	17,990	6.1
$5,000 or more	23,690	8.0
Don't know	59,450	20.1

Note: Table excludes 3.3% of stalking victims due to missing data.

Appendix table 12. Victim reasons for not reporting stalking to police

	Percent of victims
Dealt with another way	
Private or personal matter	26.7%
Reported to another official	13.6
Not important enough to report	
Minor incident	27.2
Not clear a crime occurred	11.2
Police couldn't help	
Couldn't identify offender/lacked evidence	9.5
Had no legal authority	3.0
Lacked correct protection, stay away, or restraining order	0.5*
Police wouldn't help	
Police wouldn't think it was important/would be ineffective	11.0
Police wouldn't believe respondent/would blame respondent	4.0
Previous negative experience with police	1.5*
Perpetrator was a police officer	0.8*
Feared the perpetrator	
Afraid of reprisal	5.9
Other reasons	
Protect perpetrator/perpetrator was ex-spouse or ex-partner	6.9
Contacts/behavior stopped	5.9
For the sake of the children	3.8
Respondent felt ashamed/embarrassed	3.3
Respondent or perpetrator moved away	1.3*
Other	17.6
Don't know	1.2*
Number of victims	2,055,080

Note: Table excludes 1.9% of stalking victims due to missing data. Details sum to more than 100% because multiple responses are permitted.
*Based on 10 or fewer sample cases.

Appendix table 13. Number of police contacts regarding stalking during the last 12 months

	Percent of victims
Total	100%
1	39.7
2	22.1
3	12.9
4	6.4
5-10	11.9
11-15	3.7
More than 15	3.2
Number of victims	1,240,280

Note: Table excludes 9.2% of stalking victims due to missing data.

Appendix table 14. Identity of person reporting stalking to police

	Percent of victims
Victim	83.0%
Victim's family	26.2
Friend/neighbor	11.5
Other	4.1
Employer/co-worker	2.3*
Social worker/counselor	1.4*
School official	1.4*
Security guard	1.2*
Clergy/pastor/priest	0.5*
Stranger/bystander	0.5*
Doctor/nurse	0.5*
Don't know	1.6*
Number of victims	1,350,130

Note: Table excludes 1.2% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.
*Based on 10 or fewer sample cases.

Appendix table 15. Types of action taken by police after most recent contact about stalking

	Percent of victims
Took a report	55.3%
Talked to/warned offender	32.2
Suggested protection, stay away or restraining order	20.1
Gave victim self-protection advice	17.4
Referred victim to court	8.9
Arrested offender	7.7
Asked for more evidence	6.4
Referred victim to victim services	5.4
Moved respondent to another location	1.3*
Don't know	4.1
Took no action	18.8
Number of victims	1,343,090

Note: Table excludes 1.7% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.
*Based on 10 or fewer sample cases.

Appendix table 16. Stalking victims' perceptions about why police did not take action

	Percent of victims
Didn't want to get involved	28.6%
Had no legal authority	17.7
Police were inefficient/ineffective	16.2
Didn't believe victim	13.2*
Didn't have enough evidence	11.2*
Offender was a police officer	5.7*
Could not find/identify offender	4.0*
Lacked or had incorrect protection order	3.0*
Thought it was victim's fault	2.9*
Didn't find out until too late	2.8*
Other	36.3
Number of victims	240,030

Note: Table excludes 4.9% of stalking victims due to missing data. Details sum to more than 100% because multiple responses were permitted.
*Based on 10 or fewer sample cases.

Appendix table 17. Victim perceptions of outcomes after first reporting stalking to police

	Percent of victims
Total	100%
Situation got better	28.2
Situation got worse	22.9
Situation stayed the same	48.9
Number of victims	1,325,720

Note: Table excludes 3% of stalking victims due to missing data.

Appendix table 18. Percent of stalkings in which criminal justice charges were filed and outcomes

	Percent	
Total	100%	
Charges not filed	71.5	
Charges filed	21.0	
Still pending		33.3%**
Restraining, protection, stay away order		28.5
Jailed or imprisoned		18.0
Court intervention/counseling program		12.2*
Convicted or guilty		12.0*
Fine was imposed		11.8*
Dismissed or not guilty		9.1*
Probation		8.5*
Other		12.9*
Don't know outcome of charges filed		5.1*
Don't know if charges filed	7.5	
Number of victims	1,329,790	

Note: Table excludes 2.7% of stalking victims that did not respond to whether charges were filed and 9.4% of victims that did not respond to the outcome of charges filed.
*Based on 10 or fewer sample cases.
**Details sum to more than 100% because multiple responses were permitted.

Appendix table 19. Stalking victim satisfaction with criminal justice outcome

	Percent of victims
Total	100%
Victim satisfied with outcome	45.7
Victim not satisfied with outcome	49.0
Don't know if satisfied with outcome	5.2*
Number of victims	169,040

Note: Table excludes 13.5% of stalking victims that filed charges due to missing data. Detail may not sum to 100% due to rounding.
*Based on 10 or fewer sample cases.

Appendix table 20. Stalking victim perceptions about helpfulness of officials in the criminal justice system

	Percent of victims who perceived official as—	
	Helpful	Not helpful
Patrol/police officer/sheriff	43.0%	41.9%
911 dispatcher	3.6	2.8
Detective	5.3	3.0
Prosecutor/District Attorney	6.9	7.8
Judge	7.4	7.2
Victim advocate	5.7	2.0*
Someone else	8.9	8.0
No person was helpful	36.0	~
No person was unhelpful	~	40.3
Victim did not provide response	3.3	2.7*
Number of victims	1,359,060	1,359,060

Note: Details sum to more than 100% because multiple responses were permitted.
~Not applicable.
*Based on 10 or fewer sample cases.

U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Statistics

Washington, DC 20531

PRESORTED STANDARD
POSTAGE & FEES PAID
DOJ/BJS
Permit No. G-91

Official Business
Penalty for Private Use $300

This report in portable document format and in ASCII and its related statistical data and tables are available at the BJS World Wide Web Internet site: <http://www.ojp.usdoj.gov/bjs/abstract/svus.htm>.

Office of Justice Programs

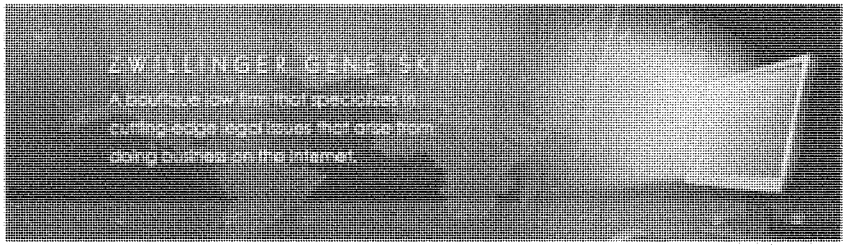
Innovation • Partnerships • Safer Neighborhoods
http://www.ojp.usdoj.gov

The Bureau of Justice Statistics is the statistical agency of the U.S. Department of Justice. Michael D. Sinclair is deputy director.

This report was written by Katrina Baum, Ph.D., Shannan Catalano, Ph.D., Michael Rand, and Kristina Rose. Cathy Maston, Patsy Klaus, Lara Allen, and Thomas Cohen provided statistical review. Tina Dorsey produced the report, Catherine Bird and Jill Duncan edited the report, and Jayne E. Robinson prepared the report for final printing.

January 2009, NCJ 224527

Law Across the Wire and Into the CloudRecent Developments in Internet Law



- Home
- Careers at Zwillinger Genetski

Subscribe to Articles

Are Smartphones Making Stakeouts A Thing Of the Past?

Author: Jennifer Granick Category: Electronic Communications Privacy Act (ECPA), Fourth Amendment

Wednesday
Apr 27, 2011

Senator Al Franken and Representative Ed Markey, inspired by last week's news that Apple iPhones and iPads store a year's worth of your location information on the handset and on any synced computer, have demanded that Apple answer questions about whether and how it uses that data. Franken and Markey should also ask the Department of Justice the same questions. While the public is only recently discovering that their personal devices create this footprint map, law enforcement and the digital forensics companies that serve them have known for quite some time. The public has a right to know what legal process, if any, the police are using before they find out where you've been for the past 12 months.

If the collected location data is sent back to Apple and stored there, then the Electronic Communications Privacy Act ("ECPA") is the best candidate for protecting that information from warrantless snooping by the police. (Same with Google, which is reportedly collecting the same kind of information, but storing it for less time.) As for the data kept on your phone or personal computer, the Fourth Amendment should protect that, but there are gaping loopholes that will open your travel data up to law enforcement eyes.

ECPA was passed on 1986 and it's safe to say that Congress wasn't thinking about protecting data generated by smartphones that fit in your pocket and can store a year's worth of cell tower and wifi access points, not to mention text messages, email, photos and the like. And yet, that is the law we rely on to protect our data stored with third party service providers.

As security researcher and computer scientist Chris Soghoian noted last week, not all data stored with a third parties is protected by ECPA. Rather, the data must be generated by the provision of one of two kinds of computing services:

An "electronic communication service" ("ECS") is "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. 2510(15).

A "remote computing service" ("RCS") is a "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. 2711(2).

ECPA protects communications content from and information pertaining to an ECS or RCS customer. But, if the service being utilized is neither an ECS, nor an RCS, law enforcement agencies could obtain the information with a mere subpoena, or the provider may voluntarily disclose it.

So the first question is whether the location data Apple and Google may be collecting from your handset is generated through the provision of either an ECS or RCS service. Modern communications technologies change so quickly that there aren't a lot of cases defining how ECPA applies to the data those services generate. However, when you use your phone's GPS or triangulation information to send a message about your physical location to your friends (i.e. to "check in" somewhere), that should be the content of a communication passed through an ECS. Officers will need a search warrant to get that data if it is not already publicly available.

When the phone company collects location data automatically generated in the process of your phone connecting to cell towers to make calls, that's not content, but it is information pertaining to your use of an ECS service. Law enforcement needs at least some kind of court order to get that information. 18 U.S.C. 2703(c); *In re The Application of the United States for an Order Directing a Provider of Electronic Communication Service to Disclose Records to the Government*, 620 F.3d 304 (3d Cir. 2010).

What about when the phone automatically generates data merely by virtue of being turned on, and the provider collects that data? If the provider is collecting the data as part of the provision of the cellular service, then that data is ECS information pertaining to the customer, and covered by ECPA. It doesn't have to be content to be ECPA protected, it just has to be generated as part of the provision of the service.

But this doesn't necessarily answer the ECPA question with regard to Apple or Google, who are not providing a communications service, but merely selling a handset that can connect to such a service. Ars Technica cites the companies' reasons for collecting this data as useful when GPS data isn't available, or to more quickly narrow down a location while GPS services are being polled (known as "assisted" or aGPS), as well as building and maintaining databases of known cell tower and WiFi basestation locations. So, if the handset manufacturers are collecting location information, not as part of providing you with cellular service, but in order to generate their own databases of information, is that an ECS service such that the data generated is covered by ECPA?

If the information would not fall under the protections of ECPA, law enforcement agencies might be able to obtain it with just a subpoena. While one court has held that your location information is Fourth Amendment protected, the primary privacy protection here has to be for the companies to collect the information in a manner that could not be traced back to a specific user. But, if this data can tell you where I've been, then Congress should ask what legal process, if any, the companies are requiring for law enforcement before disclosure.

A second privacy problem is whether any legal process is required to obtain the data directly from the handset or from your computer. ECPA doesn't apply to data stored on your personal devices, but the Fourth Amendment does. Generally, that means law enforcement needs a warrant based on probable cause to get that data. However, there are two exceptions to the warrant requirement which the government has been using to get access to computer data. One the border search exception and the other is the search incident to arrest doctrine. Both doctrines are getting a work over in the context of computer searches, and not in favor of privacy.

The border search exception holds that agents do not need any cause or judicial approval to search the body or personal effects at the border, but do need reasonable suspicion for invasive techniques like a strip search. When I was at EFF, we filed an amicus brief in the case of *United States v. Arnold*, arguing that laptop searches are so revealing and invasive that the Fourth Amendment requires agents to have some reasonable suspicion at the border to justify the intrusion. We lost that case. The Ninth Circuit panel rejected our argument that the privacy invasion resulting from searching computers is qualitatively different from, and requires higher suspicion than, searching luggage or other physical items.

This latest information about the kind of historical location data that the average laptop or smart phone holds is additional factual support for the proposition that EFF was right to argue that phone and laptop searches are categorically different types of privacy invasions than luggage searches.

The search incident to arrest doctrine is another exception to the general requirement that police obtain a warrant before conducting a search. The purpose of this exception is to protect the officer by locating and seizing any weapons the person has and to prevent the destruction of any evidence on the person. Thus, if an arrest is valid, officers may conduct a warrantless search of the arrestee and the area and objects in close proximity — i.e. the "grab area" — at about the same time as the arrest.

There aren't many cases considering whether officers can search the data stored on phones (or laptops) as a search incident to arrest, and the rulings we have go both ways. Given the rationale behind the search incident to arrest exception, courts have generally looked to the volatility of the data to see whether there's a threat of spoliation of evidence, which is clearly not an issue with the iPhone location log which stores information for a year. However, the most recent case on the issue, from the California Supreme Court earlier this year, took a different approach. That Court ruled in *People v. Diaz* that police didn't need any exigency to search text messages incident to arrest because searching data on the phone is the same as searching the arrested person and thus the Fourth Amendment doesn't require a threat to officer safety or of evidence destruction. (That ruling will probably be appealed to the federal courts.)

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

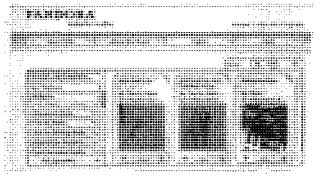
THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | APRIL 5, 2011, 8:06 A.M. ET

Mobile-App Makers Face U.S. Privacy Investigation

By AMIR EFRATI, SCOTT THURM and DIONNE SEARCEY

Federal prosecutors in New Jersey are investigating whether numerous smartphone applications illegally obtained or transmitted information about their users without proper disclosures, according to a person familiar with the matter.



Online-music streaming service Pandora, which plans an initial public offering, says in an SEC filing that it has been subpoenaed in an investigation probing information-sharing by mobile applications. John Letzing and Stacey Delo discuss.

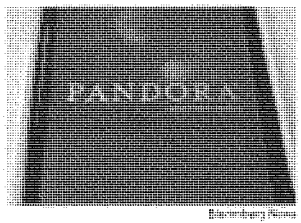
The criminal investigation is examining whether the app makers fully described to users the types of data they collected and why they needed the information—such as a user's location or a unique identifier for the phone—the person familiar with the matter said. Collecting information about a user without proper notice or authorization could violate a federal computer-fraud law.

Online music service Pandora Media Inc. said Monday it received a subpoena related to a federal grand-jury investigation of information-sharing practices by smartphone applications.

Pandora disclosed the subpoena, issued "in early 2011," in a Securities and Exchange Commission filing. The Oakland, Calif., company said it had been informed it is "not a specific target of the investigation." Pandora said it believed similar subpoenas had been issued "on an industry-wide basis to the publishers of numerous other smartphone applications."

A Pandora spokeswoman declined to comment.

The Wall Street Journal reported in December that popular applications on the iPhone and Android mobile phones, including Pandora, transmit information about the phones, their users and their locations to outsiders, including advertising networks.



Bloomberg News

Smartphone apps—of which there are thousands—are software programs that allow, say, a user to read an e-book, play a game, get sports scores or search for a restaurant.

The Journal tested 101 apps and found that 56 transmitted the phone's unique device identifier to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent a user's age, gender and other personal details to outsiders. At the time they were tested, 45 apps didn't provide privacy policies on their websites or inside the apps.

In Pandora's case, both the Android and iPhone versions of its app transmitted information about a user's age, gender, and location, as well as unique identifiers for the phone, to various advertising networks. Pandora gathers the age and gender information when a user registers for the service.

Legal experts said the probe is significant because it involves potentially criminal charges that could be applicable to numerous companies. Federal criminal probes of companies for online privacy violations are rare.

Anthony Campiti, creator of the Pumpkin Maker iPhone app, said he received a subpoena requesting information and documents related to his app. Mr. Campiti said he had turned the request over to his lawyer and didn't recall who had issued the subpoena.

"They're just doing information-gathering to get a better understanding" of the industry, Mr. Campiti said. "We're not doing anything wrong and neither is anyone else doing anything wrong."

The probe, which likely will continue for months, may not result in any charges.

Rebekah Carmichael, a spokeswoman for Paul J. Fishman, the U.S. attorney in New Jersey, declined to comment.

Earlier

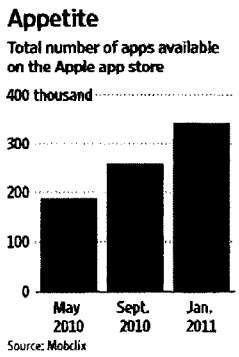
Your Apps Are Watching You

How One App Sees Location Without Asking

Apple Inc. and Google Inc., which oversee digital "stores" that offer mobile applications to users of iPhones, iPads and mobile-devices powered by Google's Android software, have been asked to provide information about the applications and app makers, the person familiar with the matter said.

An Apple spokesman declined to comment. Google didn't respond to requests for comment.

One app maker mentioned in the Journal's article, Max Binshtok, creator of the Daily Horoscope Android app, said he had not received a subpoena. Makers of other applications declined to comment or didn't respond to requests for comment. The Journal also tested its own app, which didn't send information to outsiders. A Journal spokeswoman declined to comment.



The probe centers on whether app makers violated the Computer Fraud and Abuse Act, said the person familiar with the matter. That law, crafted to help prosecute hackers, covers information stored on computers. It could be used to argue that app makers "hacked" into users' cellphones.

"This is a big hammer if the government chooses to use it," said Orin S. Kerr, a law professor at George Washington University.

Legal experts said, in general, companies rarely end up being charged with a crime, and that the current probe could morph into a civil one.

They said companies in the federal government's cross hairs often reach non-prosecution or deferred-prosecution agreements that allow the targets to avoid being criminally charged. In exchange, the companies may agree to concessions, including monetary payments or promising not to engage in future wrongdoing, among other things.

Earlier this year, federal prosecutors in New Jersey criminally charged two individuals for allegedly attacking servers at AT&T Inc. and obtaining email addresses of more than 100,000 users of Apple's iPad device, including members of the U.S. government and military. Those individuals are fighting the charges.

Several companies involved in smartphone apps are facing civil lawsuits from consumers alleging their privacy has been violated through the transmission of personal information. A Los Angeles man filed suit in U.S. District Court for the Northern District of California against Apple, Pandora and other defendants in December, seeking class-action status on behalf of iPad and iPhone users. The suit claims that apps downloaded to those devices "have been transmitting their personal, identifying information to advertising networks without obtaining their consent."

Makers of apps could also face complaints of unfair and deceptive trade practices from the Federal Trade Commission. Such complaints can be aimed at companies that fail to tell customers how they are collecting information or are violating their own terms of service.

"Hopefully this will bring about a big change in the industry and make companies be more responsible in what data is being collected," said Ginger McCall, an assistant director at privacy advocacy group Electronic Privacy Information Center.

Google recently agreed to strict privacy rules and said it would ask users before sharing data with outsiders as part of a proposed settlement with the FTC, which had claimed it violated user's privacy on its social network, Google Buzz.

Write to Amir Efrati at amir.efrati@wsj.com and Dionne Searcey at dionne.searcey@wsj.com

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

Statement of
Mai Fernandez
Executive Director
National Center for Victims of Crime

United States Senate Committee on the Judiciary
Subcommittee on Privacy, Technology and the Law
Hearing on Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy
May 10, 2011

My name is Mai Fernandez, and I am the Executive Director of the National Center for Victims of Crime. The mission of the National Center is to forge a national commitment to help victims of crime rebuild their lives. Through collaboration with local, state, and federal partners, the National Center provides resources to victims of crime across the country; advocates for laws and public policies that secure rights, resources, and protections for crime victims; delivers training and technical assistance to victim service organizations, counselors, attorneys, criminal justice agencies, and allied professionals serving victims of crime; and fosters cutting-edge thinking about the impact of crime and the ways in which each of us can help victims of crime rebuild their lives. We appreciate the opportunity to submit testimony on the issue of mobile technologies and victim privacy concerns.

The Stalking Resource Center

The National Center for Victims of Crime is uniquely positioned to offer information relevant to today's hearing drawing from our extensive experience operating the Stalking Resource Center. The mission of the Stalking Resource Center (SRC) is to enhance the ability of professionals, organizations, and systems to effectively respond to stalking. The Stalking Resource Center envisions a future in which the criminal justice system and its many allied community partners will have the best tools to effectively collaborate and respond to stalking, improve victim safety and well-being, and hold offenders accountable. The Stalking Resource Center is the only national resource on stalking and the use of technology to stalk and has a thorough understanding of the privacy concerns related to mobile technologies and how these technologies are abused by criminals.

Since its establishment in 2000, the National Center's Stalking Resource Center has trained more than 40,000 law enforcement, victim assistance, and allied professionals from across the United States. Training is provided on local, state, and national levels and includes an emphasis on the use of technology to stalk. This includes hosting, in

partnership with the National Network to End Domestic Violence, national conferences entitled The Use of Technology in Intimate Partner Stalking. These interactive, hands-on conferences provide attendees with critical information on the different technologies employed by stalkers, as well as considerations for investigation, evidence collection, prosecution, and victim safety. The Stalking Resource Center has held nine of these national conferences to date.

The staff of the Stalking Resource Center are nationally recognized as experts on the use of technology to stalk. The director of the Stalking Resource Center, Michelle M. Garcia, has twenty years experience working with victims of stalking, sexual assault, and domestic violence, advocating for victims' rights, and providing training. In addition to her work focused on violence against women, Ms. Garcia spent three years as the executive director of the Computer Learning and Mentoring Center, a non-profit that provided low- and no-cost school and community based technology education. Ms. Garcia received her Master of Public Policy degree from the University of Chicago.

Rebecca Dreke, senior program associate, brings more than twelve years of experience in victim advocacy, training and education. Ms. Dreke has trained thousands of practitioners nationally on various topics, including stalking, sexual assault, domestic violence, and hate and bias-motivated violence. Prior to joining the National Center, Ms. Dreke had worked as a social worker, victim advocate and public school teacher. Rebecca holds a Master of Science of Social Work from the University of Texas at Austin.

Prior to joining the Stalking Resource Center, Jessamyn Tracy, program associate, was a professor of criminology and criminal justice, where she specialized in teaching about women and crime. In addition to her research on victimization and fear of crime, she has over 14 years of experience in working with the criminal justice system including as a rape crisis counselor, domestic violence advocate, community service officer, and has experience working with offenders. Ms. Tracy completed her graduate work at Florida State University.

The Stalking Resource Center maintains an active network of law enforcement, prosecutors, advocates, forensic experts, and researchers with demonstrated expertise related to the use of technology to stalk. Through ongoing communications with these professionals, the Stalking Resource Center ensures that the information disseminated relating to technology is current and accessible.

In addition to providing trainings, the Stalking Resource Center also disseminates information related to technology-based stalking through its continually updated Web site at www.ncvc.org/src. This popular online resource includes a page dedicated to providing information on the use of technology to stalk, as well as a compilation of federal, state, territory, and tribal stalking laws; stalking related articles; research, guides; public awareness and outreach materials; and highlights of stalking-related news stories from across the country. In 2010, the Stalking Resource Center Web site had more than 200,000 hits made by over 80,000 unique visitors.

Specific to the use of technology, the Stalking Resource Center is currently working on developing two new resources to enhance the ability of those responding to and working with stalking victims to recognize and respond to the use of technology to stalking. The first is a 15-minute training video on the use of technology to stalk. The video content includes: an overview of the most common forms of technology used by stalkers including cell phones, computers, and GPS; victim testimony; and commentary from law enforcement, prosecutors, victim service providers, and a victim of stalking. The video content is national in scope and the video will be packaged with an accompanying discussion guide with discussion topics such as local prevalence of stalking, team investigation, and victim involvement.

The second resource is an interactive online training module on the use of technology to stalk. Content will include interactive methodologies, case studies, exercises, and other suggested activities to enhance the user's learning. Training topics will include an overview of stalking, data on offenders and victims, information on a variety of technologies used by stalkers, and profession-specific considerations for those working with victims including law enforcement, prosecutors, and advocates.

To some degree, all resources developed and disseminated by the National Center's Stalking Resource Center address the use of technology to stalk. Most notably, in 2007, the National Center published *The Model Code Revisited: Responding to the New Realities of Stalking*. This important policy document was an update to the *Model Code* published by the National Institute of Justice in the mid-1990s and was specifically intended to address advances in technology, how stalkers are using such advances, and legislative responses to this new reality.

Benefits of Mobile Technology

Today's hearing focuses on mobile technologies and it is important to note that these technologies can both enhance personal safety and jeopardize privacy. Cell phones allow crime victims to call, text, and send photos and video to 911[1] when they are in immediate danger, take photographs or video to be used as evidence, and call police and other helping agencies in non-emergency situations. Enhanced 911 (E-911) uses cell phone GPS (Global Positioning System) technology to facilitate the location of callers. Internet capable mobile devices allow victims to search the web for helping agencies and resources, email the criminal justice system personnel they work with, and connect online with others for emotional support.

The use of mobile devices can also assist law enforcement efforts to investigate and gather evidence in many stalking cases. When offenders use their own mobile devices to place phone calls, send text messages, and access the internet, they create a digital evidence trail.

[1] In September 2008, New York city officials announced the capacity to send photos and video from computers and Web-enabled cell phones and PDAs to the city's 911 and non-emergency hot lines to report crimes. While many cities' emergency systems are equipped to accept text messages, this is believed to be the first system that also is able to process photos and video.

Mobile technologies have also been proven to thwart crime, locate victims, and hold offenders accountable as demonstrated by the following headlines:

- "Officials use GPS to locate accident victim" (*Freemont Tribune*; October 14, 2010)
- "Lodi police officers use GPS to track kidnap victim's cell phone" (*The Record*; September 23, 2008)
- "Picture Taken by Cellphone Leads to Sex-Crime Arrest" (*New York Times*; September 18, 2008)
- "Police use cell phone tracking technology to place suspect in area during slaying" (*Washington Examiner*; July 2, 2008)
- "Cell phone thwarts abduction at Multnomah Falls" (*The Gresham Outlook*; August 22, 2006)
- "Would-Be Kidnapper Busted Thanks to Camera Phone" (CBS Chicago; June 12, 2006)
- "Conn. woman uses cell phone camera to help in arrest of sexual predator suspect" (NBC Hartford, CT; September 22, 2004)
- "Police: Teen abduction foiled by cell phone cam" (CNN; August 2, 2003)

Mobile technology providers have in some cases made their technologies available to crime victims at no cost. For example, Verizon's HopeLine turns no-longer-used wireless phones into support for victims of domestic violence. Since HopeLine was launched in 2001, Verizon Wireless has distributed more than 106,000 phones with more than 319 million minutes of free wireless service to be used by victims of domestic violence.

Dangers of Mobile Technology

The very same technologies that offer many benefits may also be misused by stalkers and other criminals. Although stalking behavior remains essentially the same regardless of method used, the tools available to stalkers and abusers change with each new advance in technology. Where landline telephones once facilitated the victimization of women through obscene and harassing phone calls,[2] the advent of mobile and computing technologies has expanded the ways in which individuals may be victimized. Not only has the technology advanced, but the ways in which people use technology have fundamentally altered over the course of the last two decades. Mobile devices are just that: mobile. Individuals carry devices on their person, in their belongings, and store them next to their beds at night. The ubiquity of mobile technology, in combination with its powerful capabilities, combine to create a situation in which end users may be at significant risk of criminal victimization through their electronic devices.

As of late 2010, there were more than 223 million American mobile phone users ages 13 and older; nearly 61 million were also mobile web users.[3] A market research group

[2] Sheffield, C. (1993). The Invisible Intruder. In P. Bart, & E. Moran (Eds.), *Violence Against Women* (pp. 73-78). Sage Publications.
[3] http://blog.nielsen.com/nielsenwire/press/nielsen-fact-sheet-2010.pdf

reported in April 2011 that smartphones[4] now account for half or more of all new cell phone purchases.[5] At the same time, the Bureau of Justice Statistics Report, *Stalking Victimization in the United States,*[6] found in 2009 that stalking rates in the United States occur at an overall rate of 14 per 1,000 Americans, each year. In a one year period, that equated to 3.4 million stalking victims in the United States. The abuse of mobile technologies to track, monitor, and threaten victims is, therefore, no surprise as both victims and offenders adopt mobile technologies in ever-increasing numbers and fully integrate them into their daily activities.

Mobile technology facilitates a variety of criminal activities. Sixty-six percent of stalking victims report receiving unwanted calls and messages and 31 percent report unwanted letters and emails.[7] Even more troubling is that many victims also report covert electronic monitoring that involves the use of computer and cell phone spyware and GPS tracking. Given the insidious nature of electronic monitoring, not all victims realize that they are being tracked and stalked, making it impossible to determine just how many cases involve covert digital monitoring through mobile devices. Nevertheless, it is reasonable to assume that the actual number of cases is much higher than the incidents reported by victims.

Cellular Phones

While the variety of mobile technology available to consumers today is vast, the cell phone is undoubtedly the single most pervasive device made popular by the many technologies incorporated into a single device. Even the most basic cell phones feature GPS technology, the ability to place and receive calls and text messages, and electronic notes generated by the user.

Many mobile service subscribers are unaware that their basic cell phones include GPS technology, believing that only smartphones feature this technology. In 2001, the Federal Communications Commission (FCC) mandated that all cell phone manufacturers include GPS technology in every phone by 2005 under a program known as E-911.[8] Although subscribers' monthly bills include a line charge for E-911, many do not realize that this means that GPS technology is included in their phones. In fact, for many phone models, the GPS capability is not directly available to the end user and does not appear in the phone menus or operation instructions. Nevertheless, the presence of the GPS technology does pose a possible threat in that it can be accessed and exploited by someone other than the phone user.

---

[4] Defined by PC Magazine as a cellular telephone with built-in applications and Internet access. Smartphones provide digital voice service as well as text messaging, e-mail, Web browsing, still and video cameras, MP3 player, video viewing and often video calling. In addition to their built-in functions, smartphones can run myriad applications, turning the once single-minded cellphone into a mobile computer.
http://www.pcmag.com/encyclopedia_term/0,2542,t=Smartphone&i=51537,00.asp

[5] http://npd.com/lps/pdf/CTIA_Fact_Sheet_V4.pdf

[6] Katrina Baum, et al., *Stalking Victimization in the United States,* (Washington, DC: Bureau of Justice Statistics, 2009).

[7] Ibid.

[8] For more information, see http://www.fcc.gov/pshs/services/911-services/enhanced911/

Victim cell phone location data may be obtained by stalkers in at least four ways:

1. Family location service offered by the carrier activated on the victim's cell phone.
2. Third party applications installed by the user, such as FourSquare, Latitude, or Facebook, that provide opt-in location tracking services on smart phones and other mobile devices.
3. Covert third party applications installed by the offender, such as MobiSpy, which secretly record and report the victim's location.
4. Potential misuse of unencrypted location logs generated by the phone/carrier that are housed on the phone and accessed either by the offender or a malicious software application installed by the offender.

All of the major wireless carriers offer location plans that are marketed as a tool for families to keep track of their loved ones who participate on the same phone service plan. Sprint, T-Mobile, and Verizon offer plans called Family Locator; AT&T's plan is called Family Map. Enrollment in these plans, for a fee, allows an authorized user on the account to track—in real time—the location of the other phones that share the plan. Each cell phone user on the plan may not be aware that the tracking program has been enabled, as carriers vary in their notification practices. While some users may receive repeated text messages notifying the user that the phone is being tracked, others may receive a single message confirming enrollment. Given that in cases of stalking by a current or former intimate partner, the stalker and the victim are on the same calling plan, the stalker often has physical access to the phone and can delete the notification text message. Victims can be tracked, in real time, every moment of the day.

Geo-social networking applications like FourSquare and BrightKite are marketed to allow individuals to "meet people around you, keep up with your friends, explore and discover new places." In the hands of someone who is tracking you with malicious intent, these sites provide a wealth of information.

Third party applications like MobiSpy allow an offender to track a victim without their knowledge. More sophisticated cell phone spyware programs (e.g., FlexiSpy, MobiStealth, CellSnoop) not only provide tracking capability, but the capacity for someone to monitor all your calls, text messages, and operate the phone as a listening device.[9] With cell phone spyware, an offender has complete access to a victim's phone without their knowledge. More challenging, it is often difficult to prove that spyware has been installed on a cell phone as there is no simple way to detect it.

The existence of location logs generated by the phone or carrier is clearly a privacy concern. How secure, or unsecure, this information is poses a very real concern for victims of stalking and domestic violence whose offenders are invested in tracking their victims' movements. If the offender has access to the victim's phone, how easily could they acquire this information?

In addition to the methods described above, cell phones may be used to track victims in one other way. The offender can hide a GPS-equipped cell phone in the victim's vehicle

[9] For more information on this technology, see www.squidoo.com/cell-phone-spy.

to track their movements. This happened to a Sherri Peak, a victim from Kirkland, Washington, who was stalked by her now ex-husband. At one point, the risk to Sherri and her children was determined to be so great that they were taken into police protective custody. Through diligent police work, and most importantly, a detective who believed Sherri when she reported that she was being tracked by her husband, investigators found a cell phone that had been hidden behind the dashboard and wired to the car's electrical source to remain always powered. The hidden phone was enrolled in a family location service provided by the mobile carrier allowing Sherri's husband to track her anywhere she went. The phone was also set to auto-answer and silent ring allowing the offender to call in and listen to conversations Sherri had while in the car. In essence, the cell phone functioned as both a tracking and listening device.[10]

Smartphones introduce additional safety concerns that are greater by an order of magnitude. The smartphone is far more than a phone: it is a compact mobile computing device that incorporates wireless phone technology, wireless Internet capabilities, and GPS technology. A smartphone that is always on is always connected to the network and therefore always generating data about its current location. This type of cell phone generates location data that is specific to both place and time; it generates a record of even small movements of the cell phone user throughout the day. For those who stalk, abuse, and commit other crimes that take advantage of time and location information, the cell phone is the most powerful tool available.

Other Mobile Devices

New mobile devices, such as netbooks, tablets, e-readers, or sophisticated MP3 players like the iPod Touch are becoming more difficult to distinguish from smartphones as the technological capabilities of mobile devices become more and more similar. There are only three meaningful distinctions between smart phones and other mobile devices: (1) the size and portability of the device, (2) the intended primary purpose, and (3) whether or not the device connects to the Internet through a cellular wireless network connection or a computer based wireless network. Any connection to the Internet will generate a record, which, with enough other data, can be connected back to a location.

Furthermore, mobile devices are often connected with less mobile devices like home and work desktop computer systems. Mobile devices, then, are sharing data across platforms and devices using both wireless and wired connections. Each transfer of information presents a potential vulnerability, an opportunity for criminal offenders to look at, steal, or even manipulate data in the course of their stalking behavior.

Protecting Victims

The protection of victims' information—including their location, travel history, and online browsing history—is paramount to preventing future harm against them by stalking and abusive partners. Victims, like any users of smartphones, tablets and other mobile

[10] For more information on Sherri Peak's case, see http://www.msnbc.msn.com/id/19253352/ns/dateline_nbc-crime_reports/

devices, want to use and benefit from these sophisticated technologies. Victims of intimate partner violence and stalking, however, need to be assured that their data is private and especially not discoverable by their offender. We believe that all victims of crime, and in fact any user of these technologies and services, deserve notice about what data is collected, where that data is stored, and, most importantly, the right and ability to opt-out of probing and location tracking features.[11]

User Notification and Consent

We believe mobile technology providers should assist in keeping victims safe by providing explicit, comprehensive and meaningful notification on how these technologies and services obtain, store and/or share user data and information. Victims should be provided all the information possible in order to make a truly informed decision on whether they want to use these technologies and fully understand any potential ramifications of doing so. Furthermore, we recommend all providers obtain consent from any user of these services and all users should be provided an opportunity to opt-out or revoke their consent to have their data shared or disclosed at any time. The burden of obtaining this consent should be on providers who must be able to demonstrate to users how they will continue to obtain this consent.

Mobile technology companies that utilize location-based service technologies would do well to adopt and adhere to the guidelines set out by CTIA – The Wireless Association in their *Best Practices and Guidelines for Location Based Services*. These guidelines stress the critical need for user notification and consent for any location-based service on all mobile devices. [*See Attachment A.*] We strongly recommend all companies adapt these guidelines in their own policies and pledge to follow them consistently and transparently.

Awareness Campaign(s) by Cell Phone Manufactures/Carriers

We believe mobile technology companies could further assist victims by conducting their own awareness campaigns on how these technologies could potentially be harmful to users and providing information on how users can better protect themselves from future risks. These companies could provide even simple tips on a Web site that discusses user safety. For example, the social networking site MySpace has one such page on their Web site entitled "My Space Safety."[12]

Along with user notification and consent, online pages could provide victims with important information about how their devices work, how someone might use the technology in a nefarious manner, what types of information is collected by the device, what steps a victim could take if s/he believes that someone is using the technology against them, and how victims can report abuse. The template for these safety steps

---

[11] *Probing*: when a user's device periodically checks the location of the user without the user activating or initiating the location checking. *Location tracking*: when a user's device provides history of all the places you have been and used your device. Location tracking is often used against victims in protection order and divorce cases and is easily used to stalk a victim.

[12] See http://www.myspace.com/help/safety

could be much like those that credit card companies are required to provide consumers on identity theft and fraud.

Timely and Enhanced Responsiveness to Law Enforcement

We believe all mobile technology companies could better assist victims by providing an easily-accessible and dedicated unit or division of their company that can respond to law enforcement requests for information and data in a timely manner. Frequently, investigators and attorneys need to be able to document an abuse of the technologies by a stalker or perpetrator in order to increase a victim's safety through orders of protection or for bond/bail conditions. Many criminal justice professionals express their concern at how slow and laborious the process of obtaining this information from the technology companies can be. This can be demonstrated in the case of Maija Zummo, a young woman in Cincinnati, Ohio, who was stalked, held at gun point, and had her car shot at by her stalker. As investigators worked her case, trying first to identify and then locate her stalker, Maija learned that the digital evidence trail left behind by stalkers utilizing mobile devices can be difficult to discern, even for experienced investigators. Maija's stalker, Richard Ewan, was tech savvy, mentally ill, and determined to harm Maija. He was also highly mobile, and sophisticated enough to take steps to cover his digital tracks and mislead investigators by using anonymizers[13] to reroute his Internet communications. He stalked Maija by using mobile devices at public wireless hotspots at McDonald's, Starbucks, and Panera Bread in an effort to hide his true identity.

Police sent multiple information requests, subpoenas, and warrants to a variety of companies. They contacted AT&T, Qwest Communications, Google, Facebook, Yahoo, Twitter, and others. Some companies responded immediately, others were slow and nonresponsive. As the elusive stalker's violence escalated, investigators became increasingly frustrated at their inability to receive mobile device evidence from service providers. Upset by repeated unanswered exigent requests, one investigator said in exasperation, "I thought about sending [the service provider] an email stating: 'Everyone is dead now so there is no need to expedite anything.'" [See Attachment B for more detailed information on Maija Zummo's case]

If companies were to provide a streamlined process of obtaining this information and providing it to law enforcement, victims of stalking, intimate partner violence, and other crimes would benefit greatly.

Conclusion

We recognize that issues raised by mobile technology will evolve as the technology evolves and that this hearing is part of a continuing conversation. We appreciate this committee's concern for the interests of stalking victims. While mobile technology provides both risks and benefits for victims, we hope this hearing will promote efforts to limit the risks and increase the benefits. Thank you for the opportunity to testify as part of this hearing.

---

[13] Anonymizers are services that reroute computer connections in order to mask the origin of a person's online presence.

ATTACHEMENT A

CTIA Guidelines

CTIA
The Wireless Association®

Best Practices and Guidelines for Location-Based Services

Version 2.0

Effective Date: March 23, 2010

CTIA's Best Practices and Guidelines for Location Based Services

TABLE OF CONTENTS

Section 1 - Purpose 1
Section 2 – Applicability 1
Section 3 – Scope of Coverage 2
Section 4 - Specific Guidelines 3
A. Notice 3
B. Consent 5
1. Form of Consent 5
2. Account Holder Consent 5
3. Revocation of Consent 6
C. Safeguards 7
1. Security of Location Information 7
2. Retention and Storage of Location Information 7
3. Reporting Abuse 7
4. Compliance with Laws 7
5. Education 7
6. Innovation 8
7. Compliance with Guidelines 8
Appendix – Additional References: 8

** The examples provided in the Guidelines are illustrative only and are not meant to indicate that LBS Providers must provide the features or services described in the examples.*

CTIA
The Wireless Association®

Section 1 - Purpose

CTIA Best Practices and Guidelines ("Guidelines") are intended to promote and protect user privacy as new and exciting Location-Based Services ("LBS") are developed and deployed. Location Based Services have one thing in common regardless of the underlying technology – they rely on, use or incorporate the location of a device to provide or enhance a service. Accordingly, the Guidelines are technology-neutral and apply regardless of the technology or mobile device used or the business model employed to provide LBS (e.g., a downloaded application, a web-based service, etc.).

The Guidelines primarily focus on the user whose location information is used or disclosed. It is the user whose privacy is most at risk if location information is misused or disclosed without authorization or knowledge. Because there are many potential participants who play some role in delivery of LBS to users (e.g., an application creator/provider, an aggregator of location information, a carrier providing network location information, etc.), the Guidelines adopt a user perspective to clearly identify which entity in the LBS value chain is obligated to comply with the Guidelines. Throughout the Guidelines, that entity is referred to as the LBS Provider.

The Guidelines rely on two fundamental principles: user notice and consent.

- First, LBS Providers must ensure that users receive meaningful notice about how location information will be used, disclosed and protected so that users can make informed decisions whether or not to use the LBS and thus will have control over their location information.

- Second, LBS Providers must ensure that users consent to the use or disclosure of location information, and LBS Providers bear the burden of demonstrating such consent. Users must have the right to revoke consent or terminate the LBS at any time.

Users should have confidence when obtaining an LBS from those LBS Providers that have adopted the Guidelines that their location information will be protected and used or disclosed only as described in LBS Provider notices. By receiving notice and providing consent consistent with these Guidelines, users will maintain control over their location information. The Guidelines encourage LBS Providers to develop and deploy new technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the device or technology used or business model employed.

Section 2 – Applicability

The Guidelines apply to LBS Providers. The following examples identify common situations and illustrate who is and is not an LBS Provider with obligations under the Guidelines.

CTIA
The Wireless Association®

Examples of LBS Providers:

Example 1. *A wireless carrier is the LBS Provider when it directly provides account holders or users an enhanced 411 LBS to locate nearby businesses.*

Example 2. *An application developer that provides the service for a downloadable LBS application (e.g., turn-by-turn driving) that is offered through an application storefront is the LBS Provider; a wireless carrier that provides user location information to that application developer for use in the LBS (e.g., through incidental assistance to the device's A-GPS or through other network data) is not an LBS Provider.*

Example 3. *A device manufacturer that pre-loads its own manufacturer-branded LBS application (e.g., a proprietary social networking application) is the LBS Provider; a device manufacturer that merely includes location enabled technology (e.g., A-GPS) on the device to support other applications and services, is not an LBS Provider.*

Example 4. *An entity that merely enables application providers to access location information from multiple wireless carriers (i.e., an aggregator) is not an LBS Provider, nor are the wireless carriers LBS Providers; instead, a party that uses an aggregator's data to make an LBS available to users is the LBS Provider.*

Example 5. *A wireless carrier that provides its customers "on-deck" access to a mapping service provided by a separate software developer is not the LBS Provider even if it provides the location information used by the third party; instead, the software developer is the LBS Provider.*

Caveat: The examples are illustrative only and do not imply that compliance with the Guidelines alone permits such uses or services. The terms on which access to location information is made available from wireless carriers to third parties, or the terms under which applications are made available to users, are beyond the scope of the Guidelines.

Section 3 – Scope of Coverage

The Guidelines apply whenever location information is linked by the LBS Provider to a specific device (e.g., linked by phone number, userID) or a specific person (e.g., linked by name or other unique identifier).

The Guidelines do not apply to location information used or disclosed:

- as authorized or required by applicable law (e.g., to respond to emergencies, E911, or legal process);
- to protect the rights and property of LBS Providers, users or other providers of location information;
- for testing or maintenance in the normal operation of any network or LBS; or
- in the form of aggregate or anonymous data.

Section 4 - Specific Guidelines

A. Notice

An important element of the Guidelines is *notice*. LBS Providers must ensure that potential users are informed about how their location information will be used, disclosed and protected so that they can make informed decisions whether or not to use the LBS, giving the user ultimate control over their location information.

The Guidelines do not dictate the form, placement, terminology used or manner of delivery of notices. LBS Providers may use written, electronic or oral notice so long as users have an opportunity to be fully informed of LBS Providers' information practices. Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous.

If, after having obtained consent, LBS Providers want to use location information for a new or materially different purpose not disclosed in the original notice, they must provide users with further notice and obtain consent to the new or other use.

LBS Providers must inform users how long any location information will be retained, if at all. If it is not practicable to provide an exact retention period, because, for example, the retention period depends on particular circumstances, the LBS Provider may explain that to users when disclosing its retention policies.

LBS Providers that use location information to create aggregate or anonymous data by removing or permanently obscuring information that identifies a specific device or user must nevertheless provide notice of the use.

Example 6. *An LBS Provider could create a dataset of mobile Internet users registered in a particular geographic or coverage area by removing or "hashing" information that identifies individual users from the dataset so that the LBS Provider could provide location-sensitive traffic management information or content to a highway safety organization. Notice that the LBS Provider creates or uses aggregate or anonymous data is required.*

LBS Providers that share location information with third parties must disclose what information will be provided and to what types of third parties so that users can understand what risks may be associated with such disclosures.

LBS Providers must inform users how they may terminate the LBS, and the implications of doing so. LBS Providers also must ensure that any privacy options or controls available to users to restrict use or disclosure of location information by or to others are explained to users.

Example 7. *An LBS Provider that offers a social networking service might provide a mechanism for the user to establish permissions for when, where and to whom his or her location information will be disclosed. The notice to the user could include a statement to the effect:*

"You control who will receive your location information. In 'settings' on the menu, you can select contacts you wish to block or enable all the time, or you can select a manual option to review a list of contacts each time you disclose your location."

LBS Providers must periodically remind users when their location information may be shared with others and of the users' location privacy options, if any. The form, placement, terminology used, manner of delivery, timing and frequency of such notice depends on the nature of the LBS. For example, one would expect more reminders when the service involves frequent sharing of location information with third parties and fewer reminders, if any, when the service involves one-time, user-initiated concierge service calls (e.g., locating a nearby service). In addition, depending on the circumstances, the use of an icon or other symbol to disclose when location information may be shared may be a more effective means of reminding consumers than a written notice.

In some circumstances, account holders (as opposed to users) may control the installation and operation of LBS. In addition to providing notice to the account holder, LBS Providers still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others. Once again, the content, timing and frequency of such notice depends on the nature of the LBS.

Example 8. *An LBS Provider provides an LBS to a business customer with multiple devices used by employees in the field. The LBS Provider could satisfy its notice obligation by direct notice to each device that location information is being provided to the business customer. Alternatively, pursuant to a contractual obligation between the LBS Provider and the business customer to do so, the business customer could inform its employees that it will receive user location information.*

CTIA
The Wireless Association®

B. Consent

1. Form of Consent

LBS Providers must obtain user consent to the use or disclosure of location information before initiating an LBS (except in the circumstances described below where consent is obtained from account holders and users are informed of such use or disclosure). The form of consent may vary with the type of service or other circumstances, but LBS Providers bear the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating an LBS.

The Guidelines do not dictate the form, placement, terminology used, or manner of obtaining consent as long as the consent is informed and based on notice consistent with the requirements set forth in the Notice section above. Consent may be implicit, such as when users request a service that obviously relies on the location of their device. Notice may be contained in the terms and conditions of service for an LBS to which users subscribe. Users may manifest consent to those terms and conditions electronically by clicking "I accept"; verbally by authorizing the disclosure to a customer service representative; through an IVR system or any other system reasonably calculated to confirm consent. Pre-checked boxes that automatically opt users in to location information disclosure, or, choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent.

2. Account Holder Consent

In some cases, where the actual user is different than the account holder, an account holder may control the installation and operation of LBS (e.g., business account holder utilizing LBS for fleet management; parental account holder providing phones for childrens' use). Under these circumstances, the appropriate consent may be obtained solely from the account holder. As noted above, however, LBS Providers still must ensure that notice is provided to each user or device that location information is being used by or disclosed to the account holder or others.

The following examples are illustrative of account holder consent upon which the LBS Provider may rely to use or disclose users' location:

Example 9. *Fleet Tracking/Employee Monitoring: A business entity purchases multiple lines to permit tracking employee locations to provide for rapid response repair service, just-in-time delivery, or fleet management.*

Example 10. *Public Safety: The LBS Provider enters into an agreement with a public safety organization to provide monitoring compliance with terms of supervised release and house arrest, terms of bail for bondsmen, protecting public officials on duty, or military force movements.*

CTIA
The Wireless Association®

Example 11. *Parental Controls. The LBS Provider offers a service to notify parents when a child arrives at or leaves a designated place.*

Example 12. *Family Safety. The LBS Provider offers a family safety feature to locate family members in an emergency or other specified circumstances.*

3. Revocation of Consent

LBS Providers must allow users to revoke their prior consent to use or disclose location information to all or specified groups or persons.

Example 13. *User signs up with an LBS Provider for a service that provides updates regarding user's location to a group of "friends" designated by the user. The LBS Provider must provide reasonable mechanisms for the user to discontinue such location sharing with the group at a later date.*

Where technically feasible, LBS Providers may provide for selective termination or restriction of an LBS upon account holder request. An account holder may revoke or terminate all or a portion of any users' consent to an LBS.

Example 14. *User signs up with an LBS Provider for a service that requires user's wireless carrier to periodically disclose user's location information to LBS Provider. User is a minor and the mobile device is one of several on the account of the wireless carrier's account holder who, through controls provided by the LBS Provider or upon request to the LBS Provider, decides to block the LBS or disclosure of user's location information to third parties. The account holder's election with the LBS Provider revokes the user's consent.*

Similarly, revocation of consent also occurs when certain controls for sharing location information are provided by a wireless carrier, and the account holder of the wireless carrier has decided to block disclosure of a user's location information to third parties for a line on the account holder's account.

The Guidelines do not dictate terms of service that LBS Providers must offer to users with regard to an LBS. Nor do the Guidelines dictate any technical implementation for terminating or restricting an LBS.

CTIA
The Wireless Association®

C. Safeguards

1. Security of Location Information

LBS Providers must employ reasonable administrative, physical and/or technical safeguards to protect a user's location information from unauthorized access, alteration, destruction, use or disclosure. LBS Providers should use contractual measures when appropriate to protect the security, integrity and privacy of user location information.

2. Retention and Storage of Location Information

LBS Providers should retain user location information only as long as business needs require, and then must destroy or render unreadable such information on disposal. If it is necessary to retain location information for long-term use, where feasible, LBS Providers should convert location information to aggregate or anonymized data.

3. Reporting Abuse

LBS Providers should provide a resource for users to report abuse and provide a process that can address that abuse in a timely manner.

4. Compliance with Laws

LBS Providers must comply with applicable laws regarding the use and disclosure of location information, and in particular, laws regarding the protection of minors. In addition, it is recommended that LBS Providers comply with applicable industry best practices and model codes.

5. Education

In addition to any notices required under the Guidelines, LBS Providers certifying under the Guidelines will work with CTIA in an education campaign to inform users regarding the responsible use of LBS and the privacy and other risks associated with the disclosure of location information to unauthorized or unknown third parties. All entities involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available.

CTIA
The Wireless Association®

6. Innovation

LBS Providers develop and deploy technology to empower users to exercise control over their location information and to find ways to deliver effective notice and obtain consent regardless of the device or technology used or business model employed.

7. Compliance with Guidelines

LBS Providers that comply with the Guidelines may self-certify such compliance by placing the following statement in their marketing or promotional materials:

LBS Provider follows CTIA's Best Practices and Guidelines for Location-Based Services.

Appendix – Additional References

CTIA has collected a variety of Location Based Services Privacy Policies that demonstrate the application of these Best Practices. These policies are availablc at:

http://www.ctia.org/business_resources/wic/index.cfm/AID/11924

ATTACHMENT B

Maija Zummo's Stalking Case

Maija first met Richard at the University of Wisconsin when her roommate began dating his roommate in the fall of 2002. They all lived in the same dorm, although they were several floors apart. She barely knew him, but noted that he was always at his computer. While she was still at Wisconsin, she and Richard talked a few times, and instant-messaged once or twice, but never dated or had any other relationship. In fact, she didn't even know his last name. Maija left UW after a single semester, she never really thought of him again.

About seven years later, odd things started happening. Someone stole her grill from her patio, then someone started tagging her photo on Facebook with the name "Gollum." She made her page private and the tagging stopped. Then her front door was splattered with a gallon of red paint. Next, her car was spray painted with orange paint as it sat in a parking lot downtown. In September, 2009, her car was shot with a .45. In October, it was shot with the same gun, but this time the shooter left a threatening note. The note was unsigned, but referred to her as "Gollum." The pattern of escalating violence was now undeniable.

In November, 2009 as she was walking back to her workplace with her co-worker, Richard held both of them at gunpoint in the foyer of her building. She didn't recognize him: His hoodie was pulled down, he had some sparse facial hair, and in the seven years that had lapsed since she last saw him, he didn't look like the quiet, shy boy who sat at his computer in his dorm room. He wasn't anyone she knew.

As Richard's stalking behavior continued and escalated, he was also generating digital evidence as he emailed Maija and the people in her life. Each email, each Facebook post could theoretically be traced back to an IP address that would show the location of the device user and perhaps determine the user's real identity. Because Maija had not recognized Richard, she and investigators were operating under the assumption that the stalker was a stranger. They did not know his real name, much less his address. Identifying the stalker became of paramount importance.

Richard was mobile and technologically savvy. He also had money. Although he was an Illinois resident, he obtained driver licenses in Ohio and Florida that he used to purchase firearms. Richard traveled through Utah, Colorado, Kentucky, Illinois and Canada, using mobile hotspots at popular businesses to connect his mobile devices to the internet. Richard knew about anonymizers, and even routed his connections through Europe. Investigators had to search for evidence from several companies including Google, Facebook, Yahoo, AT&T, Qwest Communications, Twitter, and others.

IP addresses, usernames, and the physical location of the internet connections were not easy to identify with any great certainty. Evidence provided by online service providers

was sometimes provided immediately in response to exigent requests, while other companies had to be contacted repeatedly before they responded to the search warrants and subpoenas. Investigators wanted to set up pen registers[1] to trap as much information as possible, but found it difficult to do so.

Furthermore, investigators were never sure what kind of device the stalker was using to connect to the internet. However, they were positive it was a mobile device given the stalker's frequent travel and strict usage of public wireless hotspots. He could have been using a phone, a laptop, a netbook, or even an iPod Touch. Their inability to determine which device he was using points to the fact that mobile devices, while designed and marketed for specific uses, very much share the same technologies and are increasingly difficult to distinguish from one another.

In the fall of 2010, Richard wrote to a friend of Maija's after he had held them at gunpoint and demanded Maija's housekeys. Richard wrote:

> "Its thanksgiving next week so im going to call a truce and you should probably use the truce time to buy some guns and learn to shoot them because im not going to mess up again. Gollums house is going to get burnt to the ground. I have never carried out a broad day light stick up before and I assumed you would be reasonable and give me what I asked for. I was just as nervous (non-chalant) as you guys and maybe i flubbed my lines a bit and you didn't hear me clearly which led to the confusion of Gollum running up the stairs and you giving me your housekeys and not hers. So, in summation tell Gollum that she is totally fucked and that my new plan to burn her house down is fool proof. p.s. – stop cooperating with the police you snitch."

By the spring of 2010, Richard had shot Maija's car, and also shot at one of Maija's colleagues. His death threats were escalating, and Maija and her family believed that Maija was in imminent danger. Investigators reassured Maija's family on April 1st, 2010 that Maija was in no danger at the moment. They believed that Richard was in Austin, Texas based on IP evidence that they had obtained from the records left by Richard's mobile devices that he used to send threatening messages. Maija's family did not feel safe, and believed that Richard was in fact much closer. They were right.

The next day, at 10:16AM, AT&T responded to a subpoena request by fax. Using AT&T's information and other sources, investigators quickly realized that Richard Ewan was not in Texas. He was about six miles away from Maija's residence. At 11:37AM, investigators used the GPS in Richard's cell phone to locate Richard. He was followed

---

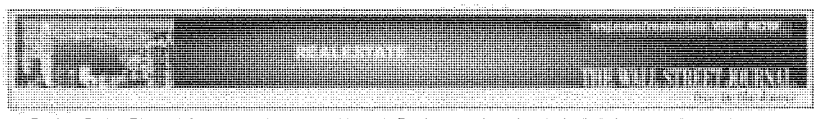
[1] A pen register is a device or service that logs all of the activity on a phone line or on an internet site, computer, or other similar technology.

on his way to Maija's home, and arrested by 2:00PM with a gun and other items that suggested he was on his way to follow through on his threats to kill Maija.

Richard claims he wanted Maija to suffer for being so popular, so cool, so hip. He wanted her to know how it felt to have none of those traits. Ironically, Maija never felt the way Richard envisioned her. She felt lonely and uncertain, and was striving to find her way in the world.

It's a mystery why he became obsessed with her so many years later. When they were both at UW he never asked her out. Therefore, she never rejected him. Yet somehow she made it onto his enemies list, his list of people he was going to get even with for being mean to him. She was first on his list, but he was planning to move on to the others. He never did. After his arrest, when the detective asked him why he terrorized Maija the way he did, he answered simply, "She rubbed me the wrong way."

Maija survived; Richard was tried and found not guilty by reason of insanity. Today, however, Maija is haunted by that 10:16AM fax. What if AT&T had responded a few hours later?



Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

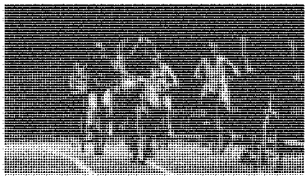
WHAT THEY KNOW | NOVEMBER 19, 2010

Insurers Test Data Profiles to Identify Risky Clients

By LESLIE SCISM And MARK MAREMONT

Life insurers are testing an intensely personal new use for the vast dossiers of data being amassed about Americans: predicting people's longevity.

Insurers have long used blood and urine tests to assess people's health—a costly process. Today, however, data-gathering companies have such extensive files on most U.S. consumers—online shopping details, catalog purchases, magazine subscriptions, leisure activities and information from social-networking sites—that some insurers are exploring whether data can reveal nearly as much about a person as a lab analysis of their bodily fluids.



Life insurers are testing new ways to predict life expectancy and they're mining personal information online and offline to do it. WSJ's Kelsey Hubbard talks to reporter Leslie Scism about the brave new world of online actuarial research.

What They Know Videos

What They Know: Websites Move to Curb Cookies

What They Know: Stalkers Turn to GPS

How Advertisers Use Internet Cookies to Track You

Related

Inside Deloitte's Life-Insurance Assessment Technology

Complete Coverage: What They Know

In one of the biggest tests, the U.S. arm of British insurer Aviva PLC looked at 60,000 recent insurance applicants. It found that a new, "predictive modeling" system, based partly on consumer-marketing data, was "persuasive" in its ability to mimic traditional techniques.

The research heralds a remarkable expansion of the use of consumer-marketing data, which is traditionally used for advertising purposes.

This data increasingly is gathered online, often with consumers only vaguely aware that separate bits of information about them are being collected and collated in ways that can be surprisingly revealing. The growing trade in personal information is the subject of a Wall Street Journal investigation into online privacy.

A key part of the Aviva test, run by Deloitte Consulting LLP, was estimating a person's risk for illnesses such as high blood pressure and depression. Deloitte's models assume that many diseases relate to lifestyle factors such as exercise habits and fast-food diets.

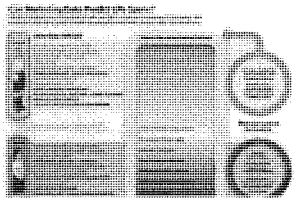
This kind of analysis, proponents argue, could lower insurance costs and eliminate an off-putting aspect of the insurance sale for some people.

"Requiring every customer to provide additional, and often unnecessary, information" such as blood or urine samples, "simply makes the process less efficient and less customer-friendly," says John Currier, chief actuary for Aviva USA.

Journal Community

Vote: Should data-mining be used by insurance companies to predict longevity?

Other insurers exploring similar technology include American International Group Inc. and Prudential Financial Inc., executives for those firms confirm. Deloitte, a big backer of the concept, has pitched it in recent months to numerous insurers.



The industry is grappling with how to get policies into the hands of middle-class families more cost-effectively. Sales of life policies to individuals are down 45% since the mid-1980s. Deloitte says insurers could save $125 per applicant by eliminating many conventional medical requirements. Under Deloitte's predictive model, the cost to achieve similar results would be $5, Deloitte says. The total underwriting costs for a policy range from $250 to $1,000, insurers say.

Making the approach feasible is a trove of new information being assembled by giant data-collection firms. These companies sort details of online and offline purchases to help categorize people as runners or hikers, dieters or couch potatoes.

They scoop up public records such as hunting permits, boat registrations and property transfers. They run surveys designed to coax people to describe their lifestyles and health conditions.

Increasingly, some gather online information, including from social-networking sites. Acxiom Corp., one of the biggest data firms, says it acquires a limited amount of "public" information from social-networking sites, helping "our clients to identify active social-media users, their favorite networks, how socially active they are versus the norm, and on what kind of fan pages they participate."

For insurers and data-sellers alike, the new techniques could open up a regulatory can of worms. The information sold by marketing-database firms is lightly regulated. But using it in the life-insurance application process would "raise questions" about whether the data would be subject to the federal Fair Credit Reporting Act, says Rebecca Kuehn of the Federal Trade Commission's division of privacy and identity protection. The law's provisions kick in when "adverse action" is taken against a person, such as a decision to deny insurance or increase rates.

The law requires that people be notified of any adverse action and be allowed to dispute the accuracy or completeness of data, according to the FTC.

Deloitte and the life insurers stress the databases wouldn't be used to make final decisions about applicants. Rather, the process would simply speed up applications from people who look like good risks. Other people would go through the traditional assessment process.

The use of the data also may require passing muster with insurance regulators. Regulators in Connecticut, New Jersey and New York, all home to major U.S. life insurers, say they haven't been briefed.

They say their concerns would include ensuring that the approach doesn't unfairly discriminate. "An insurer could contend that a subscription to 'Hang Gliding Monthly' is predictive of highly dangerous behavior, but I'm not buying that theory: The consumer may be getting the magazine for the pictures," says Thomas Considine, New Jersey's commissioner of banking and insurance.

AIG is in the early stages of analysis "to figure out what is meaningful and what is not" in the data, says Bob Beuerlein, chief actuary for its SunAmerica Financial unit. The tests are being conducted by an in-house "think tank" whose mission, he says, is "to see where we're going in the future."

A Prudential spokesman says the insurer "is looking at" the potential of marketing data, declining to discuss details.

Some insurers are taking a wait-and-see approach. Deloitte's "methodology is sound," says Mike Belko, chief underwriter at USAA Life Insurance Co., but for now, "it's too soon to say how much reliance we would put on the information."

The largest marketiug-database companies in the U.S. include Acxiom, Alliance Data Systems Corp., Experian PLC, and Infogroup. Each says it has detailed information on more than 100 million U.S. households, though contents of their databases vary as do their rules related to data use.

There are myriad sources of personal data. Acxiom recently told investors it takes in three billion pieces of information daily as businesses seek to "monetize" information about their customers. Some retailers share information about purchases made by people, including item description, price and the person's name.

Increasingly, information comes from people's online behavior. Acxiom says it buys data from online publishers about what kinds of articles a subscriber reads—financial or sports, for example—and can find out if somebody's a gourmet-food lover from their online purchases. Online marketers often tap data sources like these to target ads at Web users.

"Personally identifiable data from the online world is merged with personally identifiable information from the offline world, every day," says Jennifer Barrett, Acxiom's head of global privacy and public policy. She also says that, while Acxiom does store personally identifiable information, it doesn't store or merge anonymous online-tracking data, such as Web-browsing records.

Acxiom says it wouldn't let insurers use its data to help assess applicants, for fear of triggering the stiffer federal credit-reporting regulations. Infogroup says it isn't supplying information to insurers for this use. Experian said its marketing data may only be used for marketing purposes.

More From the Series

A Web Pioneer Profiles Users by Name
Web's New Goldmine: Your Secrets
Personal Details Exposed Via Biggest Sites
Microsoft Quashed Bid to Boost Web Privacy
On Cutting Edge, Anonymity in Name Only
Stalking by Cellphone
Google Agonizes Over Privacy
On the Web, Children Face Intensive Tracking
'Scrapers' Dig Deep for Data on Web
Facebook in Privacy Breach
The Tracking Ecosystem
Follow **@whattheyknow** on Twitter
Complete Coverage: What They Know

Units of News Corp., including The Wall Street Journal, supply information to marketing-database firms and buy information from them. "We have strict precautions around confidentiality," a spokeswoman said.

This isn't the first use of database mining in insurance. About 20 years ago, data pros found that some factors in people's credit histories have a strong correlation to claims on car and home-insurance policies.

In other words: The better your credit, the less likely you'll file a claim. Today, most car and home insurers use this phenomenon to price their policies. For this purpose, property-casualty insurers look at people's credit reports, as opposed to the consumer-marketing databases.

Life insurers haven't changed their general underwriting approach for decades, relying heavily on medical screening.

Deloitte's effort to promote predictive modeling to life insurers gained steam in recent months, boosted partly by the Aviva research. Deloitte detailed the test in May at a seminar hosted by the Society of Actuaries, a professional group.

At the seminar, a consultant helped explain Deloitte's concept by discussing imaginary 40-year-old insurance buyers, "Beth" and "Sarah."

Using readily available data, the cousultant said, an insurer could learn that Beth commutes some 45 miles to

work, frequently buys fast food, walks for exercise, watches a lot of television, buys weight-loss equipment and has "foreclosure/bankruptcy indicators," according to slides used in the presentation.

"Sarah," on the other hand, commutes just a mile to work, runs, bikes, plays tennis and does aerobics. She eats healthy food, watches little TV and travels abroad. She is an "urban single" with a premium bank card and "good financial indicators."

Deloitte's approach, the consultant said, indicates Sarah appears to fall into a healthier risk category. Beth seems to be a candidate for a group with worse-than-average predicted mortality. The top five reasons: "Long commute. Poor financial indicators. Purchases tied to obesity indicators. Lack of exercise. High television consumption indicators."

Data From 'What They Know'

The Wall Street Journal analyzed the tracking files installed on people's computers by the 50 most popular websites, plus WSJ.com. Explore the data **here** and see **separate analysis** of the files on popular children's sites.

Another consultant detailed tbe Aviva test to the seminar attendees. Deloitte didn't identify the insurer; Aviva confirmed its role to the Journal.

The consumer-marketing data for the test came from Equifax Inc.'s marketing-services unit, since bonght by Alliance Data Systems. An Alliance spokeswoman says the company was unaware of the insurance-related test, which was done before it bought the former Equifax subsidiary. Alliance "does not provide its marketing data for such purposes," she says.

The goal of Aviva's test: With 60,000 actual insurance applicants, figure out how to use the marketing databases and other information to reach the same underwriting conclusions that Aviva reached using traditional methods such as blood work. The 60,000 people were applicants Aviva had already judged.

Such predictive models wouldn't necessarily look for indicators of all diseases, such as AIDS, because the insurer would likely learn about some conditions from the answers on an application. Rather, insurers say a model would tend to look for potential risks such as, for instance, diabetes (from, say, a poor diet).

Aviva declined to discuss the process in detail, but Mr. Currier says the insurer found that the model consistently yielded results that "closely aligned with those of purely traditional underwriting decisions."

The insurer says pilot projects with marketing data are continuing in its effort to improve clients' buying experience.

Deloitte acknowledges the potentially controversial nature of its work. "No matter what their predictive powers may be, any variable that is deemed to create a legal or public-relations risk, or is counter to the company's 'values,' should be excluded from the model," its consultants wrote in an April paper.

Deloitte isn't the only firm pushing data-mining for insurers. Celent, an insurance consulting arm of Marsh & McLennan Cos., recently published a study suggesting insurers conld use social-networking data to help price policies and aid in fraud detection.

A life insurer might want to scrutinize an applicant who reports no family history of cancer, but indicates online an affinity with a cancer-research group, says Mike Fitzgerald, a Celent senior analyst.

"Whether people actually realize it or not, they are significantly increasing their personal transparency," he says. "It's all public, and it's electronically mineable."

Write to Leslie Scism at leslie.scism@wsj.com and Mark Maremont at mark.maremont@wsj.com

More From 'What They Know'

A Web Pioneer Profiles Users by Name

Web's New Goldmine: Your Secrets

Personal Details Exposed Via Biggest Websites

Microsoft Quashed Bid to Boost Web Privacy

On Web's Cutting Edge, Anonymity in Name Only

Stalking by Cellphone

On the Web, Children Face Intensive Tracking

Google Agonizes Over Privacy

'Scrapers' Dig Deep for Data on Web

Facebook in Privacy Breach

The Tracking Ecosystem

Follow **@whattheyknow** on Twitter

Complete Coverage: What They Know

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

ENGLISH

IMPORTANT: BY USING YOUR IPHONE, YOU ARE AGREEING TO BE BOUND BY THE FOLLOWING APPLE AND THIRD PARTY TERMS:

A. APPLE IPHONE SOFTWARE LICENSE AGREEMENT
B. NOTICES FROM APPLE
C. GOOGLE MAPS TERMS AND CONDITIONS
D. YOUTUBE TERMS AND CONDITIONS

APPLE INC.
IPHONE SOFTWARE LICENSE AGREEMENT
Single Use License

PLEASE READ THIS SOFTWARE LICENSE AGREEMENT ("LICENSE") CAREFULLY BEFORE USING YOUR IPHONE OR DOWNLOADING THE SOFTWARE UPDATE ACCOMPANYING THIS LICENSE. BY USING YOUR IPHONE OR DOWNLOADING THIS SOFTWARE UPDATE, AS APPLICABLE, YOU ARE AGREEING TO BE BOUND BY THE TERMS OF THIS LICENSE. UNLESS YOU RETURN THE IPHONE IN ACCORDANCE WITH APPLE'S RETURN POLICY, IF YOU DO NOT AGREE TO THE TERMS OF THIS LICENSE, DO NOT USE THE IPHONE OR DOWNLOAD THIS SOFTWARE UPDATE. IF YOU DO NOT AGREE TO THE TERMS OF THE LICENSE, YOU MAY RETURN THE IPHONE WITHIN THE RETURN PERIOD TO THE APPLE STORE OR AUTHORIZED DISTRIBUTOR WHERE YOU OBTAINED IT FOR A REFUND, SUBJECT TO APPLE'S RETURN POLICY FOUND AT http://www.apple.com/legal/sales_policies/.

1. General. The software (including Boot ROM code and other embedded software), documentation, interfaces, content, fonts and any data that came with your iPhone ("Original iPhone Software"), as may be updated or replaced by feature enhancements, software updates or system restore software provided by Apple ("iPhone Software Updates"), whether in read only memory, on any other media or in any other form (the Original iPhone Software and iPhone Software Updates are collectively referred to as the "iPhone Software") are licensed, not sold, to you by Apple Inc. ("Apple") for use only under the terms of this License. Apple and its licensors retain ownership of the iPhone Software itself and reserve all rights not expressly granted to you.

Apple will provide you any iPhone OS software updates that it may release from time to time, up to and including the next major iPhone OS software release following the version of iPhone OS software that originally shipped from Apple on your iPhone, for free. For example, if your iPhone originally shipped with iPhone 2.x software, Apple would provide you with any iPhone OS software updates it might release up to and including the iPhone 3.x software release. Such updates and releases may not necessarily include all of the new software features that Apple releases for newer iPhone models.

2. Permitted License Uses and Restrictions.
(a) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to use the iPhone Software on a single Apple-branded iPhone. Except as permitted in Section 2(b) below, this License does not allow the iPhone Software to exist on more than one Apple-branded iPhone at a time or on any other phone, and you may not distribute or make the iPhone Software available over a network where it could be used by multiple devices at the same time. This License does not grant you any rights to use Apple proprietary interfaces and other intellectual property in the design, development, manufacture, licensing or distribution of third party devices and accessories, or third party software applications, for use with the iPhone. Some of those rights are available under separate licenses from Apple. For more information on developing third party devices and accessories for the iPhone, please email madeforipod@apple.com. For more information on developing software applications for the iPhone, please email devprograms@apple.com.

(b) Subject to the terms and conditions of this License, you are granted a limited non-exclusive license to download iPhone Software Updates that may be made available by Apple for your model of the iPhone to update or restore the software on any such iPhone that you own or control. This License does not allow you to update or restore iPhones that you do not control or own, and you may not distribute or make the iPhone Software Updates available over a network where they could be used by multiple devices or multiple computers at the same time. You may make one copy of the iPhone Software Updates stored on your computer in machine-readable form for backup purposes only, provided that the backup copy must include all copyright or other proprietary notices contained on the original.

(c) You may not and you agree not to, or to enable others to, copy (except as expressly permitted by this License), decompile, reverse engineer, disassemble, attempt to derive the source code of, decrypt, modify, or create derivative works of the iPhone Software or any services provided by the iPhone Software, or any part thereof (except as and only to the extent any foregoing restriction is prohibited by applicable law or to the extent as may be permitted by licensing terms governing use of open-sourced components included with the iPhone Software). Any attempt to do so is a violation of the rights of Apple and its licensors of the iPhone Software.

(d) By storing content on your iPhone you are making a digital copy. In some jurisdictions, it is unlawful to make digital copies without prior permission from the rightsholder. The iPhone Software may be used to reproduce materials so long as such use is limited to reproduction of non-copyrighted materials, materials in which you own the copyright, or materials you are authorized or legally permitted to reproduce.

(e) You agree to use the iPhone Software and the Services (as defined in Section 5 below) in compliance with all applicable laws, including local laws of the country or region in which you reside or in which you download or use the iPhone Software and Services.

3. Transfer. You may not rent, lease, lend, sell, redistribute, or sublicense the iPhone Software. You may, however, make a one-time permanent transfer of all of your license rights to the iPhone Software to another party in connection with the transfer of ownership of your iPhone, provided that: (a) the transfer must include your iPhone and all of the iPhone Software, including all its component parts, original media, printed materials and this License; (b) you do not retain any copies of the iPhone Software, full or partial, including copies stored on a computer or other storage device; and (c) the party receiving the iPhone Software reads and agrees to accept the terms and conditions of this License.

4. Consent to Use of Non-Personal Data.
(a) Diagnostic Data. You agree that Apple and its subsidiaries and agents may collect, maintain, process and use diagnostic, technical and related information, including but not limited to information about your iPhone, computer, system and application software, and peripherals, that is gathered periodically to facilitate the provision of software updates, product support and other services to you (if any) related to the iPhone Software, and to verify compliance with the terms of this License. Apple may use this information, as long as it is in a form that does not personally identify you, to improve our products or to provide services or technologies to you.

(b) Location Data. Apple and its partners and licensees may provide certain services through your iPhone that rely upon location information. To provide these services, where available, Apple and its partners and licensees may transmit, collect, maintain, process and use your location data, including the real-time geographic location of your iPhone. The location data collected by Apple is collected in a form that does not personally identify you and may be used by Apple and its partners and licensees to provide location-based products and services. By using any location-based services on your iPhone, you agree and consent to Apple's and its partners' and licensees' transmission, collection, maintenance, processing and use of your location data to provide such products and services. You may withdraw this consent at any time by not using the location-based features or by turning off the Location Services setting on your iPhone. Not using these features will not impact the non location-based functionality of your iPhone. When using third party applications or services on the iPhone that use or provide location data, you are subject to and should review such third party's terms and privacy policy on use of location data by such third party applications or services.

5. Services and Third Party Materials.
(a) The iPhone Software enables access to Apple's iTunes Store, App Store and other Apple and third party services and web sites (collectively and individually, "Services"). Use of the Services requires Internet access and use of certain Services requires you to accept additional terms. By using this software in connection with an iTunes Store account, you agree to the latest iTunes Store Terms and Conditions, which you may access and review at http://www.apple.com/legal/itunes/ww/.

(b) You understand that by using any of the Services, you may encounter content that may be deemed offensive, indecent, or objectionable, which content may or may not be identified as having explicit language, and that the results of any search or entering of a particular URL may automatically and unintentionally generate links or references to objectionable material. Nevertheless, you agree to use the Services at your sole risk and that Apple shall have no liability to you for content that may be found to be offensive, indecent, or objectionable.

(c) Certain Services may display, include or make available content, data, information, applications or materials from third parties ("Third Party Materials") or provide links to certain third party web sites. By using the Services, you acknowledge and agree that Apple is not responsible for examining or evaluating the content, accuracy, completeness, timeliness, validity, copyright compliance, legality, decency, quality or any other aspect of such Third Party Materials or web sites. Apple, its officers, affiliates and subsidiaries do not warrant or endorse and do not assume and will not have any liability or responsibility to you or any other person for any third-party Services, Third Party Materials or web sites, or for any other materials, products, or services of third parties. Third Party Materials and links to other web sites are provided solely as a convenience to you.

(d) Financial information displayed by any Services is for general informational purposes only and should not be relied upon as investment advice. Before executing any securities transaction based upon information obtained through the Services, you should consult with a financial or securities professional who is legally qualified to give financial or securities advice in your country or region. Location data provided by any Services is for basic navigational purposes only and is not intended to be relied upon in situations where precise location information is needed or where erroneous, inaccurate, time-delayed or incomplete location data may lead to death, personal injury, property or environmental damage. Neither Apple nor any of its content providers guarantees the availability, accuracy, completeness, reliability, or timeliness of stock information, location data or any other data displayed by any Services.

(e) You agree that the Services contain proprietary content, information and material that is owned by Apple and/or its licensors, and is protected by applicable intellectual property and other laws, including but not limited to copyright, and that you will not use such proprietary content, information or materials in any way whatsoever except for permitted use of the Services or in any manner that is inconsistent with the terms of this License or that infringes any intellectual property rights of a third party or Apple. No portion of the Services may be reproduced in any form or by any means. You agree not to modify, rent, lease, loan, sell, distribute, or create derivative works based on the Services, in any manner, and you shall not exploit the Services in any unauthorized way whatsoever, including but not limited to, using the Services to transmit any computer viruses, worms, trojan horses or other malware, or by trespass or burdening network capacity. You further agree not to use the Services in any manner to harass, abuse, stalk, threaten, defame or otherwise infringe or violate the rights of any other party, and that Apple is not in any way responsible for any such use by you, nor for any harassing, threatening, defamatory, offensive, infringing or illegal messages or transmissions that you may receive as a result of using any of the Services.

(f) In addition, Services and Third Party Materials that may be accessed from, displayed on or linked to from the iPhone are not available in all languages or in all countries. Apple makes no representation that such Services and Materials are appropriate or available for use in any particular location. To the extent you choose to access such Services or Materials, you do so at your own initiative and are responsible for compliance with any applicable laws, including but not limited to applicable local laws. Apple and its licensors reserve the right to change, suspend, remove, or disable access to any Services at any time without notice. In no event will Apple be liable for the removal of or disabling of access to any such Services. Apple may also impose limits on the use of or access to certain Services, in any case and without notice or liability.

6. Termination. This License is effective until terminated. Your rights under this License will terminate automatically or otherwise cease to be effective without notice from Apple if you fail to comply with any term(s) of this License. Upon the termination of this License, you shall cease all use of the iPhone Software. Sections 7, 8, 9, 12 and 13 of this License shall survive any such termination.

[illegible]

[illegible]

8. Limitation of Liability. TO THE EXTENT NOT PROHIBITED BY APPLICABLE LAW, IN NO EVENT SHALL APPLE BE LIABLE FOR PERSONAL INJURY, OR ANY INCIDENTAL, SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, CORRUPTION OR LOSS OF DATA, FAILURE TO TRANSMIT OR RECEIVE ANY DATA, BUSINESS INTERRUPTION OR ANY OTHER COMMERCIAL DAMAGES OR LOSSES, ARISING OUT OF OR RELATED TO YOUR USE OF OR INABILITY TO USE THE IPHONE SOFTWARE AND SERVICES OR ANY THIRD PARTY SOFTWARE OR APPLICATIONS IN CONJUNCTION WITH THE IPHONE SOFTWARE, HOWEVER CAUSED, REGARDLESS OF THE THEORY OF LIABILITY (CONTRACT, TORT OR OTHERWISE) AND EVEN IF APPLE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SOME JURISDICTIONS DO NOT ALLOW THE LIMITATION OF LIABILITY FOR PERSONAL INJURY, OR OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION MAY NOT APPLY TO YOU. In no event shall Apple's total liability to you for all damages (other than as may be required by applicable law in cases involving personal injury) exceed the amount of two hundred and fifty dollars (U.S. $250.00). The foregoing limitations will apply even if the above stated remedy fails of its essential purpose.

9. Digital Certificates. The iPhone Software contains functionality that allows it to accept digital certificates either issued from Apple or from third parties. YOU ARE SOLELY RESPONSIBLE FOR DECIDING WHETHER OR NOT TO RELY ON A CERTIFICATE WHETHER ISSUED BY APPLE OR A THIRD PARTY. YOUR USE OF DIGITAL CERTIFICATES IS AT YOUR SOLE RISK. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, APPLE MAKES NO WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, AS TO MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE, ACCURACY, SECURITY, OR NON-INFRINGEMENT OF THIRD PARTY RIGHTS WITH RESPECT TO DIGITAL CERTIFICATES.

10. Export Control. You may not use or otherwise export or reexport the iPhone Software except as authorized by United States law and the laws of the jurisdiction(s) in which the iPhone Software was obtained. In particular, but without limitation, the iPhone Software may not be exported or re-exported (a) into any U.S. embargoed countries or (b) to anyone on the U.S. Treasury Department's list of Specially Designated Nationals or the U.S. Department of Commerce Denied Person's List or Entity List. By using the iPhone Software, you represent and warrant that you are not located in any such country or on any such list. You also agree that you will not use the iPhone Software for any purposes prohibited by United States law, including, without limitation, the development, design, manufacture or production of missiles, nuclear, chemical or biological weapons.

11. Government End Users. The iPhone Software and related documentation are "Commercial Items", as that term is defined at 48 C.F.R. §2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are used in 48 C.F.R. §12.212 or 48 C.F.R. §227.7202, as applicable. Consistent with 48 C.F.R. §12.212 or 48 C.F.R. §227.7202-1 through 227.7202-4, as applicable, the Commercial Computer Software and Commercial Computer Software Documentation are being licensed to U.S. Government end users (a) only as Commercial Items and (b) with only those rights as are granted to all other end users pursuant to the terms and conditions herein. Unpublished-rights reserved under the copyright laws of the United States.

12. Controlling Law and Severability. This License will be governed by and construed in accordance with the laws of the State of California, excluding its conflict of law principles. This License shall not be governed by the United Nations Convention on Contracts for the International Sale of Goods. the application of which is expressly excluded. If for any reason a court of competent jurisdiction finds any provision, or portion thereof, to be unenforceable, the remainder of this License shall continue in full force and effect.

13. Complete Agreement; Governing Language. This License constitutes the entire agreement between you and Apple relating to the iPhone Software and supersedes all prior or contemporaneous understandings regarding such subject matter. No amendment to or modification of this License will be binding unless in writing and signed by Apple. Any translation of this License is done for local requirements and in the event of a dispute between the English and any non-English versions, the English version of this License shall govern, to the extent not prohibited by local law in your jurisdiction.

14. Third Party Acknowledgements. Portions of the iPhone Software may utilize or include third party software and other copyrighted material. Acknowledgements, licensing terms and disclaimers for such material are contained in the electronic documentation for the iPhone Software, and your use of such material is governed by their respective terms. Use of the Google Safe Browsing Service is subject to the Google Terms of Service (http://www.google.com/terms_of_service.html) and to Google's Privacy Policy (http://www.google.com/privacypolicy.html).

15. Use of MPEG-4; H.264/AVC Notice.
(a) The iPhone Software contains MPEG-4 video encoding and/or decoding functionality. The iPhone Software is licensed under the MPEG-4 Visual Patent Portfolio License for the personal and non-commercial use of a consumer for (i) encoding video in compliance with the MPEG-4 Visual Standard ("MPEG-4 Video") and/or (ii) decoding MPEG-4 video that was encoded by a consumer engaged in a personal and non-commercial activity and/or was obtained from a video provider licensed by MPEG LA to provide MPEG-4 video. No license is granted or shall be implied for any other use. Additional information including that relating to promotional, internal and commercial uses and licensing may be obtained from MPEG LA, LLC. See http://www.mpegla.com.

(b) The iPhone Software contains AVC encoding and/or decoding functionality. commercial use of H.264/AVC requires additional licensing and the following provision applies: THE AVC FUNCTIONALITY IN THE IPHONE SOFTWARE IS LICENSED HEREIN ONLY FOR THE PERSONAL AND NON-COMMERCIAL USE OF A CONSUMER TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL AND NON-COMMERCIAL ACTIVITY AND/OR AVC VIDEO THAT WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. INFORMATION REGARDING OTHER USES AND LICENSES MAY BE OBTAINED FROM MPEG LA L.L.C. SEE HTTP://WWW.MPEGLA.COM.

16. Yahoo Search Service Restrictions. The Yahoo Search Service available through Safari is licensed for use only in the following countries and regions: Argentina, Aruba, Australia, Austria, Barbados, Belgium, Bermuda, Brazil, Bulgaria, Canada, Cayman Islands, Chile, Colombia, Cyprus, Czech Republic, Denmark, Dominican Republic, Ecuador, El Salvador, Finland, France, Germany, Greece, Grenada, Guatemala, Hong Kong, Hungary, Iceland, India, Indonesia, Ireland, Italy, Jamaica, Latvia, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, New Zealand, Nicaragua, Norway, Panama, Peru, Philippines, Poland, Portugal, Puerto Rico, Romania, Singapore, Slovakia, Slovenia, South Korea, Spain, St. Lucia, St. Vincent, Sweden, Switzerland, Taiwan, Thailand, The Bahamas, Trinidad and Tobago, Turkey, UK, Uruguay, US and Venezuela.

17. Microsoft Exchange Notice. The Microsoft Exchange mail setting in the iPhone Software is licensed only for over-the-air synchronization of information, such as email, contacts, calendar and tasks, between your iPhone and Microsoft Exchange Server or other server software licensed by Microsoft to implement the Microsoft Exchange ActiveSync protocol.

EA0367
Update Rev. 5/8/09

NOTICES FROM APPLE
If Apple needs to contact you about your product or account, you consent to receive the notices by email. You agree that any such notices that we send you electronically will satisfy any legal communication requirements.

GOOGLE MAPS TERMS AND CONDITIONS

Thank you for trying out the Google Maps for mobile software application! This page contains the terms and conditions (the "Terms and Conditions") for Google Maps for mobile and the enterprise version of Google Maps for mobile. In order to use this software, including any third party software made available to you in conjunction with this software and/or the related service, (collectively referred to below as "Google Maps for mobile") you agree to be bound by these Terms and Conditions, either on behalf of yourself or on behalf of your employer or other entity. If you are agreeing to be bound by these Terms and Conditions on behalf of your employer or other entity, you represent and warrant that you have full legal authority to bind your employer or such entity to these Terms and Conditions. If you don't have the legal authority to bind, please press "No" when asked whether you agree to these Terms and Conditions, and do not proceed with use of this product.

Additional Terms

Google Maps for mobile is designed to be used in conjunction with Google's Maps services and other Google services. Accordingly, you agree and acknowledge that your use of Google Maps for mobile is also subject to (a) the specific terms of service for Google Maps (which can be viewed at http://local.google.com/help/terms_local.html) including the content notices applicable thereto (which can be viewed at http://local.google.com/help/legalnotices_local.html), (b) the general Google terms of service (which can be viewed at http://www.google.com/terms_of_service.html) and (c) Google's overall privacy policy (which can be viewed at http://www.google.com/privacypolicy.html), as well as specific privacy policies, such as the Google Maps for mobile privacy policy included with this application, such provisions being hereby incorporated into these Terms and Conditions by reference. To the extent that there is any inconsistency or conflict between such additional terms and these Terms and Conditions, the provisions of these Terms and Conditions take precedence.

Network Charges

Google does not charge for downloading or using Google Maps for mobile, but depending on your plan and your carrier or provider, your carrier or other provider may charge you for downloading Google Maps for mobile or for use of your mobile phone when you access information or other Google services through Google Maps for mobile.

Non-Commercial Use Only

Google Maps for mobile is made available to you for your non-commercial use only. This means that you may use it for your personal use only; you may use it at work or at home, to search for anything you want, subject to the terms set out in these Terms and Conditions. You need to obtain Google's permission first, which you can do by contacting mobile-support@google.com, if you want to sell Google Maps for mobile or any information, services, or software associated with or derived from it, or if you want to modify, copy, license, or create derivative works from Google Maps for mobile.

Unless you have our prior written consent, you agree not to modify, adapt, translate, prepare derivative works from, decompile, reverse engineer, disassemble or otherwise attempt to derive source code from Google Maps for mobile.
Furthermore, you may not use Google Maps for mobile in any manner that could damage, disable, overburden, or impair Google's services (e.g., you may not use the Google Maps for mobile in an automated manner), nor may you use Google Maps for mobile in any manner that could interfere with any other party's use and enjoyment of Google's services.

If you have comments on Google Maps for mobile or ideas on how to improve it, please email mobile-support@google.com. Please note that by doing so, you also grant Google and third parties permission to use and incorporate your ideas or comments into Google Maps for mobile (or third party software) without further notice or compensation.

Intellectual Property

As between you and Google, you agree and acknowledge that Google owns all rights, title and interest in and to Google Maps for mobile, including without limitation all associated Intellectual Property Rights. "Intellectual Property Rights" means any and all rights existing from time to time under patent law, copyright law, trade secret law, trademark law, unfair competition law, and any and all other proprietary rights, and any and all applications, renewals, extensions and restorations thereof, now or hereafter in force and effect worldwide. You agree to not remove, obscure, or alter Google's or any third party's copyright notice, trademarks, or other proprietary rights notices affixed to or contained within or accessed in conjunction with or through the Google Maps for mobile.

Disclaimer of Warranties

Google and any third party who makes its software available in conjunction with or through Google Maps for mobile disclaim any responsibility for any harm resulting from your use of Google Maps for mobile and/or any third party software accessed in conjunction with or through Google Maps for mobile.

GOOGLE MAPS FOR MOBILE IS PROVIDED "AS IS," WITH NO WARRANTIES WHATSOEVER. GOOGLE AND SUCH THIRD PARTIES EXPRESSLY DISCLAIM TO THE FULLEST EXTENT PERMITTED BY LAW ALL EXPRESS, IMPLIED, AND STATUTORY WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY RIGHTS. GOOGLE AND ANY SUCH THIRD PARTIES DISCLAIM ANY WARRANTIES REGARDING THE SECURITY, RELIABILITY, TIMELINESS, AND PERFORMANCE OF GOOGLE MAPS FOR MOBILE AND SUCH THIRD PARTY SOFTWARE.

YOU UNDERSTAND AND AGREE THAT YOU DOWNLOAD AND/OR USE GOOGLE MAPS FOR MOBILE AT YOUR OWN DISCRETION AND RISK AND THAT YOU WILL BE SOLELY RESPONSIBLE FOR ANY DAMAGES TO YOUR COMPUTER OR MOBILE DEVICE SYSTEM OR LOSS OF DATA THAT RESULTS FROM THE DOWNLOAD OR USE OF GOOGLE MAPS FOR MOBILE. SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF IMPLIED WARRANTIES, SO THE ABOVE EXCLUSIONS MAY NOT APPLY TO YOU. YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE TO STATE AND JURISDICTION TO JURISDICTION.

Limitation of Liability

UNDER NO CIRCUMSTANCES SHALL GOOGLE OR ANY THIRD PARTY WHO MAKE THEIR SOFTWARE AVAILABLE IN CONJUNCTION WITH OR THROUGH THE GOOGLE MAPS FOR MOBILE BE LIABLE TO ANY USER ON ACCOUNT OF THAT USER'S USE OR MISUSE OF GOOGLE MAPS FOR MOBILE. SUCH LIMITATION OF LIABILITY SHALL APPLY TO PREVENT RECOVERY OF DIRECT, INDIRECT, INCIDENTAL, CONSEQUENTIAL, SPECIAL, EXEMPLARY, AND PUNITIVE DAMAGES WHETHER SUCH CLAIM IS BASED ON WARRANTY, CONTRACT, TORT (INCLUDING NEGLIGENCE), OR OTHERWISE, (EVEN IF GOOGLE AND/OR A THIRD PARTY SOFTWARE PROVIDER HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES). SUCH LIMITATION OF LIABILITY SHALL APPLY WHETHER THE DAMAGES ARISE FROM USE OR MISUSE OF AND RELIANCE ON GOOGLE MAPS FOR MOBILE OR ON PRODUCTS OR SERVICES MADE AVAILABLE IN CONJUNCTION WITH OR THROUGH GOOGLE MAPS FOR MOBILE, FROM INABILITY TO USE GOOGLE MAPS FOR MOBILE OR PRODUCTS OR SERVICES MADE AVAILABLE IN CONJUNCTION WITH OR THROUGH THE GOOGLE MAPS FOR MOBILE, OR FROM THE INTERRUPTION, SUSPENSION, OR TERMINATION OF GOOGLE MAPS FOR MOBILE OR PRODUCTS OR SERVICES MADE AVAILABLE IN CONJUNCTION WITH OR THROUGH GOOGLE MAPS FOR MOBILE (INCLUDING SUCH DAMAGES INCURRED BY THIRD PARTIES). SUCH LIMITATION SHALL APPLY NOTWITHSTANDING A FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY AND TO THE FULLEST EXTENT PERMITTED BY LAW.
SOME STATES OR OTHER JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THE ABOVE LIMITATIONS AND EXCLUSIONS MAY NOT APPLY TO YOU.

Miscellaneous Provisions

These Terms and Conditions will be governed by and construed in accordance with the laws of the State of California, without giving effect to the conflict of laws provisions of California or your actual state or country of residence. If for any reason a court of competent jurisdiction finds any provision or portion of these Terms and Conditions to be unenforceable, the remainder of these Terms and Conditions will continue in full force and effect.
These Terms and Conditions constitute the entire agreement between you and Google with respect to the subject matter hereof and supersede all prior or contemporaneous understandings or agreements, written or oral, regarding such subject matter. Any waiver of any provision of these Terms and Conditions will be effective only if in writing and signed by Google.

September 2007

YouTube Terms of Service

1. Your Acceptance

A. By using and/or visiting this website (collectively, including all content and functionality available through the YouTube.com domain name, the "YouTube Website", or "Website"), you signify your agreement to (1) these terms and conditions (the "Terms of Service"), (2)YouTube's privacy notice, found at http://www.youtube.com/t/privacy and incorporated here by reference, and (3) YouTube's Community Guidelines, found at http://www.youtube.com/t/community_guidelines and also incorporated here by reference. If you do not agree to any of these terms, the YouTube privacy notice, or the Community Guidelines, please do not use the YouTube Website.
B. Although we may attempt to notify you when major changes are made to these Terms of Service, you should periodically review the most up-to-date version http://www.youtube.com/t/terms). YouTube may, in its sole discretion, modify or revise these Terms of Service and policies at any time, and you agree to be bound by such modifications or revisions. Nothing in this Agreement shall be deemed to confer any third-party rights or benefits.

2. YouTube Website

A. These Terms of Service apply to all users of the YouTube Website, including users who are also contributors of video content, information, and other materials or services on the Website. The YouTube Website includes all aspects of YouTube, including but not limited to all products, software and services offered via the website such as the YouTube channels, the YouTube "Embeddable Player," the YouTube "Uploader" and other applications.
B. The YouTube Website may contain links to third party websites that are not owned or controlled by YouTube. YouTube has no control over, and assumes no responsibility for, the content, privacy policies, or practices of any third party websites. In addition, YouTube will not and cannot censor or edit the content of any third-party site. By using the Website, you expressly relieve YouTube from any and all liability arising from your use of any third-party website.
C. Accordingly, we encourage you to be aware when you leave the YouTube Website and to read the terms and conditions and privacy policy of each other website that you visit.

3. YouTube Accounts

A. In order to access some features of the Website, you will have to create a YouTube account. You may never use another's account without permission. When creating your account, you must provide accurate and complete information. You are solely responsible for the activity that occurs on your account, and you must keep your account password secure. You must notify YouTube immediately of any breach of security or unauthorized use of your account.
B. Although YouTube will not be liable for your losses caused by any unauthorized use of your account, you may be liable for the losses of YouTube or others due to such unauthorized use.

4. General Use of the Website--Permissions and Restrictions

YouTube hereby grants you permission to access and use the Website as set forth in these Terms of Service, provided that:

A. You agree not to distribute in any medium any part of the Website, including but not limited to User Submissions (defined below), without YouTube's prior written authorization.
B. You agree not to alter or modify any part of the Website, including but not limited to YouTube's Embeddable Player or any of its related technologies.
C. You agree not to access User Submissions (defined below) or YouTube Content through any technology or means other than the video playback pages of the Website itself, the YouTube Embeddable Player, or other explicitly authorized means YouTube may designate.
D. You agree not to use the Website, including the YouTube Embeddable Player for any commercial use, without the prior written authorization of YouTube. Prohibited commercial uses include any of the following actions taken without YouTube's express approval:
sale of access to the Website or its related services (such as the Embeddable Player) on another website;
use of the Website or its related services (such as the Embeddable Player), for the primary purpose of gaining advertising or subscription revenue;
the sale of advertising, on the YouTube website or any third-party website, targeted to the content of specific User Submissions or YouTube content;
and any use of the Website or its related services (such as the Embeddable player) that YouTube finds, in its sole discretion, to use YouTube's resources or User Submissions with the effect of competing with or displacing the market for YouTube, YouTube content, or its User Submissions. (For more information about prohibited commercial uses, see our FAQ.)
E. Prohibited commercial uses do not include:
uploading an original video to YouTube, or maintaining an original channel on YouTube, to promote your business or artistic enterprise;
using the Embeddable Player to show YouTube videos on an ad-enabled blog or website, provided the primary purpose of using the Embeddable Player is not to gain advertising revenue or compete with YouTube;
any use that YouTube expressly authorizes in writing.
F. (For more information about what constitutes a prohibited commercial use, see our FAQ.)
G. If you use the YouTube Embeddable Player on your website, you must include a prominent link back to the YouTube website on the pages containing the Embeddable Player and you may not modify, build upon, or block any portion of the Embeddable Player in any way.
H. If you use the YouTube Uploader, you agree that it may automatically download and install updates from time to time from YouTube. These updates are designed to improve, enhance and further develop the Uploader and may take the form of bug fixes, enhanced functions, new software modules and completely new versions. You agree to receive such updates (and permit YouTube to deliver these to you) as part of your use of the Uploader.
I. You agree not to use or launch any automated system, including without limitation, "robots," "spiders," or "offline readers," that accesses the Website in a manner that sends more request messages to the YouTube servers in a given period of time than a human can reasonably produce in the same period by using a conventional on-line web browser. Notwithstanding the foregoing, YouTube grants the operators of public search engines permission to use spiders to copy materials from the site for the sole purpose of and solely to the extent necessary for creating publicly available searchable indices of the materials, but not caches or archives of such materials. YouTube reserves the right to revoke these exceptions either generally or in specific cases. You agree not to collect or harvest any personally identifiable information, including account names, from the Website, nor to use the communication systems provided by the Website (e.g. comments, email) for any commercial solicitation purposes. You agree not to solicit, for commercial purposes, any users of the Website with respect to their User Submissions.
J. In your use of the website, you will otherwise comply with the terms and conditions of these Terms of Service, YouTube Community Guidelines, and all applicable local, national, and international laws and regulations.
K. YouTube reserves the right to discontinue any aspect of the YouTube Website at any time.

5. Your Use of Content on the Site

In addition to the general restrictions above, the following restrictions and conditions apply specifically to your use of content on the YouTube Website.

A. The content on the YouTube Website, except all User Submissions (as defined below), including without limitation, the text, software, scripts, graphics, photos, sounds, music, videos, interactive features and the like ("Content") and the trademarks, service marks and logos contained therein ("Marks"), are owned by or licensed to YouTube, subject to copyright and other intellectual property rights under the law. Content on the Website is provided to you AS IS for your information and personal use only and may not be downloaded, copied, reproduced, distributed, transmitted, broadcast, displayed, sold, licensed, or otherwise exploited for any other purposes whatsoever without the prior written consent of the respective owners. YouTube reserves all rights not expressly granted in and to the Website and the Content.
B. You may access User Submissions for your information and personal use solely as intended through the provided functionality of the YouTube Website. You shall not copy or download any User Submission unless you see a "download" or similar link displayed by YouTube on the YouTube Website for that User Submission.

C. User Comments are made available to you for your information and personal use solely as intended through the normal functionality of the YouTube Website. User Comments are made available "as is", and may not be used, copied, reproduced, distributed, transmitted, broadcast, displayed, sold, licensed, downloaded, or otherwise exploited in any manner not intended by the normal functionality of the YouTube Website or otherwise as prohibited under this Agreement.
D. You may access YouTube Content, User Submissions and other content only as permitted under this Agreement. YouTube reserves all rights not expressly granted in and to the YouTube Content and the YouTube Website.
E. You agree to not engage in the use, copying, or distribution of any of the Content other than expressly permitted herein, including any use, copying, or distribution of User Submissions of third parties obtained through the Website for any commercial purposes.
F. You agree not to circumvent, disable or otherwise interfere with security-related features of the YouTube Website or features that prevent or restrict use or copying of any Content or enforce limitations on use of the YouTube Website or the Content therein.
G. You understand that when using the YouTube Website, you will be exposed to User Submissions from a variety of sources, and that YouTube is not responsible for the accuracy, usefulness, safety, or intellectual property rights of or relating to such User Submissions. You further understand and acknowledge that you may be exposed to User Submissions that are inaccurate, offensive, indecent, or objectionable, and you agree to waive, and hereby do waive, any legal or equitable rights or remedies you have or may have against YouTube with respect thereto, and agree to indemnify and hold YouTube, its Owners/Operators, affiliates, and/or licensors, harmless to the fullest extent allowed by law regarding all matters related to your use of the site.

6. Your User Submissions and Conduct

A. As a YouTube account holder you may submit video content ("User Videos") and textual content ("User Comments"). User Videos and User Comments are collectively referred to as "User Submissions." You understand that whether or not such User Submissions are published, YouTube does not guarantee any confidentiality with respect to any User Submissions.
B. You shall be solely responsible for your own User Submissions and the consequences of posting or publishing them. In connection with User Submissions, you affirm, represent, and/or warrant that: you own or have the necessary licenses, rights, consents, and permissions to use and authorize YouTube to use all patent, trademark, trade secret, copyright or other proprietary rights in and to any and all User Submissions to enable inclusion and use of the User Submissions in the manner contemplated by the Website and these Terms of Service.
C. For clarity, you retain all of your ownership rights in your User Submissions. However, by submitting User Submissions to YouTube, you hereby grant YouTube a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the User Submissions in connection with the YouTube Website and YouTube's (and its successors' and affiliates') business, including without limitation for promoting and redistributing part or all of the YouTube Website (and derivative works thereof) in any media formats and through any media channels. You also hereby grant each user of the YouTube Website a non-exclusive license to access your User Submissions through the Website, and to use, reproduce, distribute, display and perform such User Submissions as permitted through the functionality of the Website and under these Terms of Service. The above licenses granted by you in User Videos terminate within a commercially reasonable time after you remove or delete your User Videos from the YouTube Website. You understand and agree, however, that YouTube may retain, but not display, distribute, or perform, server copies of User Submissions that have been removed or deleted. The above licenses granted by you in User Comments are perpetual and irrevocable.
D. In connection with User Submissions, you further agree that you will not submit material that is copyrighted, protected by trade secret or otherwise subject to third party proprietary rights, including privacy and publicity rights, unless you are the owner of such rights or have permission from their rightful owner to post the material and to grant YouTube all of the license rights granted herein.
E. You further agree that you will not, in connection with User Submissions, submit material that is contrary to the YouTube Community Guidelines, found at http://www.youtube.com/t/community_guidelines, which may be updated from time to time, or contrary to applicable local, national, and international laws and regulations.
F. YouTube does not endorse any User Submission or any opinion, recommendation, or advice expressed therein, and YouTube expressly disclaims any and all liability in connection with User Submissions. YouTube does not permit copyright infringing activities and infringement of intellectual property rights on its Website, and YouTube will remove all Content and User Submissions if properly notified that such Content or User Submission infringes on another's intellectual property rights. YouTube reserves the right to remove Content and User Submissions without prior notice.

7. Account Termination Policy

A. YouTube will terminate a User's access to its Website if, under appropriate circumstances, they are determined to be a repeat infringer.
B. YouTube reserves the right to decide whether Content or a User Submission is appropriate and complies with these Terms of Service for violations other than copyright infringement, such as, but not limited to, pornography, obscene or defamatory material, or excessive length. YouTube may remove such User Submissions and/or terminate a User's access for uploading such material in violation of these Terms of Service at any time, without prior notice and at its sole discretion.

8. Digital Millennium Copyright Act

A. If you are a copyright owner or an agent thereof and believe that any User Submission or other content infringes upon your copyrights, you may submit a notification pursuant to the Digital Millennium Copyright Act ("DMCA") by providing our Copyright Agent with the following information in writing (see 17 U.S.C 512(c)(3) for further detail):
   A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed;
   Identification of the copyrighted work claimed to have been infringed, or, if multiple copyrighted works at a single online site are covered by a single notification, a representative list of such works at that site;
   Identification of the material that is claimed to be infringing or to be the subject of infringing activity and that is to be removed or access to which is to be disabled and information reasonably sufficient to permit the service provider to locate the material;
   Information reasonably sufficient to permit the service provider to contact you, such as an address, telephone number, and, if available, an electronic mail;
   A statement that you have a good faith belief that use of the material in the manner complained of is not authorized by the copyright owner, its agent, or the law; and
   A statement that the information in the notification is accurate, and under penalty of perjury, that you are authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.
B. YouTube's designated Copyright Agent to receive notifications of claimed infringement is: Heather Gillette, 901 Cherry Ave., San Bruno, CA 94066, email: copyright@youtube.com, fax: 650-872-8513. For clarity, only DMCA notices should go to the Copyright Agent; any other feedback, comments, requests for technical support, and other communications should be directed to YouTube customer service through http://www.google.com/support/youtube. You acknowledge that if you fail to comply with all of the requirements of this Section 5(D), your DMCA notice may not be valid.
C. Counter-Notice, If you believe that your User Submission that was removed (or to which access was disabled) is not infringing, or that you have the authorization from the copyright owner, the copyright owner's agent, or pursuant to the law, to post and use the content in your User Submission, you may send a counter-notice containing the following information to the Copyright Agent:
   Your physical or electronic signature;
   Identification of the content that has been removed or to which access has been disabled and the location at which the content appeared before it was removed or disabled;
   A statement that you have a good faith belief that the content was removed or disabled as a result of mistake or a misidentification of the content; and
   Your name, address, telephone number, and e-mail address, a statement that you consent to the jurisdiction of the federal court in San Francisco, California, and a statement that you will accept service of process from the person who provided notification of the alleged infringement.
D. If a counter-notice is received by the Copyright Agent, YouTube may send a copy of the counter-notice to the original complaining party informing that person that it may replace the removed content or cease disabling it in 10 business days. Unless the copyright owner files an action seeking a court order against the content provider, member or user, the removed content may be replaced, or access to it restored, in 10 to 14 business days or more after receipt of the counter-notice, at YouTube's sole discretion.

9. Warranty Disclaimer

[illegible]

10. Limitation of Liability

[illegible]

YOU SPECIFICALLY ACKNOWLEDGE THAT YOUTUBE SHALL NOT BE LIABLE FOR USER SUBMISSIONS OR THE DEFAMATORY, OFFENSIVE, OR ILLEGAL CONDUCT OF ANY THIRD PARTY AND THAT THE RISK OF HARM OR DAMAGE FROM THE FOREGOING RESTS ENTIRELY WITH YOU.

The Website is controlled and offered by YouTube from its facilities in the United States of America. YouTube makes no representations that the YouTube Website is appropriate or available for use in other locations. Those who access or use the YouTube Website from other jurisdictions do so at their own volition and are responsible for compliance with local law.

11. Indemnity

You agree to defend, indemnify and hold harmless YouTube, its parent corporation, officers, directors, employees and agents, from and against any and all claims, damages, obligations, losses, liabilities, costs or debt, and expenses (including but not limited to attorney's fees) arising from: (i) your use of and access to the YouTube Website; (ii) your violation of any term of these Terms of Service; (iii) your violation of any third party right, including without limitation any copyright, property, or privacy right; or (iv) any claim that one of your User Submissions caused damage to a third party. This defense and indemnification obligation will survive these Terms of Service and your use of the YouTube Website.

12. Ability to Accept Terms of Service

You affirm that you are either more than 18 years of age, or an emancipated minor, or possess legal parental or guardian consent, and are fully able and competent to enter into the terms, conditions, obligations, affirmations, representations, and warranties set forth in these Terms of Service, and to abide by and comply with these Terms of Service. In any case, you affirm that you are over the age of 13, as the YouTube Website is not intended for children under 13. If you are under 13 years of age, then please do not use the YouTube Website. There are lots of other great web sites for you. Talk to your parents about what sites are appropriate for you.

13. Assignment

These Terms of Service, and any rights and licenses granted hereunder, may not be transferred or assigned by you, but may be assigned by YouTube without restriction.

14. General

You agree that: (i) the YouTube Website shall be deemed solely based in California; and (ii) the YouTube Website shall be deemed a passive website that does not give rise to personal jurisdiction over YouTube, either specific or general, in jurisdictions other than California. These Terms of Service shall be governed by the internal substantive laws of the State of California, without respect to its conflict of laws principles. Any claim or dispute between you and YouTube that arises in whole or in part from your use of the YouTube Website shall be decided exclusively by a court of competent jurisdiction located in Santa Clara County, California. These Terms of Service, together with the Privacy Notice at http://www.youtube.com/t/privacy and any other legal notices published by YouTube on the Website, shall constitute the entire agreement between you and YouTube concerning the YouTube Website. If any provision of these Terms of Service is deemed invalid by a court of competent jurisdiction, the invalidity of such provision shall not affect the validity of the remaining provisions of these Terms of Service, which shall remain in full force and effect. No waiver of any term of this these Terms of Service shall be deemed a further or continuing waiver of such term or any other term, and YouTube's failure to assert any right or provision under these Terms of Service shall not constitute a waiver of such right or provision. YouTube reserves the right to amend these Terms of Service at any time and without notice, and it is your responsibility to review these Terms of Service for any changes. Your use of the YouTube Website following any amendment of these Terms of Service will signify your assent to and acceptance of its revised terms. YOU AND YOUTUBE AGREE THAT ANY CAUSE OF ACTION ARISING OUT OF OR RELATED TO THE YOUTUBE WEBSITE MUST COMMENCE WITHIN ONE (1) YEAR AFTER THE CAUSE OF ACTION ACCRUES. OTHERWISE, SUCH CAUSE OF ACTION IS PERMANENTLY BARRED.

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

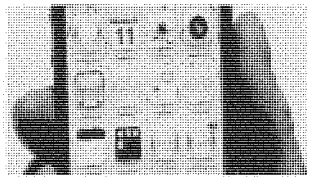
TECHNOLOGY | APRIL 25, 2011

IPhone Stored Location in Test Even if Disabled

By JENNIFER VALENTINO-DEVRIES

Apple Inc.'s iPhone is collecting and storing location information even when location services are turned off, according to a test conducted by The Wall Street Journal.

The location data appear to be collected using cellphone towers and Wi-Fi access points near a user's phone and don't appear to be transmitted back to Apple. Apple didn't immediately respond to a request for comment.



Apple's iPhone is collecting and storing location data even when location services are turned off, according to a Journal test. Jen Valentino explains on digits.

Earlier

The Really Smart Phone

Google Defends Way It Gets Phone Data

Apple, Google Collect User Data

Digits: What Your iPhone Knows About You

Complete Coverage: What They Know

Outside Research

IPhone Stores Months of Location Data

Geothought: A Location Technology Blog

Journal Community

Still, the fact that the iPhone is collecting and storing location data—even when location services are turned off—is likely to renew questions about how well users are informed about the data being gathered by their cellphones. The fact that the iPhone stores months' worth of location data was disclosed by two researchers last week.

The discovery of an unencrypted location file on the iPhone created an uproar among people concerned that their phones could be searched and their location data used against them. On Saturday, Rep. Edward Markey (D., Mass.) called for a congressional investigation into the iPhone location storage, saying that unprotected location information on the phone could put children at risk from predators who hack their phones.

The discovery of the iPhone location file comes amid growing concern about cellphone tracking overall.

Last week, the Journal reported that Apple's iPhone and cellphones powered by Google Inc.'s Android software transmitted their locations back to Google and Apple, respectively.

And last year, a Journal investigation showed that many of the most popular cellphone "apps" go even further, sharing location data and other personal information with third-party companies without a user's knowledge or consent.

Apple and Google have both previously said that the data they receive is anonymous and that users can turn it off by disabling location services.

How concerned are you that the iPhone tracks and stores your location?

- Very
- Somewhat
- Not at all
- Don't have an iPhone

SUBMIT VOTE **View Results »**

However, it appears that turning off location services doesn't disable the storage of location data on iPhones. The Journal tested the collection of data on an iPhone 4 that had been restored to factory settings and was running the latest version of Apple's iOS operating system.

The Journal disabled location services (which are on by default) and immediately recorded the data that had initially been gathered by the phone. The Journal then carried the phone to new locations and observed the data. Over the span of several hours as the phone was moved, it continued to collect location data from new places.

These data included coordinates and time stamps; however, the coordinates were not from the exact locations that the phone traveled, and some of them were several miles away. The phone also didn't indicate how much time was spent in a given location. Other technology watchers on blogs and message boards online have recorded similar findings.

Independent security researcher Ashkan Soltani verified the Journal's findings.

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

Home | Shop | Answers | Radar: News & Commentary | Safari Books Online | Conferences | Training | School of Technology

Insight, analysis, and research about emerging technologies

SEARCH

Data | Gov 2.0 | Mobile | Programming | Publishing | Web 2.0 Find us on: About Radar

Got an iPhone or 3G iPad? Apple is recording your moves

Print
Listen

A hidden file in iOS 4 is regularly recording the position of devices.

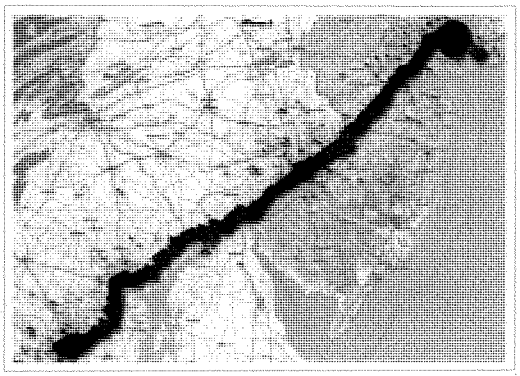
by Alasdair Allan | @aallan | Comments: 230 | 20 April 2011

5,133 Like 12K

Update, 4/27/11 — Apple has posted a response to questions raised in this report and others.

By Alasdair Allan and Pete Warden

Today at Where 2.0 Pete Warden and I will announce the discovery that your iPhone, and your 3G iPad, is regularly recording the position of your device into a hidden file. Ever since iOS 4 arrived, your device has been storing a long list of locations and time stamps. We're not sure why Apple is gathering this data, but it's clearly intentional, as the database is being restored across backups, and even device migrations.



A visualization of iPhone location data. Click to enlarge.

The presence of this data on your iPhone, your iPad, and your backups has security and privacy implications. We've contacted Apple's Product Security team, but we haven't heard back.

What makes this issue worse is that the file is unencrypted and unprotected, and it's on any machine you've synched with your iOS device. It can also be easily accessed on the device itself if it falls into the wrong hands. Anybody with access to this file knows where you've been over the last year, since iOS 4 was released.

In the following video, we discuss how the file was discovered and take a look at the data contained in the file. Further details are posted below.

What information is being recorded?

All iPhones appear to log your location to a file called "consolidated.db." This contains latitude-longitude coordinates along with a timestamp. The coordinates aren't always exact, but they are pretty detailed. There can be tens of thousands of data points in this file, and it appears the collection started with iOS 4, so there's typically around a year's worth of information at this point. Our best guess is that the location is determined by cell-tower triangulation, and the timing of the recording is erratic, with a widely varying frequency of updates that may be triggered by traveling between cells or activity on the phone itself.

Who has access to this data?

Don't panic. As we discuss in the video, there's no immediate harm that would seem to come from the availability of this data. Nor is there evidence to suggest this data is leaving your custody. But why this data is stored and how Apple intends to use it — or not — are important questions that need to be explored.

Related books by Alasdair Allan and Pete Warden

What are the implications of this location data?

The cell phone companies have always had this data, but it takes a court order to access it. Now this information is sitting in plain view, unprotected from the world. Beyond this, there is even more data that we have yet to look at in depth.

For example, in my own case I (Alasdair) discovered a list of hundreds of thousands of wireless access points that my iPhone has been in range of during the last year.

How can you look at your own data?

We have built an application that helps you look at your own data. It's available at petewarden.github.com/iPhoneTracker along with the source code and deeper technical information.

What can you do about this?

An immediate step you can take is to encrypt your backups through iTunes (click on your device within iTunes and then check "Encrypt iPhone Backup" under the "Options" area).

Related:

- iPhone tracking: The day after

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General *Washington, D.C. 20530*

May 9, 2011

The Honorable Al Franken
United States Senate
Washington, D.C. 20510

Dear Senator Franken:

This responds to your letter to Assistant Attorney General Lanny A. Breuer dated April 12, 2011, regarding the Computer Fraud and Abuse Act (CFAA). The Department of Justice endeavors every day to protect both public safety and individual privacy, and the CFAA plays a key role in those efforts. An identical response has been sent to Senator Blumenthal, who joined in your letter.

As you noted, some courts disagree about the precise scope of the term "exceeds authorized access" under the CFAA. The November 2010 edition of the Department of Justice's *Prosecuting Computer Crimes* manual describes several categories of cases that interpret this term. Your question concerns the most uncertain of these categories: where the defendant's action is not expressly prohibited, but the use is contrary to the implicit interests of the owner or operator of the computer system. Courts have reached different conclusions on whether criminal or civil liability is appropriate under the CFAA in this circumstance. *Compare Motorola, Inc. v. Lenko Corp.*, 609 F. Supp. 2d 760, 767 (N.D. Ill. 2009) (finding that an employee's "improper purpose" was sufficient evidence that the employee exceeded her authorization, even without an official policy in place), *with LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 n.7 (9th Cir. 2009) (stating in dicta that defendant does not "exceed authorized access" under the CFAA when he breaches a duty of loyalty to authorizing party). The Eleventh Circuit's ruling in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), sheds additional light on the dispositive impact of a guideline or policy that expressly prohibits a defendant's action. Further, the Ninth Circuit recently decided *United States v. Nosal*, 2011 WL 1585600 (9th Cir. 2011). The Department is still examining the ruling, and expects it to provide more guidance. As more prosecutions are brought under this clause of the CFAA, additional rulings should help to clarify the scope of this term.

We cannot comment on any ongoing cases or the precise facts that may be considered by prosecutors who might examine the CFAA in the context of smartphone application providers. Nevertheless, when deciding whether to bring an indictment under the CFAA, Department prosecutors consider a wide range of factors, including the particular facts involved, the law of

the applicable circuit and the actual conduct. When legal precedent is uncertain, the Department recommends that prosecutors proceed carefully and be guided by statutory language and their circuit's court rulings. The Department is continually providing guidance to prosecutors and seeking to promote greater clarity in the law, through ongoing training to Computer Hacking and Intellectual Property coordinators in U.S. Attorneys' Offices, publication of manuals such as the *Prosecuting Computer Crimes* manual mentioned above, and legal support to prosecutors as they apply the CFAA to emerging technologies and evolving methods of criminal conduct. To the extent that we identify gaps in the CFAA, we would be happy to work with your committee to identify and potentially correct them.

Additionally, the Department is working diligently with other parts of the Administration to develop proposals for amendments to the CFAA that will address the ongoing threat to our computer networks and the nation's cybersecurity needs. We hope to be able to share these proposals with Congress in the near future.

Second, your letter also asked the Department to update our *Prosecuting Computer Crimes* manual to clarify that the definition of "computer" under the CFAA includes many mobile and electronic devices beyond traditional computers, as the Eighth Circuit recently discussed in *United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011). Thank you for bringing this issue to our attention. This change will be included in the updates to the electronic edition of the manual that are currently underway.

Third, you asked about the resources that the Department of Justice has at its disposal to ensure the safety and privacy of American citizens. The Department relies on a robust set of legal, technological, and human resources, all of which are vital to the success of our mission. For more specific details of our needs for the coming year, we would direct you to the President's 2012 proposed budget, which outlines our detailed requests. In particular, the budget includes a request for funding for the Department to establish six International Computer Hacking and Intellectual Property ("ICHIP") attachés at embassies around the world. *Criminal Division FY 2012 President's Budget*, 19. Because computer crime is so often transnational in nature, it is vital that the Department of Justice have strong overseas representation to ensure that we can work more quickly and effectively with our international partners when investigating and prosecuting international computer crimes that target American citizens. The ICHIP program would establish Department of Justice representatives at hotspots for computer and intellectual property crime around the world, and would help ensure that we can continue to protect American citizens' privacy, both at home and abroad. We hope that Congress will provide the resources that we need to establish this program and expand our resources to fight international computer crime.

Finally, we would emphasize that the Department's investigations and prosecutions for privacy crimes often rely on lawful access to electronic evidence stored by communications providers. The Electronic Communications Privacy Act ("ECPA") governs this access. ECPA thus enables the government to investigate and prosecute hackers, identity thieves, and other online criminals. Only by ensuring that ECPA effectively and efficiently allows for lawful access to such records can the Department fulfill this important mission. We know that the Senate Judiciary Committee continues to examine this important issue, and we look forward to working with you and Congress to ensure that public safety and online individual privacy continue to be protected through ECPA's careful balances.

We hope this information is helpful. Please do not hesitate to contact this office if we may provide additional assistance regarding this or any other matter.

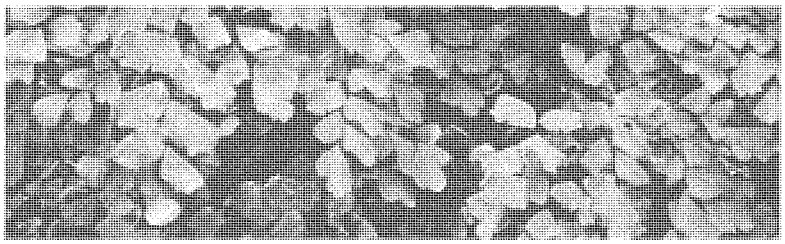
Sincerely,

Ronald Weich
Assistant Attorney General

Search

Alex Levinson

alex [dot] levinson [at] me [dot] com /// @alexlevinson



Home About Me

Next →

Posted on April 21, 2011 by alexlevinson

3 Major Issues with the Latest iPhone Tracking "Discovery"

UPDATE: http://alexlevinson.wordpress.com/2011/04/23/3-new-thoughts-on-mobile-location/

Today, two researchers for O'Reilly media published an article claiming discovery of a hidden tracking system on the iOS 4 operating system. Using simple techniques, Alasdair Allan and Pete Warden extracted data off of an iOS version 4 device and wrote an open source software utility to effectively graph this data onto a map. As a fellow researcher, I champion their creativity and their development. As an expert in this field, I have three points of argument to raise.

1) Apple is *not* collecting this data.

And to suggest otherwise is completely misrepresenting Apple. I quote:

> *Apple is gathering this data, but it's clearly intentional, as the database is being restored across backups, and even device migrations.*

Apple is not harvesting this data from your device. This is data on the device that you as the customer purchased and unless they can show concrete evidence supporting this claim – network traffic analysis of connections to Apple servers – I rebut this claim in full. Through my research in this field and all traffic analysis I have performed, not once have I seen this data traverse a network. As rich of data as this might be, it's actually illegal under California state law:

> *(a) No person or entity in this state shall use an electronic tracking device to determine the location or movement of a person.*

I don't think that's a legal battle Apple wants to face considering the sale of over 100 million iDevices worldwide. That raises the question – how is this data used? It's used all the time by software running on the phone. Built-In applications such as Maps and Camera use this geolocational data to operate. Apple provides an API for access to location awareness called Core Location. Here is Apple's description of this softare library:

> *The Core Location framework lets you determine the current location or heading associated with a device. The framework uses the available hardware to determine the user's position and heading. You use the classes and protocols in this framework to configure and schedule the delivery of location and heading events. You can also use it to define geographic regions and monitor when the user crosses the boundaries of those regions.*

Seems pretty clear. So now the question becomes why did this "hidden" file secretly appear in iOS 4?

2) This hidden file is neither new nor secret.

It's just moved. Location services have been available to the Apple device for some

time. Understand what this file is – a log generated by the various radios and sensors located within the device. This file is utilized by several operations on the device that actually is what makes this device pretty "smart". This file existed in a different form prior to iOS 4, but not in form it is today.

Currently, ***consolidated.db*** lies within the "User Data Partition" on the device. This is a logical filesystem that maintains non-system level privileges and where most of the data is stored. When you perform an iOS Backup through iTunes, it is backing up this partition. Prior to iOS 4, a file called ***h-cells.plist*** actually existed in the /root/Library/caches/locationd folder, but with hidden access from other software and applications. ***h-cells.plist*** contained much of the same information regarding baseband radio locations as ***consolidated.db*** does now, but in Apple Property List format rather than sqlite3. Through my work with various law enforcement agencies, we've used ***h-cells.plist*** on devices older than iOS 4 to harvest geolocational evidence from iOS devices.

So lets recap.

h-cells.plist = Pre iOS 4 / Radio Logs including Geolocational Data / Hidden from Forensic Extraction (usually)

consolidated.db = iOS 4+ / Radio logs including geolocational Data / Easily acquired through simple forensic techniques

The change comes with a feature introduced in iOS 4 – Mutlitasking and Background Location Services. Apps now have to use Apple's API to operate in the background – remember, this is not pure unix we're dealing with – it is only a logical multitasking through Apple's API. Because of these new APIs and the sandbox design of 3rd party applications, Apple had to move access to this data. Either way, it is not secret, malicious, or hidden. Users still have to approve location access to *any* application and have the ability to instantly turn off location services to applications inside the Settings menu on their device. That does not stop the generation of these logs, however, it simply prevents applications from utilizing the APIs to access the data.

3) This "discovery" was published months ago.

I understand that Mr. Allan and Mr. Warden are valued researchers for O'Reilly, but they have completely missed the boat on this one. In the spirit of academia,

due diligence is a must to determine who else has done such research. Mr. Allan, Mr. Warden, and O'Reilly have overlooked and failed to cite an entire area of research that has already been done on this subject and claimed full authorship of it. Let's break down my history:

Back in 2010 when the iPad first came out, I did a research project at the Rochester Institute of Technology on Apple forensics. Professor Bill Stackpole of the Networking, Security, & Systems Administration Department was teaching a computer forensics course and pitched the idea of doing forensic analysis on my recently acquired iPad. We purchased a few utilities and began studying the various components of apple mobile devices. We discovered three things:

- Third Party Application data can contain usernames, passwords, and interpersonal communication data, usually in plain text.
- Apple configurations and logs contain lots of network and communication related data.
- Geolocational Artifacts were one of the single most important forensic vectors found on these devices.

After presenting that project to Professor Stackpole's forensic class, I began work last summer with Sean Morrissey, managing director of Katana Forensics on it's iOS Forensic Software utility, Lantern. While developing with Sean, I continued to work with Professor Stackpole an academic paper outlining our findings in the Apple Forensic field. This paper was accepted for publication into the Hawaii International Conference for System Sciences 44 and is now an IEEE Publication. I presented on it in January in Hawaii and during my presentation discussed ***consolidated.db*** and it's contents with my audience – my paper was written prior to iOS 4 coming out, but my presentation was updated to include iOS 4 artifacts.

Throughout the summer, I worked extensively with Sean on both developing Lantern and writing custom software to interpret forensic data for customers of ours who needed better ways of searching for and interpreting data.

When the iPhone 4 came out, I was one of the first people in San Francisco to grab one (yes I waited to be in the front of that awful line).

— (Look for the RIT shirt)

Within 24 hours of the iPhone 4's release, we had updated Lantern to support forensic analysis of iOS 4.0 devices. Within 36 hours, we had began writing code to investigate ***consolidated.db.*** Once a jailbreak came out for iOS 4, I wrote a small proof of concept application to harvest the contents of consolidated.db and feed it to a server for remote location tracking.

Ever since then, location artifacts have been a main area of interest for me. I'm now the Lead Engineer for Katana Forensics leading all technical research and development of both Lantern and private utilities. I travelled to Salt Lake City, UT in November for the Paraben Forensics Innovation Conference (PFIC) and presented with Sean on iOS Forensics including the content of ***consolidated.db***. At that same conference, Sean and I announced the development of Lantern 2.0 which would fully support the interrogation of ***consolidated.db*** and other geolocational artifacts scattered throughout the device.

April 27, 2011 07:30am EST | 1 Comment

Most Mobile Apps Lack Privacy Policies: Study

By Mark Hachman 1 31

A study jointly performed by TRUSTe and Harris Interactive indicates that just 19 percent of the top 340 free applications contain a link to a privacy policy, a problem as mobile privacy issues come to the fore.

Over the past few days, the blogosphere has been consumed with whether or not the iPhone is tracking users, and even with location features turned off. The largest percentage (32 percent) of those surveyed by Harris/TRUSTe were iPhone owners, with 26 percent using BlackBerrys, 25 percent using Android phones, and 7 percent using Windows phones.

But app vendors can also collect their own information, and the Harris poll indicated that 74 percent of the 1000 smartphone users the poll surveyed indicated that they do not like advertiser tracking, 77 percent don't want to share their location with app owners, and that 85 percent would like the choice to opt in or opt out of targeted mobile ads.

"This survey makes it crystal clear that privacy concerns are a huge stumbling block to consumer

usage of applications and websites on smartphones," said *Fran Maier*, president and executive chair of TRUSTe. "As growth of the mobile market continues to surge, the industry needs a dedicated approach to educate consumers about how their data is being used and lets them make choices whether or not to engage. Overcoming consumer hesitancy and addressing increased lawmaker and regulator concerns require privacy practices that include notice and choice."

Half of those surveyed actually said they have read a mobile privacy policy; with 51 percent saying that they actively seek them out.

The poll also revealed that 98 percent of those polled consider having some access to mobile privacy controls is important, and 85 percent say they've restricted some type of mobile information sharing on mobile applications. Less than a third of those polled said that their smartphone alerts them when location information is collected.

About 37 percent of those surveyed said they would be willing to share information with an app vendor in exchange for a lower-cost app.

For more from Mark, follow him on Twitter @MarkHachman.

For the top stories in tech, follow us on Twitter at @PCMag.

We Recommend

Five Reasons Not to Buy an iPad 2

iPhone Users Are About to Be Screwed Over

iPhone 5G Sighting Shows Edge-to-Edge Screen

Infographic: The End of the Computer as We Know It

Report: Apple Planning Something Special for Apple Stores Anniversary

From Around The Web

ExxonMobil's earnings: The real story you won't hear in Washington *ExxonMobil's Perspectives*

Possible iPhone 5 pictures revealed *BGR.com*

Retire at age 66, or wait one more year? *BankRate.com*

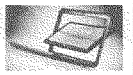
Hands On With The New Netflix App For Android Devices *ReelSEO*

iPad's New Nemesis *CNBC*

[what's this]

Inside PCMag

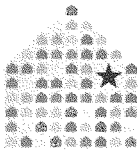
Don't Need A Chromebook



Very Cool Looking Laptops

Longest-Lasting Phones

PCMag's Guide to Security Software



NNEDV

The Testimony of
The National Network to End Domestic Violence
with The Minnesota Coalition for Battered Women

For the Hearing of the Senate Judiciary Committee
Subcommittee on Privacy, Technology and the Law
United States Senate
Protecting Mobile Privacy: Your Smartphones, Tablets, Cell Phones and Your Privacy

May 10, 2011

Introduction

Chairman Franken, Ranking Member Coburn, and distinguished Members of the Committee, the National Network to End Domestic Violence, on behalf of its member coalitions including the Minnesota Coalition for Battered Women, thanks you for the opportunity to submit testimony on this important issue. The National Network to End Domestic Violence (NNEDV) is a social change organization dedicated to creating a social, political, and economic environment in which violence against women no longer exists. Founded in 1990 and officially incorporated in 1995, NNEDV represents 56 state and territory domestic violence coalitions who in turn represent nearly 2,000 local domestic violence service providers across the country.

In 2002, NNEDV's Safety Net Technology Project was launched nationally to educate victims of stalking, sexual and domestic violence, their advocates and the general public on the strategic use of technology to increase personal safety and privacy. For the past nine years, the Safety Net Project has been providing training, education, support and technical assistance for domestic violence victims and their advocates as they navigate the benefits and challenges of the Internet and other forms of technology. One issue the Safety Net Project has long focused on is survivor safety and privacy in an increasingly networked and mobile world. The Safety Net Project provides ongoing trainings, tools, and advice that helps victims increase and maintain their online and mobile privacy when using social networking sites and location based and social location sharing services. We also train victim advocates, law enforcement, lawyers, prosecutors, and others how to recognize and hold abusers accountable when they misuse technology, such as global positioning system (GPS) or spyware programs, to monitor and stalk.

NNEDV works closely with our 56 member coalitions, including The Minnesota Coalition for Battered Women. The Minnesota Coalition for Battered Women is a well-established, membership organization with 83 local, regional, and national member programs located throughout Minnesota. The Coalition has existed for almost 30 years as the state's primary voice for battered women and has a strong history of effectively carrying out public policy that advances women's safety and security.

Minnesota has long been a leader in the domestic violence movement, especially with implementing legislative policy that supports and protects battered women and children. They were one of the first states to adopt a stalking statute in the early 1990s and most recently, the Coalition initiated and monitored the passage of several amendments to the stalking statute to update and increase protections for victims. A significant provision in this statute now includes the use of modern technologies being used as a means to stalk a victim. The Minnesota stalking statute (MN Stat §609/748 sudb. 2(6)) specifically states that it is a criminal act of stalking if a person "repeatedly mails or delivers or causes the delivery by any means, including electronically, of letters, telegrams, messages, packages, through assistive devices for the visually or hearing impaired, or any communication made through any available technologies or other objects". The Coalition supported the passage of this provision in 2010 because they received reports from battered women throughout the state that modern technology was being misused by abusers to stalk victims.

As we address the Committee's questions it is critical to point out that technology does not cause stalking. If a victim removes all technology from her life, her controlling abuser will simply resort to utilizing

For more information please contact: Cindy Southworth, Vice President of Development and Innovation
and founder of the Safety Net Technology Project at the National Network to End Domestic Violence
Web: www.nnedv.org/SafetyNetDocs Email: safetynet@nnedv.org Phone: 202-543-5566

non-technological means to harass, monitor, and stalk. However, since technology is prevalent in our lives, stalkers and abusers use this readily available tool to facilitate their harm and control. Abusive partners want control and power over the victim. In fact, the most dangerous time for a victim of domestic violence is when she takes steps to leave the abusive relationship.[1] Women who are separated from their abusive partners are 3 times more likely than women who are divorced and 25 times more likely than married women to be victims of violence at the hands of an intimate partner.[2] Many victims are stalked relentlessly for years after having escaped from their partners. Batterers who stalk their former partners are the most dangerous and pose the highest lethality risk.[3] In fact, 54% of femicide victims reported stalking behavior to the police before the victims were killed by their stalkers.[4] Eighty percent of women who are stalked by former husbands are physically assaulted by that partner and 30 percent are sexually assaulted by that partner.[5]

Stalking is an extremely dangerous event for victims and it can be equally dangerous for those around. The abuser who knows the location of a shelter program in which the victim is residing and seeking safety can target the entire shelter and put all the residents at serious risk of harm. The Minnesota Coalition for Battered Women recently surveyed their 83 member programs and received numerous accounts of how batterers misuse modern technology to further monitor, control, and intimidate women. Batterers misuse various forms of technology in conjunction with one another to optimize the level of control and power over their victims.

When victims are harmed by abusers who misuse technology, some people suggest that the victim get rid of the technology to prevent the stalking or harassment. For some victims who are in the process of planning to leave an abuser, changing phone numbers, getting rid of a cell phone, or discontinuing social networking or location sharing sites may actually increase suspicion by the abusive partner and increase the risk for violence. Sometimes when an abuser's ability to remotely track a victim is interrupted, the abuser escalates his violence in an attempt to regain control over the victim. There are additional reasons why "simply discontinuing" her use of technology might result in greater harm to a victim. For instance, many victims with disabilities use technology to decrease barriers, assist with activities in their daily lives and facilitate or enable communication with the outside world. In these instances, it may be impossible or very difficult for the victim to stop using the technology, despite the fact that the stalker might be misusing it to monitor or control her.[6]

Mobile Technology's Benefits to Victims

As technologies converge, mobile phones are able to do so much more for victims who are fleeing violence. Victims can use technology to call 911, take pictures of an abuser who violates a no-contact order, send and receive emails from supportive family member, search for help on the Internet, and map directions in real-time. This instant access to information has made it easier for victims of domestic violence to seek and find safety from abuse. From their mobile devices, victims can locate a domestic violence program in their community, reach out for support, find information about protection orders, and search for housing and employment opportunities. In addition, mobile devices have enabled survivors of abuse to stay in touch with their families and friends and find support in new communities, which often helps reduce isolation, an integral part of an abusive relationship. For people experiencing violence who are Deaf or have a disability, accessible mobile devices and relay services can decrease barriers and ensure access to help at crucial moments. For example, people who are Deaf can use a web browser or Instant Messaging program on a mobile phone to

---

[1] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).

[2] Ronet Bachman and Linda Salzman, Bureau of Justice Statistics, *Violence Against Women: Estimates From the Redesigned Survey* 1 (January 2000).

[3] Jacqueline Campbell, "Prediction of Homicide of and by Battered Women", *Assessing Dangerousness: Violence by Sexual Offender, Batterers, and Sexual Abusers* 96 (J. Campbell, ed., 1995). Also:
Barbara J. Hart, "Assessing Whether Batterers Will Kill,"(1990) Available at: http://www.mincava. umn.edu/ hart/lethali.htm),

[4] Judith McFarlane et al., "Stalking and Intimate Partner Femicide," *Homicide Studies* 3, no. 4 (1999).

[5] Center for Policy Research, *Stalking in America*, July 1997

[6] Fraser, C., Olsen, E., Lee, K., Southworth, C. and Tucker, S. (2010), The New Age of Stalking: Technological Implications for Stalking. Juvenile and Family Court Journal, 61: 39–55.

make calls via IP Relay to hotlines or 911. In summary, new technology and mobile technology can benefit many victims.

Cell phones can be a lifeline for battered women and victims of sexual assault and stalking. Enhanced 911 features of cell phones provide operators with critical location information of a victim. Cell phones have also been beneficial in helping victims and finding abusers. In 2005, a young woman in Maryland used text messaging to get help while being kidnapped by her ex-boyfriend. Hiding the phone between the passenger seat and the door, she texted her sister who called 911 and relayed the license plate number and other crucial information. The woman was rescued by New York police. [7]

In March 2011, a man was arrested for kidnapping his 4-year-old son outside of a domestic violence center, where, fearing for her safety, the boy's mother had gone to seek help in obtaining a restraining order. By quickly working with the man's cell phone service provider, police were able to track his movements based upon his cell phone signal. He was taken into custody without incident and the boy was returned to his mother. The man was jailed, charged for assault, and his estranged wife was granted a restraining order against him.[8]

Past Harm to Victims from Abusers and Stalkers who Misuse Mobile Technologies

Although it is obvious that mobile devices can be quite helpful they can also store or provide sensitive information about the user's activities, communications, and location. As technology evolves, stalkers and abusers quickly misuse it for nefarious purposes. Years ago, abusers who enforced rigid control over their victims' movements would check the odometer on the car to discover, by noting the excessive miteage, whether the victim had dared venture to the grocery store when the abuser had forbidden any trip beyond picking up the children at school. Enhanced technologies have provided more sophisticated tools for the same behaviors and crimes.

In a recent case in Northern St. Louis County, MN, an advocate reported that a woman who entered the domestic violence program located within a county building received a text message from her abuser within five minutes of entering the building. The abuser asked why she was in the county building. The woman was extremely frightened and the advocate helped her obtain an Order for Protection (OFP) at the local courthouse. After filing the OFP, the woman received another text message asking why she went to the courthouse and if she was filing an OFP against him. The only device the woman had on her was her smart phone and they later concluded that her abuser was tracking her via a location tracking application or service on her phone.

In another situation in Minnesota, an immigrant woman from Thailand who sought emergency housing in a metro area domestic violence shelter discovered that her American citizen husband had used a location tracking application or service on her phone to monitor and control her whereabouts. The Thai woman came to America with a limited understanding of the American judicial system and spoke very little English. Her only family in the United States was her husband who was physically, emotionally and psychologically abusive towards her. He even went so far as to apply for an Order for Protection against his Thai wife in order to further manipulate and control her. Finally, through the police, she was able to escape her abusive husband and seek shelter at the local domestic violence program. While staying at the shelter, her abusive husband sent her text messages asking why she was there and told her to come home. He woutd call taxi cabs to wait for her outside of the shelter at all hours of the day until she was relocated to another location. The Thai woman did not know her husband used her cell phone to monitor her whereabouts but she did suspect he was monitoring her. It seemed too coincidental that he would randomly show up at places where she was going or he would know where she had been during the day. It wasn't until she arrived at the shelter that she realized her abusive husband was using an application on her cell phone to track her. Battered women who are limited English

[7] Lee, Jennifer. "Cellphone Messages Lead Police to Abducted Maryland Woman." *The New York Times - Breaking News, World News & Multimedia*. 11 June 2005. Web. 26 Apr. 2011. <http://www.nytimes.com/>.
[8] Terry, Lynne. "Washington Police Used Cell Phone Pings to Zero in on Fugitive in Amber Alert." *Oregon Local News, Breaking News, Sports & Weather - OregonLive.com*. 2 Mar. 2011. Web. 26 Apr. 2011. http://www.oregonlive.com/pacific-northwest-news/index.ssf/2011/03/washington_police_used_cell_phone_pings_to_zero_in_on_fugitive_in_amber_alert.html

proficient (LEP) are often some of the most vulnerable battered women and they need additional safeguards to protect them against abusers.

In 2004, a stalker in California purchased a cell phone with location tracking service expressly for the purpose of tracking his ex-partner. He attached the cell phone to the underside of her car and was only caught when the victim saw him under her car changing the cell phone's battery.[9] Numerous cases of GPS stalking have arisen since then. In 2010, an Arizona man stalked his wife using a location service before allegedly murdering their two children and shooting himself.[10] In 2009, in Seattle, a man used the location service on his estranged wife's phone to track her to a local store. After finding her speaking to a man there, he shot and killed their five children and himself.[11]

It is difficult to determine the prevalence of cases involving misuse of mobile technology. Although research is beginning to emerge, victims of stalking often do not know all of the methods a statker uses to gain information. Victims' unsubstantiated reports are tikely to be disbelieved and offenders are unlikely to disclose their illegal stalking tactics. Additionally, many stalking cases are never reported to law enforcement, so reliance on police reports will, again, provide an underestimate. Research from data collected in 2006 shows that more than 1 in 4 stalking victims reported that their statker used some form of technology to stalk them.[12] Of those who were aware and able to report being stalked electronically, 83 percent reported being stalked by email or instant messaging. Additionally, 46 percent reported that the stalker used a camera to monitor their actions, and 10 percent reported that GPS technology was used to monitor them.[13] With the growing use of mobile location-based services, it is our experience that perpetrators are location-tracking victims more often and in increasingly varied ways. Paradoxically, when crimes are committed using digital technology, there is often digital evidence that can assist in investigating and prosecuting the abusers.

Harm to Victim from Abusers and Stalkers who Misuse Mobile Technologies

This committee has expressed an interest in learning about location tracking through mobile devices and location-based services used in mobile phones and other devices. As mentioned earlier, mobile devices that have location services can be quite helpful, particularly in cases where law enforcement can use that information to locate someone who dials 911 or is missing. For victims, GPS-enabled mobile devices allow them to use applications that list nearby shopping, hospitals or police stations, provide quick real-time directions, and more. However, the location capability of GPS also has risks when it is misused.

Stalkers may misuse technology and enable location products offered through a wireless phone service provider or install location tracking applications onto GPS-enabled cell phones.. Generally, locator services provided directly from a cell phone carrier as part of a family plan require some level of authorization to access the victim's account and activate the service. Unfortunately, since most stalkers are former intimate partners, it is sometimes possible for them to find a way to impersonate the victim, access the account, and add these optional location services. Most cell phone carriers, however, have added extra authentication and verification steps, such as automatically sending a text message to the phone informing them that a tracking application or service has been enabled. For this reason, stalkers may favor third-party location tracking applications (available in some app stores or via Internet) because some of these tracking applications and services do not provide as much notice to the consumer or verification that consent to track has been obtained. There are ways stalkers can install a location-tracking application on to the victim's phone without the victim's knowledge. Depending on the type of application, the stalker can then monitor the location of the victim's phone via a website or his cell phone to monitor the real-time or historical movement of the victim's phone.

---

[9] Boghossian, N. (2004, September 4). High-tech tale of stalking in the 21st century. *LA Daily News*, p.N1

[10] Scheck, Justin. "Stalkers Exploit Cellphone GPS." *Business News, Finance News, World, Political & Sports News from The Wall Street Journal - Wsj.com.* 3 Aug. 2010. Web. 26 Apr. 2011.
<http://online.wsj.com/article/SB10001424052748703467304575383522318244234.html>.

[11] Ibid.

[12] Baum, K., Catalano, S., Rand, M., & Rose, K. (2009, January). Stalking Victimization in the United States. *Bureau of Justice Statistics Special Report. NCJ 224527.* 1-15.

[13] Ibid.

Another method in which an abuser may attempt to discover sensitive victim information is through call history and other data collected by cell phone service providers and devices. Risks regarding information stored on the device is highest for victims who have not yet fled and have regular contact with the abuser who can, with physical access to the phone, track the extent to which victims may be reaching out for help and trying to plan an escape. The location data collected by cell phone service providers is not typically accessible to the general public. Generally law enforcement must subpoena the cell phone provider for that information.

Sometimes, the mobile device stores location information. For example, certain iPhone and iPad devices may automatically store a file with historical location information of the Wi-Fi hotspots and cell towers nearest where you have been. When this historical data is viewed by an abuser, there is a risk that an abusive partner could use this file to see where the victim has been. It is yet unclear all the ways a technology-savvy abuser might attempt to misuse this data, however the information in this file might provide information about where the victim has been going versus real-time location tracking of the victim. For example if a victim is secretly visiting a domestic violence center but told her abuser that she was across town at the library, the historical location information might alert the abuser to her plans to leave. While this sort of location information on a device can reveal information the victim wants to hide from her abuser, if an abuser is monitoring and controlling the victim to that extent, it is unfortunately likely that the abuser is also using other technologies to control and monitor the victim possibly even including spyware or keystroke loggers on the victim's home computer or smart phone.

As technologies converge, and voice, data, and location are offered by one mobile device, the information these devices collect and store can be revealing. At the same time, some benefits of this technological convergence can be helpful for survivors seeking to use their mobile device to call for help, search the Internet for critical legal information, and use location services to identify the nearest police department. To support the privacy of all consumers, including the safety of victims, it is critical that companies be transparent about what data is being collected, when it is collected, what application or service is using the data, who the data is shared with, and how long the data is stored. Companies must also allow consumers to choose what information can or cannot be collected and with whom that information will or will not be shared.

Protecting Victims

To increase victim safety and privacy, whenever possible, NNEDV works with an impressive array of technology companies to incorporate privacy features into their products. Many technology companies, including AOL, Facebook, Google, Loopt, Microsoft, Twitter and Verizon, have proactively solicited NNEDV's input and feedback before releasing new products. Apple recently contacted NNEDV and we hope that Apple will continue to work with us to increase privacy for all consumers including enhanced safety for victims.

NNEDV has worked closely with wireless phone carriers such as Verizon and third-party Location Based Service (LBS) applications such as Loopt and Google Latitude to ensure that an abuser cannot turn on a location tracking service on the victim's phone without the victim's knowledge. With special consideration to victim safety, some third-party location-sharing applications even allow a victim to manually set her location so if her abuser forces her to share her location while she is still in the relationship and risking violent retribution, she can manually set a false location and then secretly travel to meet with a victim advocate, a police officer or an attorney.

In this digital age, any company that is rolling out services that use a consumer's personally identifiable information or location should proactively identify and address risks for victims of domestic and sexual violence, stalking and abuse. This is not only good business but it can save lives. For example, since 2007, NNEDV has worked with Google to ensure that the confidential addresses of domestic violence shelters are removed from Google's Street View and the Google Maps application. NNEDV has also assisted Verizon, Google, Loopt and other companies in working to prevent stalkers and abusers from misusing products and in creating user privacy and notification options for location-based services and other products. We welcome

further opportunities to assist Apple and other companies on mobile privacy options that enhance the privacy of all consumers, especially those with heightened safety concerns.

Technology companies that develop location tracking tools or applications that rely on location tracking to improve their functionality or speed can help protect victims by ensuring that the consumer has notice of the information collected, whether that information is transmitted in real-time, and the length of time for which location information is retained. To best protect victims, and comply with industry standards, cell phone service providers, application developers, and device manufacturers should follow the Wireless Association's (CTIA) *Best Practices and Guidelines for Location Based Services*.[14] These guidelines "rely on two fundamental principles: user notice and consent."[15]

Users should be informed about how their location information will be used, disclosed and shared. This process should be prominent, transparent, and easy to understand. As noted in CTIA's *Guidelines*, "Any notice must be provided in plain language and be understandable. It must not be misleading, and if combined with other terms or conditions, the LBS portion must be conspicuous."[16] Knowing how and when their location information (via mobile device) is gathered and shared will help empower victims to develop strategies to minimize their vulnerability and determine whether or not it is safe to carry their mobile phone and/or to purchase a new pre-paid phone that will provide greater privacy and safety.

Users must have the opportunity to actively and meaningfully consent to the use, disclosure, or sharing of their location information. Meaningful consent must be prominent, succinct, and very easy to navigate. "Pre-checked boxes that automatically opt users in to location information disclosure, or, choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement ordinarily would be insufficient to express user consent."[17] Consent is especially critical when the product or application does not require location information in order to function. For example, some mobile internet browsers may retain location information regarding past wireless access points users have accessed. This may allow the device to more quickly access wireless internet in the future, when an individual returns to that location. However, this is not critical to the functioning of the device. The device can search anew for internet access each time the user visits that physical location. While this will take more time, some consumers would prefer an increased wait time to having the device maintain unencrypted location log files. This may be true for victims of stalking and domestic violence, who have very real concerns about their personal safety.

Consumers can only truly consent when they have been provided with enough information to gain a full understanding of the collection, transmission, and retention practices and policies of the applications and services they use. As CTIA's *Guidelines* suggest, "All entities involved in the delivery of LBS, including wireless carriers, device manufacturers, operating system developers, application aggregators and storefront providers, should work to educate users about the location capabilities of the devices, systems, and applications they use as well as to inform them of the various privacy protections available."[18] When consumers understand all elements of their devices and applications, they can make fully informed decisions that may enhance the privacy of many users and increase the safety of some especially vulnerable consumers, including battered women and consumers with low literacy and/or limited English proficiency.

When developing products that may track or share location or other sensitive information, device manufacturers and application developers should consider and proactively address and minimize potential misuses of their product. They should consult with organizations, such as NNEDV and its member coalitions, that work with victims to determine how similar products have been misused in the past and work closely with technology companies to identify low cost, but high impact notifications which might alert a victim to monitoring or stalking. Relatively simple safeguards can be added to help prevent misuse of the product and unauthorized

[14] CTIA. *Best Practices and Guidelines for Location Based Service*. Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf
[15] Ibid.
[16] Ibid.
[17] CTIA. *Best Practices and Guidelines for Location Based Service*. Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf
[18] Ibid.

access to information. For location-based services, this could take the form of periodic text messages, splash notification, or an ever-present icon to notify and remind the user that a tracking application is on the device. It can also take the form of a central transparent place to view all device features and additional applications that are requesting use of your mobile phone's location. The iPhone, for example, lists all applications (e.g. Camera, Maps, Loopt, Foursquare, Twitter, Yelp, Dictionary, etc.) that want to use location services and provides the user with an easy way to turn the location services on or off for the entire phone or for any individual application. Robust verification and authentication processes will also help prevent illegitimate access to information.

Finally companies should develop processes that will respond to and support victims quickly when technology is being misused by abusers or stalkers to harm. Companies should create an accessible and responsive process that provide clear and quick information to users about how their technology works, how to work with either the company or law enforcement to stop the abusive behavior, and resources that can provide assistance to victims.

Conclusion

Mobile devices have, undeniably, become an amazing safety tool for victims of violence and stalking. Knowing that one can summon help with the press of a single key can provide incredible peace of mind to a victim of stalking or abuse. Unfortunately, mobile devices can also be misused by abusers to stalk, monitor, and locate victims. By working together with groups like NNEDV to protect those most vulnerable to misuse of their location and personally identifiable data, a variety of companies in the mobile industry have demonstrated a commitment to minimizing any possible risks and maximizing benefits for all consumers are fully considered. NNEDV recommends first, that all mobile providers and application developers follow the Wireless Association's (CTIA) *Best Practices and Guidelines for Location Based Services*[19] and second, that companies work proactively with organizations such as NNEDV that specialize in addressing how technology impacts victims to anticipate and address potential harms before they ever occur. When companies proactively design safety and privacy options into their products and services with victims clearly in mind, they help victims of domestic violence, sexual violence and stalking stay alive and be better protected, and they prevent abusers and stalkers from easily misusing their products to further perpetrate abuse and harm. Designing privacy, notice and consent into mobile devices, applications and services that use location or personally identifiable data will keep us all – victims, the victim's family and friends, police officers, and community members – safer. It is good business and it may save lives.

[19] CTIA. *Best Practices and Guidelines for Location Based Service*. Volume 2.0. March 23, 2010. Available at: http://files.ctia.org/pdf/CTIA_LBS_Best_Practices_Adopted_03_10.pdf

nielsenwire

- Consumer
- Featured Insights
- Global
- Media + Entertainment
- Online + Mobile

nielsen.com | contact us | careers

- Reports + Downloads

Home » Nielsen News, Online + Mobile

Print
View Comments
ShareThis

Search the archive...

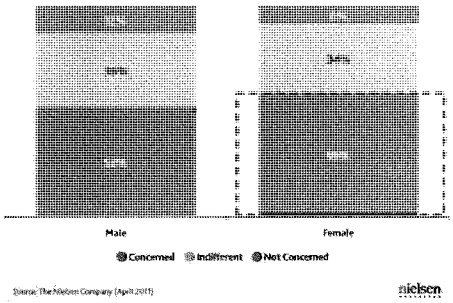
Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location

April 21, 2011

More and more mobile applications allow consumers to share information about where they are by voluntarily "checking in" to a location or by having their GPS-enabled smartphone automatically transmit that information via the app. Some marketers reward consumers for sharing their location with loyalty points, discount coupons for nearby businesses, or other promotional "badges" and benefits.

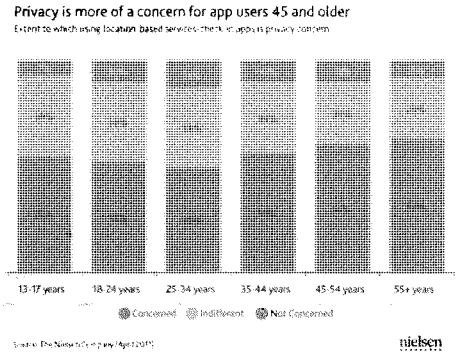
But despite the growing popularity of check-in services in the U.S., there are still many who are reticent to share information about their geographic location. According to The Nielsen Company's latest research on mobile applications, most mobile app downloaders, which Nielsen defines as those mobile subscribers who have downloaded an application in the past 30 days, are concerned about privacy when it comes to sharing their location via mobile phone. This concern is more pronounced among women app downloaders, with 59 percent reporting they have privacy concerns compared to 52 percent of male app downloaders.

Female app users are more concerned about privacy



Source: The Nielsen Company (April 2011)

Age is a factor as well. Mobile app downloaders between the ages of 25-34 were the least likely to have privacy concerns. Privacy concerns were considerably higher among those over the age of 45.



As consumers become increasingly familiar with location-based apps, and as marketers earn their trust and become more savvy about understanding what benefits consumers expect in exchange for that information, consumers will become more comfortable with the idea of location-based mobile applications.

Jonathan Carson, CEO, Telecom, at The Nielsen Company, will be sharing these and other insights on consumers and mobile apps at the upcoming AppNation conference in San Francisco on April 27.

For more: Contact The Nielsen Company or read about our global practices.

Tags: location-based services, mobile apps, privacy, smartphones

Related Posts

- Insights on the Emerging Mobile App Economy
- Consumers and Mobile Apps in the U.S.: All About Android and Apple iOS
- U.S. Parents Say Almost A Third of the Apps on Their Phone Were Downloaded by Their Children
- Number of Americans Watching Mobile Video Grows More than 40% in Last Year
- How to Succeed in Russia

2 people liked this.

Add New Comment

Login

Showing 3 comments

Sort by newest first

Aca

How large is the sample size?

Lynn

Especially interesting given recent news that security researchers said they found a file hidden in the operating software of iPhones and iPads that can contain

tens of thousands of records of a user's precise geographical location, each marked with a timestamp. http://abcnews.go.com/Technolo...

Maximilian Weigl

Then you should definitely be interested in what Google's Android is doing with your location data: http://online.wsj.com/article/...

Subscribe by email + RSS

Reactions

edolinski via twitter

Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location: http://ow.ly/4GDbM

6 days ago

jeanmanolo via twitter

Shhhhhhhhhhhhh!! Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location http://t.co/SplCQnh #latism

1 week ago

ThitMat17 via twitter

The biggest problem with adopting location-based apps remains privacy. Nielsen recent survey of US app downloaders http://bit.ly/enhCHT

1 week ago

LocalSearchAds via twitter

Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location | Nielsen Wire - http://shar.es/H7Rfv

1 week ago

OnlineAdAssoc via twitter

Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location | Nielsen Wire http://t.co/TgyNIPV

1 week ago

miriammolina1 via twitter

Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location | Nielsen Wire http://t.co/QtvENFL

1 week ago

DOMSET via twitter

Schreckgespenst Location Based Services: Viele fürchten um ihre Privatsphäre, wenn sie #Apps mit Geodiensten nutzen: http://dld.bz/Ye6v

1 week ago

Uber_RICH via twitter

RT @nielsenwire: Privacy Please! U.S. Smartphone App Users Concerned with Privacy When it Comes to Location http://t.co/3wjoYn3

3 weeks ago

The_ARF via twitter

Apple, listening? RT @xplusone: #privacy study, "59% of female app DLers report privacy concerns compared to 52% of males http://ow.ly/4EW20

3 weeks ago

gemamora via twitter

Privacy please! U.S. Smartphone APP users concerned with privacy when it comes to location http://bit.ly/enhCHT

3 weeks ago

Show more reactions

blog comments powered by DISQUS

Recommend 9K

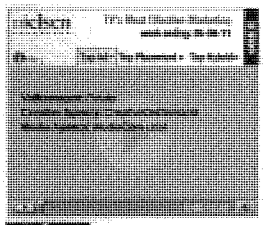
Enter Email For Updates Subscribe

Weekly Monthly

Monthly Archive

Select Month

Top Ads



- About
- Careers
- Privacy Policy
- Contact

Most Commented

- Twitter Quitters Post Roadblock to Long-Term Growth
- Teens Don't Tweet; Twitter's Growth Not Fueled By Youth
- Twitter's Tweet Smell Of Success
- Global Advertising: Consumers Trust Real Friends and Virtual Strangers the Most
- Social Networking's New Global Footprint
- Social Media: The Next Great Gateway for Content Discovery?
- Top Mobile Phones, Sites and Brands for 2009
- Time Spent on Facebook up 700%, but MySpace Still Tops for Video
- Americans Watching More TV Than Ever; Web and Mobile Video Up too
- Is Social Media Impacting How Much We Email?

Nielsen In The News

- In Shift, Ads Try to Entice Over-55 Set (NY Times)
- Bad News for Small-Towners Seeking Daily Group Deals (Ad Age)
- China Sets Pace in Brand Innovation (Financial Times)
- Ownership of TV Sets Falls in US (NY Times)
- U.K. Royal Wedding Draws 22.8 Million Viewers on U.S. Networks (Bloomberg)
- Media circus lured by royal nuptials (Financial Times)
- Media's Ageing Audiences (The Economist)
- Ford revives trading advertising (Detroit Free Press)
- China consumer goods: Left on the shelf (Financial Times)
- Global Advertising Spending Rose in 2010 (Bloomberg)

© 2011 The Nielsen Company. All Rights Reserved. Terms of Use | Privacy Policy

Are We In a Bull Market?

If you have a $500,000 portfolio, you should download the latest report by *Forbes* columnist Ken Fisher's firm. It tells you where we think the stock market is headed and why. This must-read report includes our latest stock market prediction, plus research and analysis you can use in your portfolio right now. ▸ Click Here to Download

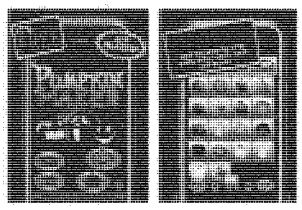
FISHER INVESTMENTS

THE WALL STREET JOURNAL.
WSJ.com

DECEMBER 19, 2010, 8:42 PM ET

How One App Sees Location Without Asking

One advertising company has found a way to estimate the location of iPhone app users without notifying them, a Wall Street Journal investigation revealed.



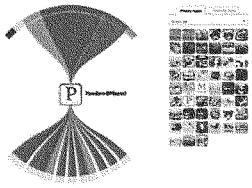
Screen shots from Pumpkin Maker's page in the iTunes Store.

That's not supposed to happen. Apple Inc. requires users to agree before apps can tap the phone's location. Apple declined to comment.

The Journal discovered the apparent discrepancy when it tested the iPhone app Pumpkin Maker. The pumpkin-carving app transmitted the location of the Journal's test phone without asking permission.

The app's maker, Anthony Campiti, says he inserted a software "kit" from an advertising network, Greystripe Inc. That's a common practice among app makers, who use these ready-made kits to place ads and generate revenue. Some apps use multiple kits; one of the 101 iPhone and Android apps tested by the Journal sent information to eight ad networks.

Explore the Data



What They Know

See more about privacy on phones from the Wall Street Journal's series on Internet-tracking technology.

- **Your Apps Are Watching You**
- **What Can You Do? Not Much**
- **The Journal's Cellphone Testing Methodology**
- **What Settings to Look for in Apps**
- **Unique Phone ID Numbers Explained**
- Follow **@whattheyknow** on Twitter

Greystripe Chief Executive Michael Chang says his company's software located the phone by identifying its Internet address. That's common among websites, less so on mobile devices. Most apps use Global Positioning System satellites or maps of Wi-Fi hot spots to locate users.

Greystripe's method wasn't particularly precise. The app reported latitude and longitude coordinates about three miles from the Denver office of the Journal's contractor. Other apps tested by the Journal located a phone within 25 feet.

Mr. Chang says Greystripe's method does not violate Apple's rules because it doesn't use the GPS system or other location information from the phone itself. He says Greystripe takes user privacy "extremely seriously."

It's unclear how widespread this practice may be. Pumpkin Maker was the only app tested by the Journal that reported latitude and longitude coordinates without asking a user's permission to tap location. It was also the only app that sent data to Greystripe. Mr. Chang says Greystripe also uses Internet addresses to locate phones using Google's Android operating system.

A handful of other iPhone apps tested by the Journal transmitted more general locations, such as Denver, or a zip code. It was often

not clear where the app obtained the city or zip code information.

Mr. Campiti, Pumpkin Maker's developer, says he wasn't aware of Apple's policy requiring user permission for tapping the phone's location "because we don't do that." Mr. Campiti says Greystripe's technique is acceptable because "they need to be able to do that to effectively advertise."

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

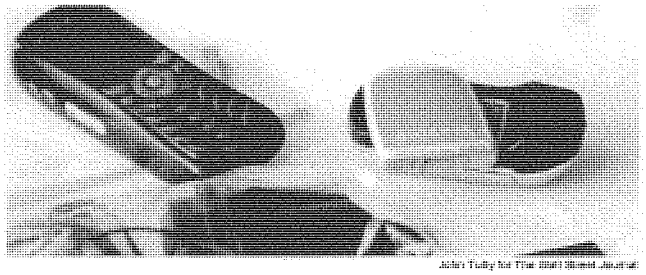
See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

WHAT THEY KNOW | AUGUST 3, 2010

Stalkers Exploit Cellphone GPS

By JUSTIN SCHECK



Cellphones of domestic-abuse victims staying at A Safe Place in New Hampshire are taken apart to disable their tracking systems.

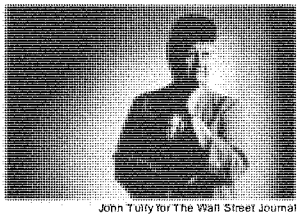
Phone companies know where their customers' cellphones are, often within a radius of less than 100 feet. That tracking technology has rescued lost drivers, helped authorities find kidnap victims and let parents keep tabs on their kids.

But the technology isn't always used the way the phone company intends.

One morning last summer, Glenn Helwig threw his then-wife to the floor of their bedroom in Corpus Christi, Texas, she alleged in police reports. She packed her 1995 Hyundai and drove to a friend's home, she recalled recently. She didn't expect him to find her.

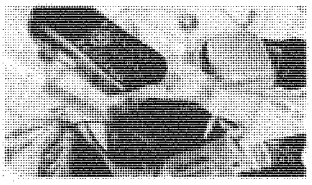
The day after she arrived, she says, her husband "all of a sudden showed up." According to police reports, he barged in and knocked her to the floor, then took off with her car.

The police say in a report that Mr. Helwig found his wife using a service offered by his cellular carrier, which enabled him to follow her movements through the global-positioning-system chip contained in her cellphone.



John Tully for The Wall Street Journal

Marsie Silvestro, who runs battered-women shelters, says tracking is a problem.



Technology is enhancing the reach of stalkers, allowing them to take advantage of location-based social networking applications. WSJ's Andy Jordan reports.

Mr. Helwig, in an interview, acknowledged using the service to track his wife on some occasions. He says he signed up for the tracking service last year. "AT&T had this little deal where you could find your family member through her cellphone," he says. But he didn't use it to find his wife that day, he says. Mr. Helwig, who is awaiting trial on related assault charges, declined to comment further about the matter. He has pleaded not guilty.

The allegations are a stark reminder of a largely hidden cost from the proliferation of sophisticated tracking technology in everyday life—a loss of privacy.

Global-positioning systems, called GPS, and other technologies used by phone companies have unexpectedly made it easier for abusers to track their victims. A U.S. Justice Department report last year estimated that more than 25,000 adults in the U.S. are victims of GPS stalking annually, including by cellphone.

In the online world, consumers who surf the Internet unintentionally surrender all kinds of personal information to marketing firms that use invisible tracking technology to monitor online activity. A Wall Street Journal investigation of the 50 most-popular U.S. websites found that most are placing intrusive tracking technologies on the computers of visitors—in some cases, more than 100 tracking tools at a time.

The cellphone industry says location-tracking programs are meant to provide a useful service to families, and that most providers take steps to prevent abuse. Mike Altschul, chief counsel for wireless-telecommunications trade group CTIA, says recommended "best practices" for providers of such services include providing notification to the person being tracked.

Mr. Helwig's wife had received such a notification, by text message, from AT&T. A spokesman for AT&T Inc. says it notifies all phone users when tracking functions are activated. But users don't have the right to refuse to be tracked by the account holder. Turning off the phone stops the tracking.

Dig Deeper

Graphic: A locator map provided to a user of AT&T's FamilyMap program

On Web's Frontier, Anonymity in Name Only

Follow **@whattheyknow** on Twitter

Digits: Info Needed to Identify You: 33 Bits

Personal Details Exposed Via Biggest U.S. Websites

The Journal's Methodology

What They Know About You

Explore the Data

Digits: Your Questions on Digital Privacy

Digits: Analyzing What You Have Typed

Digits: Lawsuit Tackles Files That 'Re-Spawn' Cookies

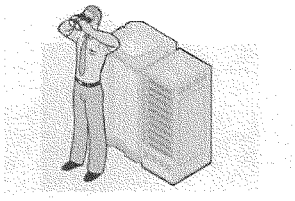
Full Coverage: wsj.com/WTK

Glossary

Cellphone companies will deactivate a tracking function if law-enforcement officials inform them it is being used for stalking. Mr. Altschul says authorities haven't asked carriers to change their programs. He adds that carriers have long supported programs to give untraceable cellphones to domestic-violence victims.

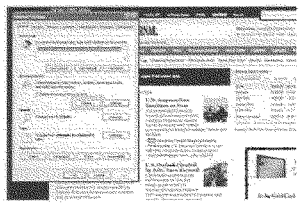
In Arizona this year, Andre Leteve used the GPS in his wife's cellphone to stalk her, according to his wife's lawyer, Robert Jensen, before allegedly murdering their two children and shooting himself. Mr. Jensen says Mr. Leteve's wife, Laurie Leteve, didn't know she was being tracked until she looked at one of the family's monthly cellphone bills, more than 30 days after the tracking began. Mr. Leteve, a real-estate agent, is expected to recover. He has pleaded not guilty to murder charges, and is awaiting trial. The law firm representing him declined to comment.

Key tracking terminology



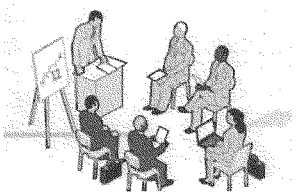
How to Protect Yourself

Almost every major website you visit is tracking your online activity. Here's a step-by-step guide to fending off trackers.



The Tracking Ecosystem

Surfing the Internet kickstarts a process that passes information about you and your interests to tracking companies and advertisers. See how it works.



Back Next

In a suspected murder-suicide last year near Seattle, a mechanic named James Harrison allegedly tracked his wife's cellphone to a store. After he found her there with another man, he shot to death his five children and himself, according to the Pierce County Sheriff's Office.

Therapists who work with domestic-abuse victims say they are increasingly seeing clients who have been stalked via their phones. At the Next Door Solutions for Battered Women shelter in San Jose, Calif., director Kathleen Krenek says women frequently arrive with the same complaint: "He knows where I am all the time, and I can't figure out how he's tracking me."

In such cases, Ms. Krenek says, the abuser is usually tracking a victim's cellphone. That comes as a shock to many stalking victims, she says, who often believe that carrying a phone makes them safer because they can call 911 if they're attacked.

There are various technologies for tracking a person's phone, and with the fast growth in smartphones, new ones come along frequently. Earlier this year, researchers with iSec Partners, a cyber-security firm, described in a report how anyone could track a phone within a tight radius. All that is required is the target person's cellphone number, a computer and some knowledge of how cellular networks work, said the report, which aimed to spotlight a security vulnerability.

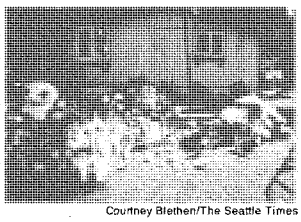
The result, says iSec researcher Don Bailey, is that "guys like me, who shouldn't have access to your location, have it for very, very, very cheap."

That is, in part, an unintended consequence of federal regulations that require cellphone makers to install GPS chips or other location technology in nearly all phones. The Federal Communications Commission required U.S. cellular providers to make at least 95% of the phones in their networks traceable by satellite or other technologies by the end of 2005. The agency's intention was to make it easier for people in emergencies to get help. GPS chips send signals to satellites that enable police and rescue workers to locate a person.

To a large extent, that potential has been fulfilled. Last year, for example, police in Athol, Mass., working with a cellphone carrier, were able to pinpoint the location of a 9-year-old girl who allegedly had been kidnapped and taken to Virginia by her grandmother. In December, police in Wickliffe, Ohio, tracked down and arrested a man who allegedly had robbed a Pizza Hut at gunpoint by tracking the location of a cellphone they say he had stolen.

Mr. Altschul, of the cellphone-industry trade group, says the tracking technology has been of great help to both law-enforcement officials and parents. "The technology here is neutral," he says. "It's actually used for peace of mind."

But as GPS phones proliferated, tech companies found other uses for the tracking data. Software called MobileSpy can "silently record text messages, GPS locations and call details" on iPhones, BlackBerrys and Android phones, according to the program's maker, Retina-X Studios LLC. For $99.97 a year, a person can load MobileSpy onto someone's cellphone and track that phone's location.



Courtney Blethen/The Seattle Times

A memorial near Seattle for five children murdered by their father, who then killed himself, after tracking his wife by cellphone.

Craig Thompson, Retina-X's operations director, says the software is meant to allow parents to track their kids and companies to keep tabs on phones their employees use. He says the company has sold 60,000 copies of MobileSpy. The company sometimes gets calls from people who complain they are being improperly tracked, he says, but it hasn't been able to verify any of the complaints.

Installing such programs requires a person to physically get hold of the phone to download software onto it.

GPS-tracking systems provided by cellular carriers such as AT&T and Verizon Communications Inc. are activated remotely, by the carriers.

Domestic-violence shelters have learned the consequences. As soon as victims arrive at shelters run by A Safe Place, "we literally take their phones apart and put them in a plastic bag" to disable the tracking systems, says Marsie Silvestro, director of the Portsmouth, N.H., organization, which houses domestic-violence victims in secret locations so their abusers can't find them.

The organization put that policy in place after a close call. On Feb. 26, Jennie Barnes arrived at a shelter to escape her husband, Michael Barnes, according to a police affidavit filed in a domestic-violence case against Mr. Barnes in New Hampshire state court. Ms. Barnes told police she was afraid that Mr. Barnes, who has admitted in court to assaulting his wife, would assault her again.

Ms. Barnes told a police officer that "she was in fear for her life," according to court filings. The next day, a judge issued a restraining order requiring Mr. Barnes to stay away from his wife.

Later that day, court records indicate, Mr. Barnes called his wife's cellular carrier, AT&T, and activated a service that let him track his wife's location. Mr. Barnes, court records say, told his brother that he planned to find Ms. Barnes.

The cellular carrier sent Ms. Barnes a text message telling her the tracking service had been activated, and police intercepted her husband. Mr. Barnes, who pleaded guilty to assaulting his wife and to violating a restraining order by tracking her with the cellphone, was sentenced to 12 months in jail. A lawyer for Mr. Barnes didn't return calls seeking comment.

Another source for cellphone tracking information: systems meant to help police and firefighters. Some cellular carriers provide services for law-enforcement officers to track people in emergencies. Using such systems requires a person to visit a special website or dial a hot-line number set up by the carrier and claim the data request is for law-enforcement purposes.

Cellular carriers say they try to verify that callers are legitimate. An AT&T spokesman says an office is manned around the clock by operators who ask for subpoenas from law-enforcement officials using the system.

But federal law allows carriers to turn over data in emergencies without subpoenas. Al Gidari, a lawyer who represents carriers such as Verizon, says such location-tracking systems can be easy to abuse. Police, he says, often claim they need data immediately for an emergency like a kidnapping, and therefore don't have time to obtain a warrant, in which a judge must approve an information request.

In Minnesota, Sarah Jean Mann claimed last year in a county-court petition for a restraining order that her

estranged boyfriend, a state narcotics agent, followed her by tracking her cellphone and accessing her call and location records through such a system. The court issued the restraining order. The boyfriend, Randy Olson, has since resigned from the police force. He didn't respond to calls seeking comment.

Mr. Gidari says law-enforcement's easy access to such data makes the systems easy to abuse. He says carriers would like to have a system in place requiring agents to get warrants. Without such a requirement, there is little carriers can do to resist warrantless requests, say Mr. Gidari and Mr. Altschul of trade group CTIA. Federal law says carriers may comply with such requests, and law-enforcement agencies have pressured them to maintain the tracking systems, Mr. Gidari says.

The easiest way for stalkers to locate a target—and perhaps the most common, say therapists who work with victims and abusers—is by using systems offered by carriers. When cellphone users sign up for a "family plan" that includes two or more phones, they have the option to contact the carrier and activate a tracking feature intended to allow them to keep tabs on their children.

The AT&T FamilyMap program, for example, is free for 30 days and requires only a phone call to activate. . . "Know where your kids and loved ones are at any time!" says AT&T's website. The system is for parents, says an AT&T spokesman. He says the company hasn't received complaints about FamilyMap being used by stalkers.

The system provides an on-screen map on the smartphone or computer of the person doing the tracking. A dot on the map shows the location and movement of the person being followed. The carrier sends a text-message to the person being tracked that their phone is registered in the program.

These add-on services can be lucrative for carriers. AT&T debuted its FamilyMap system in April 2009. It charges $9.99 a month to track up to two pbones, $14.99 for up to five. FamilyMap users must agree to "terms-of-use" stating that they may not use the system to "harrass, stalk, threaten" or otherwise harm anyone.

In Corpus Christi, Mr. Helwig and his wife, who had been married since early 2008, bought phones under an AT&T family plan. Mr. Helwig says he activated the feature last year. His wife says she received a text message that a tracking function had been activated on her phone, but wasn't sure how it was activated. Her husband, she says, initially denied turning on the tracking function.

Journal Community DISCUSS

Ignorance is NOT bliss and it is time for this to be fully debated out in the open.

—Stephen Babbitt

She says she eventually came up with a plan to flee to the house of a family whose children she baby-sat. Her husband "had no idea where they lived" or even their names, she says. As she was packing, her husband confronted her. Tbey argued, and, according to her statements in police reports, Mr. Helwig dragged her around by her hair.

The police came. She says she told them she didn't want them to arrest Mr. Helwig, that she simply wanted to leave. The police told Mr. Helwig to stay away from her for 24 hours, she says.

As she drove to her friend's house, she says, she made sure her phone was off so Mr. Helwig couldn't track her. But she turned it on several times to make calls. The next day, Mr. Helwig was outside in a rage, according to police reports.

Mr. Helwig forced his way into the house, pushed her to the floor, took her car keys and drove away in her Hyundai, according to police reports.

Police arrested Mr. Helwig a short distance away. Mr. Helwig, a firefighter, is facing charges of assault and interfering with an emergency call. His trial is scheduled to begin this summer.

Mr. Helwig and his wife divorced, and she left Corpus Christi. She says she doesn't want to testify against him.

She says she is more careful about trusting her cellphone now.

Write to Justin Scheck at justin.scheck@wsj.com

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

The Washington Post

Back to previous page

Parting with privacy with a quick click

By Cecilia Kang, Published: May 8

When Scott Fitzsimones turned 13, he got an iPhone, set up accounts for Facebook and Pandora and went on an apps downloading spree. At the same time, the new teenager lost many protections over his privacy online.

The games he plays know his location at any given moment through the phone's GPS technology. He has entered his parents' credit card number to buy apps, and iTunes has his family's e-mail address and everyone's full names. Facebook knows his birth date and the school he attends.

At an age when his parents won't let him go to the mall alone and in an era when he would never open up to a stranger, Fitzsimones, who lives in Phoenix, already has a growing dossier accumulating on the Web. And while Congress has passed laws to protect the youngest of Internet users from sharing much information about themselves, once those children become teens, the same privacy rules no longer apply.

"It's the Wild West for teens when it comes to privacy online," said Kathryn Montgomery, a privacy advocate and communications professor at American University.

The federal government has a history of regulating media to protect children under age 12. Examples are the 1998 children's Internet privacy law and television advertising limits that were set for broadcasters and cable networks in 1990. And recent problems with Internet privacy and security — such as last week's breaches at Sony's online gaming network — have led to renewed calls for regulations to protect consumers. For the first time, the White House has called for Internet privacy rules.

But experts on adolescent development say youths between 13 and 18 deserve special attention. Reps. Edward J. Markey (D-Mass.) and Joe Barton (R-Tex.) said last week they are working on a bill to limit the collection of personal information about teens and prevent targeted marketing to them.

Adolescents are among the most voracious and precocious users of new mobile Internet services, constantly making grown-up decisions with grown-up consequences, experts say. But, according to Montgomery, "Their ability to make decisions is still forming and clearly different from that of adults."

'I never say no'

With few restraints, teens are creating digital records that also shape their reputations offline. All the status updates, tweets and check-ins to specific locations can be reviewed by prospective employers, insurance companies and colleges.

Web firms say sensitive data can be collected only with permission and that parents can set controls on phones and desktop computers to help keep teens out of the public eye. But for teens like Fitzsimones, the opportunities to share information online are so frequent and routine that they hardly even stop to think about them.

The first time he was asked to share his location on the game Pocket God, the seventh-grader paused for a moment to consider why the company would want to know his whereabouts.

But he feared that if he didn't agree, his experience on the app would be limited, and Fitzsimones wanted to get started on his cartoon pygmy adventure on Oog Island. So he tapped "okay," feeling comfort in the masses; his friends, after all, were using the app and never complained.

Since then, such decisions have been easier. He automatically agreed when Angry Birds, Pandora and other apps asked to track his location.

"I never say no. It's more annoying than anything when they ask, but I'm used to it now," said Fitzsimones, now 14, who writes blogforteens.com.

Such decisions are often done under stressful conditions and without enough information about the risks involved, privacy advocates say. Social pressures play out on the Internet, and teens are constantly tested on how much they are willing to expose of themselves in order to play games and participate in social networks, advocates say.

Bolt Creative, which runs Pocket God, said its social networking partner, Open Feint, gets the location data so users can see how their scores rank among people within their vicinity.

Chief executive Dave Castelnuovo said location data is only collected voluntarily. Making too much of a fuss about privacy could turn off users, he said.

"At the end of the day, we're in the entertainment business and we're a small team at that. We only have 5 seconds to engage a user once they open our game otherwise we lose that customer," Catelnuovo wrote in an e-mailed response. "All customers have access to the privacy policy for Open Feint but if we were to present them with additional warnings, cautions and terms and conditions in a form that is impossible to ignore or misunderstand, it will end up ruining the experience that they paid for."

That perspective concerns privacy and adolescent development experts, who say numerous studies show that teenagers can be more impulsive online.

A 2009 paper by neurobiologists and marketing experts at the University of California at Irvine reported that teens were more susceptible than adults to online advertising and take greater risks with their information online. If a group of friends is meeting for a movie at the AMC Theatre in downtown D.C., for instance, a teen who badly wants to join may send out notice through a public status update — without thinking about the risks of disclosing that information to anyone who might be on a social networking site.

Brain development

The prefrontal cortext, the part of the brain that makes planned and rational decisions, doesn't fully develop until the 30s, according to the UC Irvine report, coauthored by Frances Leslie, a professor of pharmacology and neurobiology. "Whereas adults rely on a sophisticated interplay between multiple brain structures to make risk-return trade-offs, this is simply unavailable to adolescents," she and her co-authors wrote in "Adolescents' Psychological and Neurobiological Development: Implications for Digital Marketing."

Hemu Nigam, a security expert and former chief privacy officer for My Space, says that means companies should be making their privacy settings for teens tighter by default. "We as parents can to a degree protect our teens from bad content, but we can't protect them from their own conduct," Nigam said.

The new challenge in teen privacy involves mobile phones, which are used by six out of 10 teens. Nearly all of those users send text messages and exchange pictures, according to the Pew American Internet and Life project. Three out of 10 teens access the Internet on smartphones.

On phones, privacy policies are often unclear. The Federal Trade Commission said it is investigating one app company that explains its privacy policy only after 152 screen clicks from a mobile device.

About a half of smartphone users read app privacy policies, according to a recent study by industry-funded privacy group Truste. Privacy advocates estimate the numbers are lower for teens.

Up to parents

So parents like Jordan Glicksman's set rules. He could download only teen-appropriate games on his iPod Touch. They forbade him from giving out personal information like his home address.

But the 14-year-old regularly agrees to location requests from games and Facebook's Places program. He admits he's never read through a privacy policy and doesn't know how much information about him is out there on the open Web.

Glicksman, who is temporarily living in Israel, got swept up in a policy change that made his Facebook profile more widely available. He started getting "friend" requests from adult strangers. Stories he shared about sports and his status updates were public. "I don't know how that happened, and it was creepy," he said.

But it hasn't slowed him down; he doesn't give it much thought when he checks in a few times a day to his Facebook app and plays games.

Revelations that Apple and Google may have logged the locations of mobile users has brought new attention to Internet privacy from lawmakers, who will question the two companies about their geo-locational collection at a hearing this week.

Foursquare and Gowalla, two popular location-based services, have built a business out of users broadcasting their locations online so that companies can push local coupons and retail suggestions. Both companies set 13 as the minimum age for users.

Foursquare co-founder Naveen Selvadurai said parental controls can help teens opt out of certain services. They don't track users' movements, and location is only detected by voluntary "check-ins," he said.

But he said the firm didn't consider special protections for teens.

"With a lot of these things, we will figure things out as we go along," Selvadurai said in an interview. "We are still a younger service, and most of the policies are trying to catch up with things people are doing."

Sponsored Links

Penny Stock Soaring 3000%
Sign up for Free to find out what the next 3000% Stock Winner Is!
www.PennyStocksUniverse.com

Mortgage Rates Hit 2.99%
If you owe under $729k you probably qualify for Gov't Refi Programs
www.SeeRefinanceRates.com

Netflix ® FREE TRIAL
Watch Unlimited TV Shows & Movies Now! Only $7.99/mo. After 1 mo. Free!
www.Netflix.com

Buy a link here

© The Washington Post Company

US 20100020776A1

(19) United States

(12) Patent Application Publication

(10) Pub. No.: US 2010/0020776 A1

(43) Pub. Date: Jan. 28, 2010

Youssef et al.

(54) WIRELESS NETWORK-BASED LOCATION APPROXIMATION

(75) Inventors: **Adel Amin Youssef**, Milpitas, CA (US); **Arunesh Mishra**, Mountain View, CA (US); **Sam Liang**, Palo Alto, CA (US); **Michael Chu**, Los Altos, CA (US); **Ravi Jain**, Palo Alto, CA (US)

Correspondence Address:
GOOGLE
Lerner, David, Littenberg, Krumholz & Mentlik, LLP
600 South Avenue West
Westfield, NJ 07090 (US)

(73) Assignee: **Google Inc.**, Mountain View, CA (US)

(21) Appl. No.: **12/315,079**

(22) Filed: **Nov. 26, 2008**

Related U.S. Application Data

(60) Provisional application No. 60/990,488, filed on Nov. 27, 2007, provisional application No. 61/196,167, filed on Oct. 15, 2008.

Publication Classification

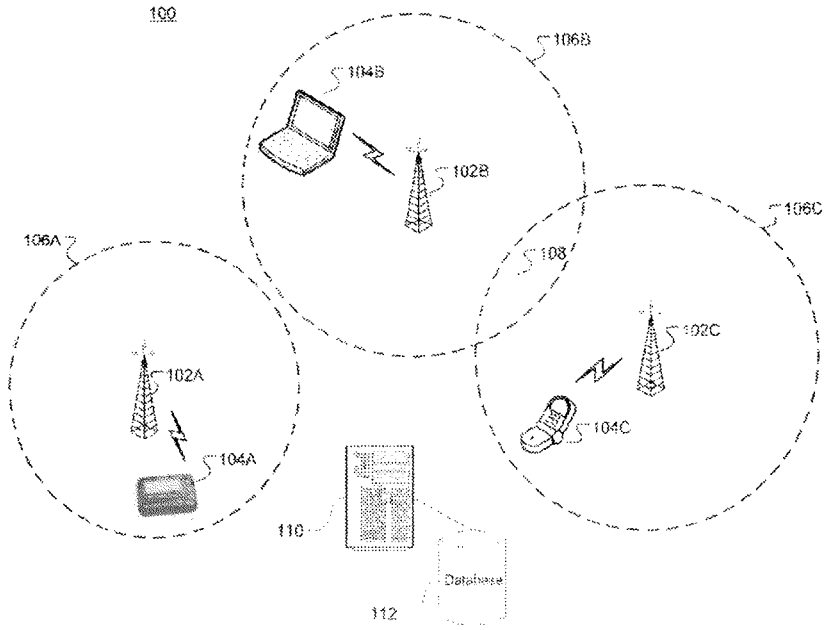
(51) **Int. Cl.**

H04W 8/02	(2009.01)
H04W 24/00	(2009.01)
H04W 4/02	(2009.01)

(52) **U.S. Cl.** **370/338**; 455/456.3

(57) **ABSTRACT**

The invention pertains to location approximation of devices, e.g., wireless access points and client devices in a wireless network. Location estimates may be obtained by observation/analysis of packets transmitted or received by the access point. For instance, data rate information associated with a packet is used to approximate the distance between a client device and the access point. This may be coupled with known positioning information to arrive at an approximate location for the access point. Confidence information and metrics about whether a device is an access point and the location of that device may also be determined. Accuracy of the location determination may be affected by factors including propagation and environmental factors, transmit power, antenna gain and diversity, etc. A location information database of access points may employ measurements from various devices over time. Such information may identify the location of client devices and provide location-based services to them.



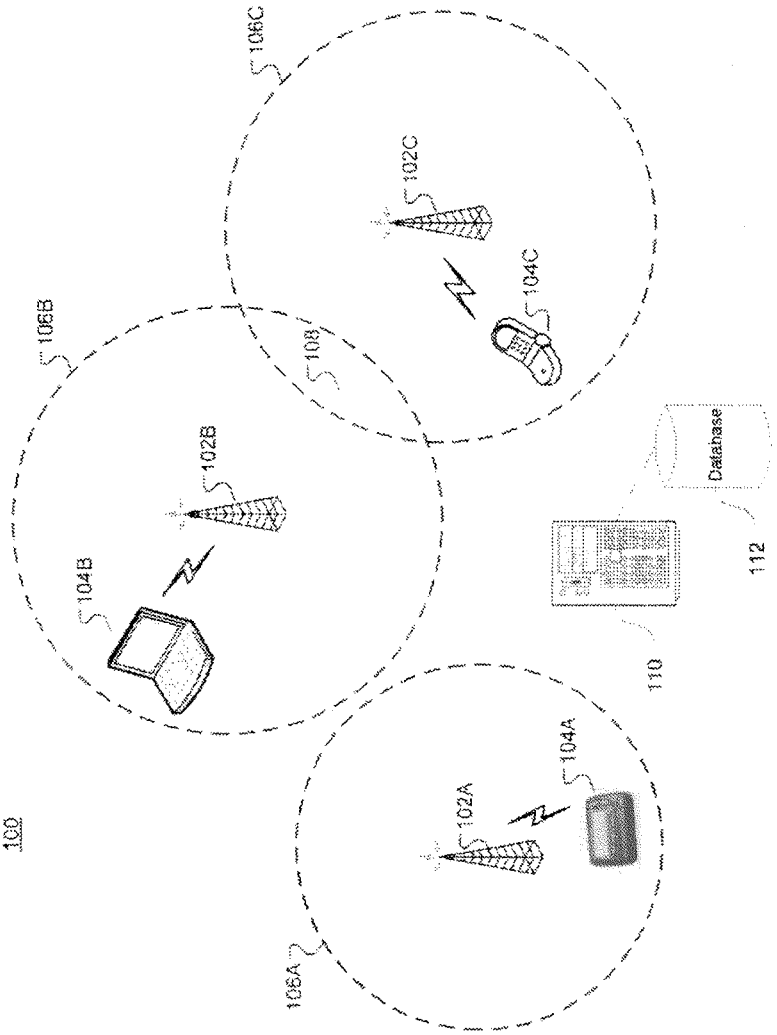
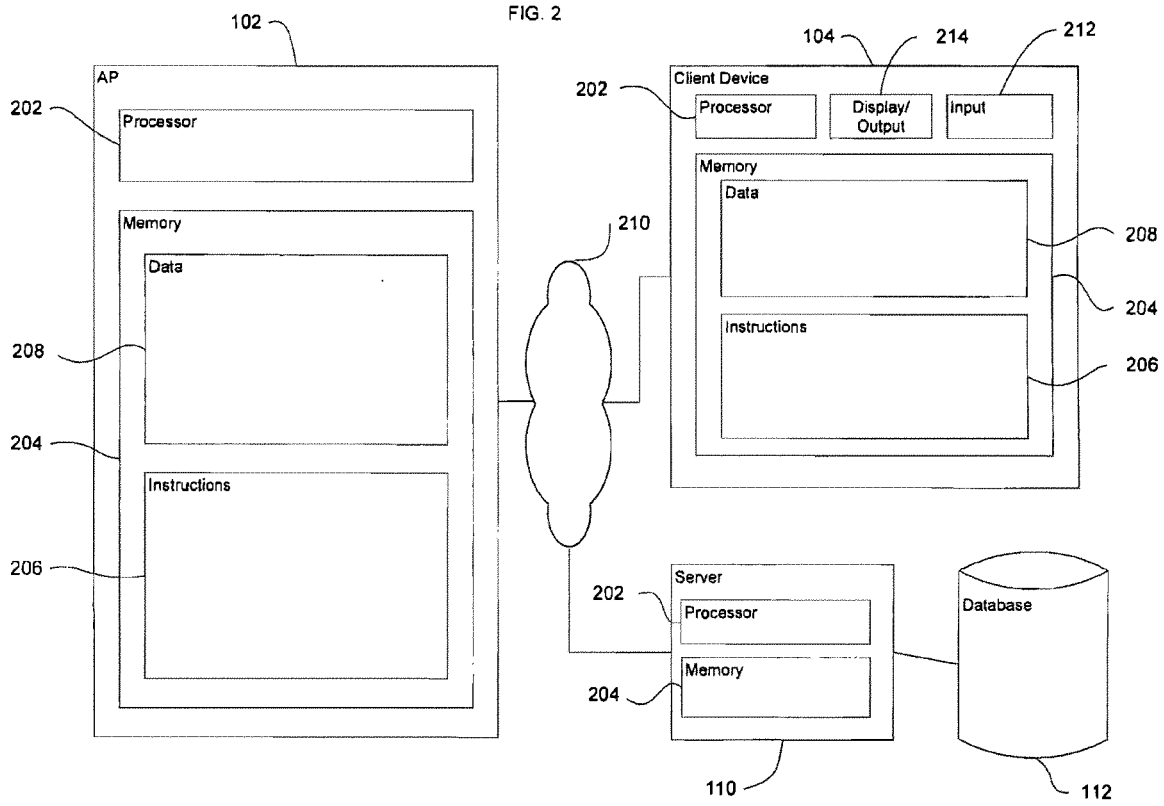

100
106A
102A
104A
106B
104B
102B
108
106C
102C
104C
110
Database
112

FIG. 1

FIG. 2


102
AP
202
Processor
Memory
Data
208
204
Instructions
206
210
104
214
212
Client Device
202
Processor
Display/ Output
Input
Memory
Data
208
204
Instructions
206
Server
202
Processor
Memory
204
110
Database
112

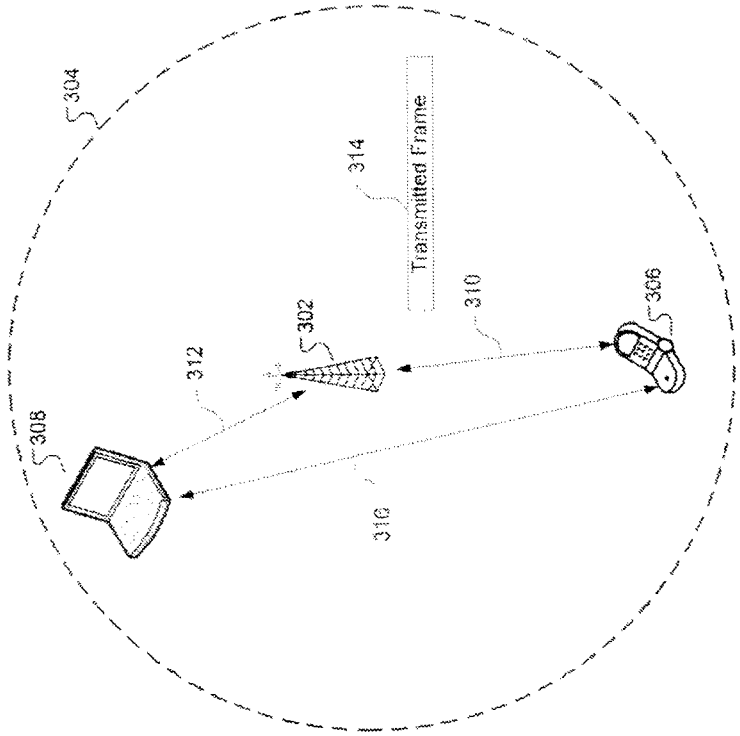


FIG. 3

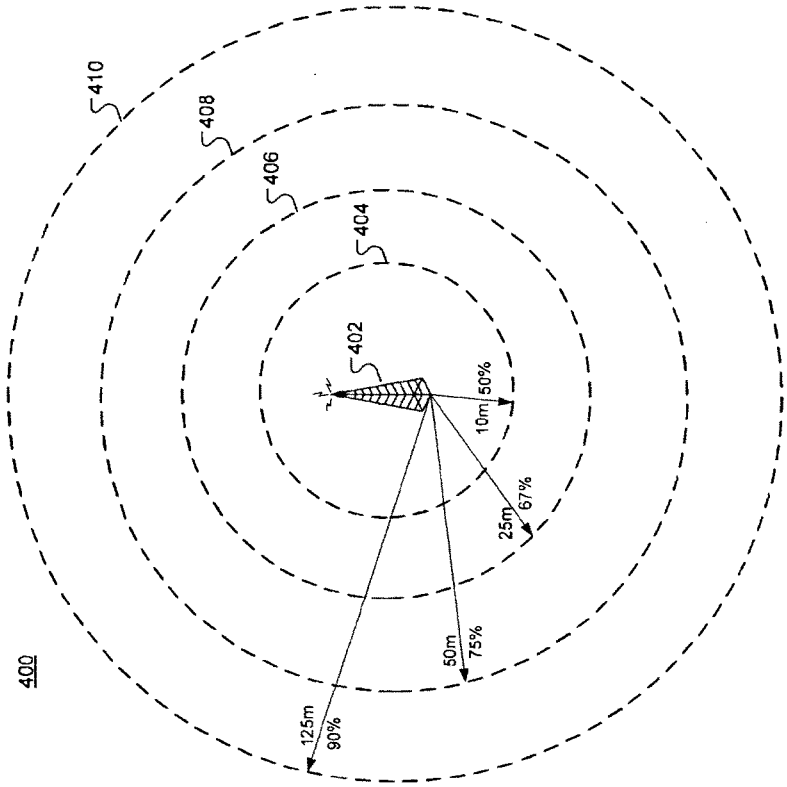


FIG. 4

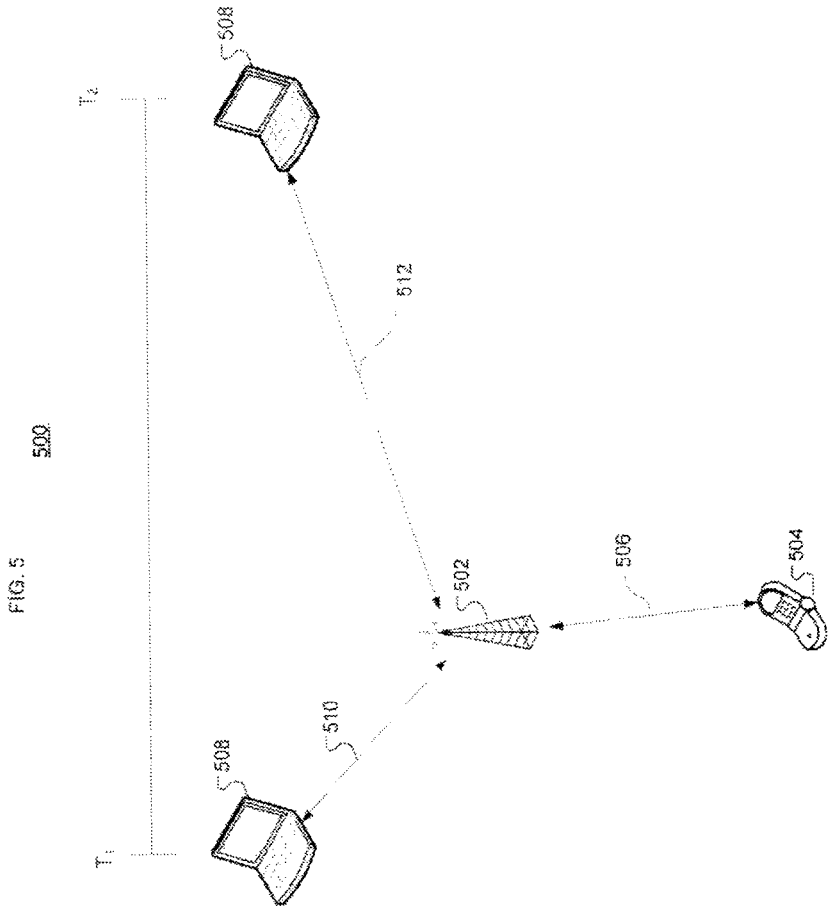


FIG. 5

FIG. 6B

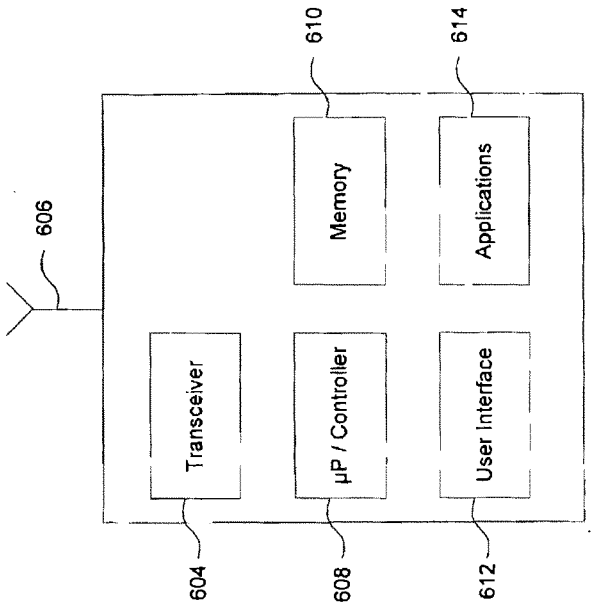
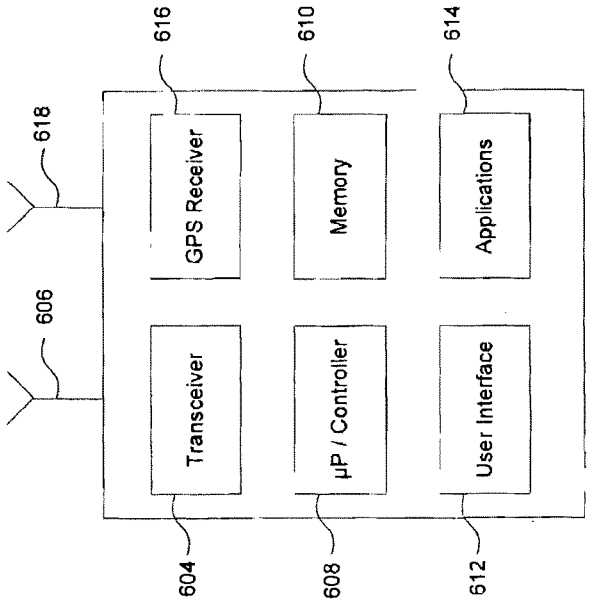

602
606
Transceiver
604
µP / Controller
608
Memory
610
User Interface
612
Applications
614

FIG. 6A


600
606
618
Transceiver
604
GPS Receiver
616
µP / Controller
608
Memory
610
User Interface
612
Applications
614

WIRELESS NETWORK-BASED LOCATION APPROXIMATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of the filing date of United States Provisional Patent Application No. 61/196,167, entitled "Wireless Network-Based Location Approximation," attorney docket GOOGLE 3.8-020, filed Oct. 15, 2008, and of United States Provisional Patent Application No. 60/990,488, entitled "Accuracy Analysis of Wireless Base Station Location," attorney docket number 2525.1180000, filed Nov. 27, 2007, the entire disclosures of which are hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates generally to approximating the location of electronic devices such as wireless access points ("APs") and client devices.

[0004] 2. Description of Related Art

[0005] Wireless networks offer a wide variety of services using a number of different architectures. Client devices such as mobile phones, laptops and PDAs may connect to APs via cellular/PCS networks as well as wireless local area networks ("WLANs") such as IEEE 802.11, Bluetooth® or other Wi-Fi® networks.

[0006] Location-based services can leverage the physical location of a client device to provide an enhanced service or experience for a user. A location-based service may determine the location of the user by using one of several technologies for determining position, then use the location and possibly other information to provide personalized applications and services.

[0007] Conventional cellular/PCS networks may position their APs (e.g., base stations) in accordance with specific coverage criteria. The locations of these base stations may be placed at known locations. Client devices in such networks may include GPS-enabled handsets, which enable accurate determination of the location of the devices.

[0008] In contrast, WLANs networks may include APs which are relatively small or portable (e.g., mini base stations or wireless routers), and which may be placed at locations as needed. The exact locations of APs in this situation may not be known. For instance, a corporate wireless network may have a number of APs distributed across the corporate campus. So long as the APs provide adequate coverage, a general knowledge of their location such as which building they are in may suffice.

[0009] Another type of scenario where the specific location of the APs may not be known is in a building-wide (e.g., an airport terminal) or city-wide mesh or ad-hoc WiFi network. In such cases, users may access APs set up by one or more service providers.

[0010] In such cases, the APs and client devices themselves may not be GPS-enabled. Or the devices may be located indoors or in other environments where GPS does not operate. Thus, it may be difficult or impossible to offer location-based services without some way to determine the positions of the APs and/or the client devices.

BRIEF SUMMARY OF THE INVENTION

[0011] The present invention provides systems and methods for estimating AP locations as well as estimating the confidence and accuracy for such locations. Using such information, the locations of client devices may also be determined, which in turn enables the use of location-based services.

[0012] In accordance with an embodiment of the present invention, a computer-implemented method of estimating the location of a wireless device is provided. The method comprises obtaining a packet of data transmitted from a first wireless device to a second wireless device; determining whether one of the first and second wireless devices is a wireless access point; determining the data rate of the transmitted data packet; if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and assigning an estimated location to the wireless access point based upon the evaluation.

[0013] In one alternative, the predetermined criterion is stored in a database such as in a look-up table. Here, the evaluation includes identifying a distance in the look-up table associated with the determined data rate. In one example, the transmitted data packet is obtained by a client device and the method further includes identifying a distance associated with the data rate, wherein the distance is used as a separation between the first wireless device and the client device. Here, if the client device is at a known location, then the method may further comprise assigning a distance between the wireless access point and the client device to be the same as the distance between the first wireless device and the client device; and triangulating a position of the wireless access device using the known location of the client device, the distance between the first wireless device and the client device and the distance between the wireless access point and the client device to obtain the estimated location. In this example, the client device may use a GPS receiver to obtain the known location.

[0014] In another alternative, the predetermined criterion includes a worst-case distance estimate based upon at least one parameter. In an example, the at least one parameter includes one or more of a channel propagation characteristic, a transmitter characteristic and a receiver characteristic.

[0015] In yet another alternative, the method further comprises revising the estimated location of the wireless access point based upon multiple data packets sent or received by the wireless access point.

[0016] In another alternative, the method further comprises determining a position of the client device based upon the estimated location of the wireless access point and providing a location-based service to the client device based on the determined position.

[0017] In accordance with another embodiment of the present invention, a computer-implemented method of estimating confidence in a status of a wireless device is provided. The method comprises obtaining one or more packets of data transmitted from a first wireless device to a second wireless device; evaluating the one or more transmitted data packets to identify a frame type for each respective data packet; identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and assigning a confidence value to the identification of the wireless access point.

[0018] In one alternative, if the frame type of at least one of the respective data packets is a management frame, then identifying the first wireless device as a wireless access point. In this case the method sets the confidence value for the

identification of the wireless access point to a maximum confidence value. Optionally, if the frame type of at least one of the respective data packets is not the management frame, then the method evaluates whether the frame type of any of the respective data packets is a control frame. Here, if the frame type of at least one of the respective data packets is the control frame, then the method identifies the first wireless device as the wireless access point and sets the confidence value for the identification of the wireless access point to a value between the maximum confidence value and a minimum confidence value.

[0019] In another alternative, identifying the first wireless device or the second wireless device as the wireless access point further includes analyzing a number of frames transmitted or received by each device

[0020] In accordance with another embodiment of the present invention, a computer-implemented method of estimating confidence in a location of a wireless device is provided. Here, the method comprises obtaining one or more packets of data transmitted from a first wireless device to a second wireless device; determining that the first or second wireless device is a wireless access point based upon the transmitted packets; determining an estimated location of the wireless access point; and assigning a confidence value to the estimated location.

[0021] In one alternative, the confidence value represents a percentage likelihood that the wireless access point is contained within a specified area of interest. In another alternative, the estimated location is based on multiple data points. In this case, a confidence code may be applied to each data point. In one example, the confidence code for each data point is calculated using a weighted function. In another example, the confidence code for each data point represents a likelihood that that data point is valid or an outlier.

[0022] In yet another embodiment of the present invention, an apparatus for use in a wireless network comprises memory for storing information associated with a plurality of devices in the wireless network, means for communicating with one or more of the plurality of devices in the wireless network and a processor. The processor is operable to estimate a location of an access point device in the wireless network based upon data packet information sent to or received from the access point device. The processor is adapted to provide location based service information to one or more client devices associated with the access point device upon estimation of the location.

[0023] In one alternative, the data packet information for a given data packet includes a data rate of the given data packet. Here, the information stored in the memory includes distance estimates associated with different data rates. The processor determines the location estimate of the access point device by comparing the data rate of the given data packet to the different data rates and distance estimates stored in the memory.

[0024] In another alternative, the processor is operable to estimate the location of the access point device using the data packet information for multiple data packets sent to or received from the access point device. The processor is further operable to rank the data packet information for each of the multiple data packets to obtain approximate distances based upon each such packet. In one example, the processor estimates the location using a centroid of the approximate distances. In another example, the processor is further operable to assign a confidence in the estimated location of the access point device. The confidence may represent a likelihood that the access point device is within a given area. Optionally, the confidence is based upon at least one of spatial diversity of selected devices associated with the access point device, receiver characteristics of the selected devices, transmitter characteristics of the selected devices, and freshness of information stored in memory or the data packet information sent to or received from the access point device.

[0025] In yet another alternative, the processor comprises a plurality of processing devices in a distributed architecture and the memory stores the information so that the information is accessible to one or more of the plurality of processing devices.

[0026] Each of the aforementioned methods and processes may be performed by a processor such as a CPU, microprocessor, ASIC or other computing device. Furthermore, such methods and processes may be stored on a computer-readable recording medium (e.g., CD-ROM, DVD, Blue Ray disc, flash memory or the like) for execution by a processor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0027] FIG. 1 illustrates an exemplary wireless network in accordance with aspects of the present invention.

[0028] FIG. 2 illustrates aspects of a wireless network in accordance with aspects of the present invention.

[0029] FIG. 3 illustrates an exemplary configuration for estimating device location in accordance with aspects of the present invention.

[0030] FIG. 4 illustrates an exemplary confidence and positioning diagram in accordance with aspects of the present invention.

[0031] FIG. 5 illustrates an exemplary dynamic scenario for location estimation.

[0032] FIGS. 6A-B illustrate exemplary wireless devices for use with aspects of the present invention.

DETAILED DESCRIPTION

[0033] The instant application is related to United States Provisional Patent Application No. 60/990,569, entitled "Locating Electronic Devices Using Passive Radios," attorney docket number 16113-0938P01, filed Nov. 27, 2007, United States Provisional Patent Application No. 60/990,259, entitled "Estimating Location Using Cell ID and Application Specific Data," attorney docket number 2525.1140000, filed Nov. 26, 2007, United States Provisional Patent Application No. 60/990.238, entitled "Disambiguation of Wireless Data Clusters Using Preclassification," attorney docket number 2525.116000, filed Nov. 26, 2007, United States Provisional Patent Application No. 60/990,247, entitled "Method and System for Cell-Id Remapping Detection and Adaptation," attorney docket number 2525.1170000, filed Nov. 26, 2007, and United States Provisional Patent Application No. 60/990,597, entitled "Wireless Base Station Location Estimation," attorney docket number 2525.1150000, filed Nov. 27, 2007, the entire disclosures of which are hereby incorporated by reference herein.

[0034] The instant application is also related to U.S. patent application Ser. No. _____, entitled "Determining Location Information Using Passive Radios," attorney docket number 16113-0938001, filed concurrently herewith, U.S. patent application Ser. No. _____, entitled "Systems and Methods for Estimating Location Using Cell ID and Application Specific Data," attorney docket number 2525.1140001, filed concurrently herewith, U.S. patent application Ser. No. _____,

entitled "Disambiguation of Wireless Data Clusters Using Preclassification," attorney docket number 2525.116001, filed concurrently herewith, U.S. patent application Ser. No. _____, entitled "Method and System for Cell-Id Change Detection and Updating," attorney docket number 2525.1170001, filed concurrently herewith, U.S. patent application Ser. No. _____, entitled "Wireless Base Station Location Estimation," attorney docket number 2525.1150001, filed concurrently herewith, and U.S. patent application Ser. No. _____, entitled "Accuracy Analysis of Wireless Base Station Location," attorney docket number 2525.1180001, filed concurrently herewith, the entire disclosures of which are hereby incorporated by reference herein.

[0035] The aspects, features and advantages of the present invention will be appreciated when considered with reference to the following description of preferred embodiments and accompanying figures. The same reference numbers in different drawings may identify the same or similar elements. Furthermore, the following description does not limit the present invention; rather, the scope of the invention is defined by the appended claims and equivalents.

[0036] FIG. **1** provides an exemplary WLAN **100** which may have a number of APs **102** (e.g., **102**A, **102**B and **102**C) as well as one or more client devices **104** (e.g., **104**A, **104**B and **104**C) as shown. The APs **102** may include devices of different types from various manufacturers and may have different capabilities. Some APs **102** may be wireless routers that can support dozens of client devices or more, while some APs may act as signal repeaters. The client devices **104** may also be of different types and have different capabilities. For instance, as shown client device **104**A may be a PDA, **104**B may be a laptop/notebook computer, and **104**C may be a mobile phone.

[0037] The WLAN **100** may also include a server **110** that is in wired or wireless communication with some or all of the APs **102**. A database **112** may be associated with the server **110**. The database **112** may be used to store data related to the APs **102** and/or the client devices **104**. For instance, the database **112** may maintain location-related records for the APs **102**.

[0038] Each AP **102**, each client device **104** and the server **110** may contain at least one processor, memory and other components typically present in a computer. FIG. **2** illustrates an alternative view **200** of a single AP **102**, a single client device **104** and server **110** identifying such components. As shown, the AP **102** includes a processor **202** and memory **204**. Components such as a transceiver, power supply and the like are not shown in any of the devices of FIG. **2**.

[0039] Memory **204** stores information accessible by the processor **202**, including instructions **206** that may be executed by the processor **202** and data **208** that may be retrieved, manipulated or stored by the processor. The memory may be of any type capable of storing information accessible by the processor, such as a hard-drive, ROM, RAM, CD-ROM, flash memories, write-capable or read-only memories. The processor **202** may comprise any number of well known processors, such as processors from Intel Corporation. Alternatively, the processor may be a dedicated controller for executing operations, such as an ASIC.

[0040] The instructions **206** may comprise any set of instructions to be executed directly (such as machine code) or indirectly (such as scripts) by the processor. In that regard, the terms "instructions," "steps" and "programs" may be used interchangeably herein. The instructions may be stored in any computer language or format, such as in object code or modules of source code. The functions, methods and routines of instructions in accordance with the present invention are explained in more detail below.

[0041] Data **208** may be retrieved, stored or modified by processor **202** in accordance with the instructions **206**. The data may be stored as a collection of data. For instance, although the invention is not limited by any particular data structure, the data may be stored in computer registers, in a relational database as a table having a plurality of different fields and records.

[0042] The data may also be formatted in any computer readable format such as, but not limited to, binary values, ASCII or EBCDIC (Extended Binary-Coded Decimal Interchange Code). Moreover, the data may include any information sufficient to identify the relevant information, such as descriptive text, proprietary codes, pointers, references to data stored in other memories (including other network locations) or information which is used by a function to calculate the relevant data.

[0043] Although the processor **202** and memory **204** are functionally illustrated in FIG. **2** as being within the same block, it will be understood that the processor and memory may actually comprise multiple processors and memories that may or may not be stored within the same physical housing or location. For example, some or all of the instructions and data may be stored on a removable CD-ROM and others within a read-only computer chip. Some or all of the instructions and data may be stored in a location physically remote from, yet still accessible by, the processor **202**. Similarly, the processor **202** may actually comprise a collection of processors which may or may not operate in parallel. Data may be distributed and stored across multiple memories **204** such as hard drives or the like.

[0044] In one aspect, AP **102** communicates with one or more client devices **104** and the server **110** via wireless network **210** (e.g., a Wi-Fi®-type network such as an 802.11 g network or a Bluetooth®-type network). Each client device **104** and the server **110** may be configured similarly to the AP **102** with a processor **202**, memory **204** and instructions **206**, as well as one or more user input devices **212** and a user output device, such as display **214**. Each client device **104** and the server **110** may be a general purpose computer, intended for use by a person, having all the components normally found in a personal computer such as a central processing unit ("CPU"), display, CD-ROM or DVD drive, hard-drive, mouse, keyboard, touch-sensitive screen, speakers, microphone, wireless modem and all of the components used for connecting these elements to one another.

[0045] Each device on the network **100** may transmit and receive data (packets) according to a known protocol in a segment (channel) of allotted portion the spectrum (frequency band). For instance, the IEEE 802.11 series of protocols specifies the format of various types of packets which may be transmitted in preset channels of the spectrum, such as the ISM band located in the 2.4 GHz frequency range or the public safety band located in the 4.9 GHz frequency range.

[0046] Depending upon their configuration, each AP may have a coverage area **106** such as coverage areas **106**A, **106**B and **106**C as shown in FIG. **1**. In many instances the coverage areas **106** of adjacent APs **102** may overlap, such as shown by overlap region **108**. It should be understood that the coverage

areas **106** in real-world implementations may be affected due to transmit power requirements, signal attenuation, multipath and other factors.

[0047] As discussed above, it is desirable to provide location-based services to client devices. While some client devices may include a GPS receiver or some other tool to determine and/or communicate the device's location, many client devices may not have such equipment or capabilities. Thus, in accordance with one aspect of the present invention, the location of a given client device may be determined based upon the location(s) of one or more APs, either alone or in conjunction with other network-related information.

[0048] In such a scenario, one important issue is that in many instances the specific location of an AP **102** may not be known. Therefore, in accordance with another aspect of the present invention, systems and methods are provided to estimate an AP's location using data rate information between the AP and one or more client devices. FIG. **3** illustrates an exemplary configuration **300** with a single AP **302** having a coverage area **304**. A first client device **306** and a second client device **308** are located within the coverage area **304**.

[0049] In the present example, the client device **306** may be "associated" with the AP **302**, transmitting packets to and receiving packets from the AP **302**. Here, the client device **306** is not GPS enabled and is not otherwise configured to determine its location. In contrast, the client device **308** may include a GPS receiver or other means of performing geolocation.

[0050] In this example, the client device **306** is located a first distance **310** from the AP **302**, while the client device **308** is located a second distance **312** from the AP. And the client device **306** is located a third distance **316** from the client device **308**. The client device **308** performs geolocation using its GPS receiver or by other means to accurately determine its location.

[0051] Furthermore, the client device **308** may be configured to observe or capture data packets such as frame **314** transmitted to or from the AP **302**. By way of example, the client device **308** may be a laptop having a wireless transceiver that can operate in a "sniffer" or "monitor" mode, thereby handling transmitted frames **314** without requiring the client device **308** to be associated with the AP **302**.

[0052] In accordance with one embodiment, the client device **308** receives and captures the frame(s) **314**. The client device **308** may analyze the frame **314**, such as with an analyzer program executed by its processor. Alternatively, the server **110** may execute the analyzer program. The analyzer program may parse different portions of the frame **314** and perform error checking on the frame **314**. As part of the analysis, it is determined which device (e.g., AP **302** or client device **306**) transmitted the frame **314**, as well as the data rate at which the transmitter sent the frame **314**. The data rate may be identified by data in the frame **314** itself or may be otherwise identifiable. For example, the data rate is the rate of transmission from the AP **302** to the client device **306** or from the client device **306** to the AP **302**. Alternatively, if the client device **308** is associated with the AP **302** and is communicating with the AP **302** (as opposed to merely sniffing packets), then the data rate may be the rate transmitted from the AP **302** to the client device **308** or from the client device **308** to the AP **302**.

[0053] Using this information, the client device **308** or the server **110** may estimate the distance of the client device **308** relative to the AP **302** and/or the client device **306**. For instance, the data rate may be used as an estimate of channel quality to indicate the physical separation between client device **308** and the AP **302** or between the client device **308** and the client device **306**. In one example, a look-up table may be used to estimate the distance. An exemplary look-up table is provided below.

Rate	Distance
5 Mbps	250 meters
10 Mbps	125 meters
54 Mbps	30 meters

[0054] As shown in this example, the higher the data rate, the shorter the distance. However, the distance may be adjusted by various parameters as will be discussed below. The distances in the look-up table may be approximated using a worst-case estimate based on various channel parameters such as propagation characteristics, transmit power, antenna gain, receiver sensitivity and other radio characteristics for both the transmitter and receiver, as well as terrain type, etc.

[0055] In accordance with another aspect, so long as the client device **308** is able to capture and properly decode a packet containing a transmitted frame, then it is determined that the distance between the client device **308** and the transmitting entity (e.g., AP **302** or client device **306**) must fall within the worst-case estimate. If the client device **308** is not associated with the AP **302**, then some platforms may not provide or process certain frames. In the case where client device **308** is associated with the AP **302**, then more information about the AP **302** may be available which can be used to improve the accuracy of the AP's location. For instance, in addition to the frames that client device **308** observes between the AP **302** and the client device **306**, client device **308** also has frames transmitted to itself by the AP **302**. These frames also have data rate information associated with them, so this is another opportunity to obtain an estimate of the distance between the AP **302** and the client device **308**.

[0056] Thus, in one alternative the frame(s) observed between AP **302** and client device **306** provide a first estimate or multiple estimates which can be used to determine a first approximate distance **312**, while the frame(s) received by the client device **308** from AP **302** provide a first estimate or multiple estimates which can be used to determine a second approximate distance **312**. In this case, weights or rankings may be applied to the first and second approximate distances to arrive at a resultant distance **312**. Of course, it should be understood that there may be other client devices within the area **304** in communication with the AP **302**. In that situation, there may be even more approximate distances **312** calculated/weighted to arrive at an even more accurate resultant distance **312**.

[0057] If the packet cannot be decoded or is decoded with uncorrectable errors, then the distance approximation may not be performed. Alternatively, if the packet cannot be decoded properly, it may be inferred that the distance **312** between AP **302** and client device **308** is greater than the distance **310** between the AP **302** and the client device **306**.

[0058] The above look-up table may be supplemented or otherwise parameterized based upon additional factors besides distance. For instance, the table can be parameterized based upon the transmit power values of the transmitter. Or if the transmit power values are unknown, a certain distribution

of common transmit power values can be used as an approximation. The table can also be parameterized based upon the environment where the packet/frame was captured. For example, in a dense urban environment, one may expect a high multipath coefficient. On the other hand, in a rural environment, one may expect the propagation pattern to be very symmetric, leading to larger distances for the same data rate. The table could also be parameterized based upon the receiver's radio characteristics, such as the sensitivity, antenna gain and any diversity metrics (e.g., multiple antennas) which may be applicable.

[0059] Calibration or otherwise updating of the look-up table may be done based on the power, radio sensitivity and/or vendor information of the various devices. For instance, different radios may have very different RF characteristics. Some APs are operable to transmit at higher power than others. Thus, at the same data rate, a higher power AP may be located farther away than a lower power AP.

[0060] Similarly, it may be beneficial to evaluate the sensitivity of the receiver of the client device **308**. By way of example, a dedicated sniffer/scanner may have a much higher gain antenna/receive chain than the radio receiver on a laptop, which in turn may have a higher gain than the radio on a cellular phone.

[0061] Vendor and model information for a given device and its radio/receiver may be determined based upon the device's MAC address (e.g., using the object identifier ("OID")) and frames transmitted by the device. This in turn may be used to evaluate the power and sensitivity of the radio/receiver.

[0062] Once the packet containing a frame is properly decoded, the frame may be examined to determine whether it was sent by the AP **302** or the client device **306** (or some other entity). This information may provide additional insight into the specifications of the particular AP **302** or client device **306**. For instance, if the frame information identifies the AP **302** as being of a specific type, then that may indicate the power level(s) at which the AP **302** operates.

[0063] If the decoded frame was sent by the AP **302**, then the distance determined using the look-up table gives an accurate upper bound on the separation between the client device **308** and the AP **302**. This is coupled with the location of the client device **308** provided by its self-geolocation. Thus, starting with the client device **308** at a center point of a circle similar to the coverage area **304**, the AP **302** can be determined to be within a radius of the circle, where the radius is the distance identified by the look-up table.

[0064] If the decoded frame was sent by the client device **306**, then the distance determined using the look-up table identifies the maximum separation between the client device **306** and the client device **308**. Similarly, the distance determined using the data rate (and possibly other information) in the look-up table also provides the maximum separation between the client device **306** and the AP **302**. Using the geometrical principal known as the Triangle Inequality, the maximum separation between the AP **302** and the client device **308** is no more than twice the distance determined using the look-up table.

[0065] As discussed above, because the client device **308** has a GPS receiver or can otherwise determine its position using geolocation, the location of client device **308** is known. Thus, in accordance with another aspect of the invention, the location of the AP **302** is determined by triangulating using the distance between the client devices **306** and **308** and the distance between the AP **302** and the client device **308**.

[0066] This process may be repeated by analyzing multiple packets sent between the AP **302** and the client device **306** (or other client devices falling within the coverage area **304**. Multiple estimates of the location of the AP **302** may be made by the client device **308** and/or other client devices having geolocation capabilities.

[0067] Alternatively, an estimate of the location of the AP **302** may be performed using a centroid (mean location) of multiple points associated with the AP **302**. These points may correspond to locations obtained by the same or different client devices **308** using the AP **302** at the same or different times. A coverage radius of the AP **302** may also be estimated so that most or all the points in a collection are covered.

[0068] Once a given packet/frame has been captured and decoded by the client device **308**, then the location estimation process for the AP **302** may be done by the client device **308**, the AP **302** or other entity such as server **110** of FIG. **1**. By way of example only, the look-up table may be stored in database **112**. This database may be accessible only to the server **110**, to some or all of the APs **102**, and/or to some or all of the client devices **104**. Alternatively, the database **112** may be a distributed database spread among various nodes of the wireless network, including some of the APs **102** and/or the server **110**.

[0069] Returning to FIG. **3**, once the location of the AP **302** has been estimated, then that information may be used to provide location-based services to the client device **306**. For instance, this may be done relying solely on the location of the AP **302**, and that location estimate is used when offering location-enabled features to the user of the client device **306**. Alternatively, the location of the client device **306** itself may be determined using the processes discussed above with regard to the AP **302**. Here, for example, once the AP **302** location has been estimated, the Triangle Inequality or other geolocation technique (e.g., time difference of arrival ("TDOA"), angle of arrival ("AOA"), etc.) may be used to estimate the location of the client device **306**. As above, repeated measurements may be used to determine the location before or during offering location-enabled services to the user of the client device **306**.

[0070] In accordance with other aspects of the present invention, the confidence of the location of an AP may be estimated. The confidence determination may include an evaluation as to whether the transmitting entity is in fact an AP. And the confidence determination may evaluation the relative accuracy of the physical location for that transmitting entity.

[0071] In one evaluation, it is important to determine whether the device of interest is really an AP. This may be done by evaluating different types of frames sent to (or received from) the device of interest. Depending upon the protocol of the WLAN, there may be management frames, control frames, data frames, etc. which are sent and received by devices in the network. In the example of FIG. **3**, if the client device **308** decodes a management frame such as a beacon frame, then it is determined that the transmitting entity is the AP **302**. However, if the decoded frame is a control frame such as a "Request To Send" ("RTS"), "Clear to Send" ("CTS"), "Acknowledgement" ("ACK"), "Power Save-Poll" ("PS-POLL"), or "Contention Free-End" ("CF-END"), then the transmitter may or may not be the AP **302**.

[0072] Another indicator of whether the device of interest is the AP **302** is the number of frames it transmits. For example, a high number of frames such as control frames sent over a short period of time (e.g., **100** control frames sent in 2 minutes) may suggest that the device is an AP. Similarly, a high number of frames received may also suggest that the device is an AP.

[0073] Data and metrics concerning the device of interest may be obtained by various client devices **308** at the same or different periods of time. Such information may be stored in a database such as database **112**. These various indicators are analyzed to provide some value of confidence that the device is an AP. By way of example only, the confidence may be expressed as a percentage value (e.g., 90%) that the device of interest is an AP. An exemplary algorithm may rely on a number of factors to obtain confidence levels/values. For instance, spatial, temporal and/or platform diversity of GPS measurements would be relevant. Also, the types of frames that are used in the measurement, such as data frames, management frames and/or control frames may affect the confidence. And the source of the measurement may be a relevant factor, such as if it is a trusted party providing the readings versus uploading them through an Open API implementation.

[0074] In another evaluation, the confidence in the location of the AP **302** is determined. Here, the confidence may be expressed as a percentage, e.g., that it is 90% likely that the device of interest is within a certain radius/area). Factors affecting this analysis include spatial diversity of the different client devices which interact with the AP. In addition, whether the client devices are of different types may be relevant to the evaluation. For instance, the antenna gain and overall robustness of the receiver may impact the accuracy of the measurements taken. Here, the data taken by a high quality receiver with multiple spatially diverse antennas having high gain may be given a higher weight in the analysis than data taken from a receiver with a single, low gain antenna.

[0075] Furthermore, the accuracy of the GPS or other geolocation measurements may affect the accuracy calculation. Here, for instance, a differential GPS receiver may be determine the client device **308**'s position to within a meter or less, while a non-differential GPS receiver may determine the position to within 5-25 meters or more. In addition, while the accuracy of a GPS measurement outdoors with a clear view of the sky may be close to optimum, performance degradations may occur in urban canyon environments where fewer satellites are "visible" and especially when the GPS receiver is located indoors. In the latter case, the GPS receiver may be unable to fix a location at all. Also the "freshness" of the data collected may be relevant to the confidence determination. Here, more recent data may be given a higher weight in the analysis than older data. As above, an exemplary algorithm may rely on a number of additional factors to obtain accuracy. For instance, spatial, temporal and/or platform diversity of GPS measurements would be relevant. Also, the types of frames that are used in the measurement, such as data frames, management frames and/or control frames may affect the confidence. And the source of the measurement may be a relevant factor, such as if it is a trusted party providing the readings versus uploading them through an Open API implementation.

[0076] In accordance with another aspect of the present invention, processes to determine the accuracy of AP locations are provided. In one embodiment, the measurements taken by various client devices determine a confidence that a given AP is within a certain area. One or more data points represented the expected position of the given AP may be calculated based upon the various factors discussed herein. A "confidence code" may be applied to each data point.

[0077] The confidence code may be calculated using a weighted function. The weights used by the weighted function may be obtained based on information of the collected data such as size of the collection (e.g., the cardinality or number of points in the collection), platform information of the client devices, temporal and/or spatial diversity of the points corresponding to the client devices, etc. One or more estimates of the location of the AP may be adjusted based on the calculated confidence code. A Monte Carlo-type analysis may also be performed.

[0078] In order to provide more accurate estimation of AP locations and coverage regions, several factors can be taken into account to analyze the accuracy of such estimations. The factors may include the number of points, platform information of corresponding client devices, temporal diversity of the points, spatial diversity of the points, etc. For example, the estimated location for a given AP will be more accurate when using more points for the estimation.

[0079] More variety of platforms of client devices indicates more users for the AP, and may increase the accuracy of the estimation. With regard to temporal diversity, points spanning multiple distinct times may contribute to a more accurate estimation than points spanning fewer distinct times. Also, with regard to spatial diversity, more accurate estimation can be achieved by using points spread in a larger space than points clustered in a smaller area. A weight function can be used to calculate a confidence code based on the above information. Accordingly, the estimated location and coverage radius for the given AP can be adjusted based on the confidence code.

[0080] In one example, the confidence code represents the likelihood that a particular data point is valid or an outlier. For instance, this may be expressed as a percentage (e.g., 90% likely that the data point is valid), as a ranking (e.g., a 4 on a scale of 1-5, with 1 being the lowest confidence and 5 being the highest confidence), or some other relative indicator. The confidence code may then be used to discard outliers. Once this is done, the system may compute a "best circle" representing the likely position of the AP of interest.

[0081] In an alternative, multiple circles may be provided as shown in the confidence and positioning diagram **400** of FIG. **4**. In this example, AP **402** may be placed in the center of multiple concentric circles **404**, **406**, **408** and **410**. Each circle may be associated with both an area and a confidence value. For instance, the innermost circle **404** may indicate that there is a 50% likelihood that the AP **402** is within **10** meters of the epicenter of that circle. The next smallest circle **406** may be used to indicate that there is a 67% likelihood of the AP **402** being within 25 meters of the epicenter of that circle. The next circle **408** may be used to indicate that there is a 75% likelihood of the AP **402** being within 50 meters of the epicenter of that circle. And the outermost circle **410** may be used to indicate that there is a 90% chance of the AP **402** being within 125 meters of the epicenter of that circle. In one example, an $O(n^2)$ algorithm may be used to detect outliers. This may be done as follows. First, the centroid of a given number of points may be computed. Then for each point, its distance to the centroid may be computed. If the distance for a given point exceeds a threshold, then the point may be marked or otherwise identified as an outlier. The process may be refined

by removing some/all outliers and repeating the above. This may be repeated until there are no more outliers or the algorithm converges.

[0082] As discussed herein, the location of a given AP may be based on a number of measurements taken by one or more client devices. The raw data collected by a client device may be processed locally or sent to a central repository (e.g., server **110** of FIG. 1) for processing. Regardless of which device performs the calculations, each distance and/or each location estimate may be stored in a database, for instance as part of a location table. The location table may store, for one or more APs, a unique identifier for the AP (such as a MAC address, IP address or SSID), a location estimate (e.g., latitude and longitude coordinates and/or height), a time the location estimate was obtained/calculated, a coverage radius for the AP, a confidence for the location estimate (e.g., 90% likely to be within 50 meters of the specific position), equipment type (e.g., transceiver make/model) and/or RSSI information. If multiple location measurements are made, some or all of them may be stored in the location table. Calculated locations and associated estimates such as discussed above with regard to FIG. 4 may also be stored in the location table.

[0083] The server **110** may provide AP location information from the location table to users upon request. In addition, when a location is needed for a given client device, the server **110** may obtain relevant data for one or more APs from the location table and either provide them to the client device or perform location calculations for the client device's position.

[0084] By way of example, a client device without geolocation capabilities may perform a scanning or sniffing operation to obtain a list of all APs that can be observed by the client device. This list may then be evaluated against a database of APs such as the aforementioned location table to determine the specific or estimated locations of the observed APs. Given the (likely) AP locations, a location of the client device may be estimated as set forth above.

[0085] In accordance with other aspects of the present invention, the client devices may be stationary or may be moving. In either situation, the data rate between a given client device and a serving AP may change. This may be due to a number of factors such as multipath interference, error rates, etc. For example, a client device may use a maximum data rate (e.g., 54 Mbps) at first to communicate with an AP. If there is no ACK control frame received from the AP, then the client device may drop or back off its data rate to 24 Mpbs or less until it receives the ACK. Thus, in one example, changes in the data rate between a given client device and the AP may be used to refine the distance estimate. As different measurements may occur at different data rates, there may be multiple distance estimates and/or location estimates for a given AP. Statistical processing may be used to arrive at an average distance or most likely location estimate for a given confidence level. In the case where the client device includes a GPS receiver, if that device captures multiple frames relating to an AP, then it may also obtain multiple GPS measurements and use the data rate as a bounding factor. Such measurements of GPS signals and/or frames may be aggregated in a localization process to obtain a more accurate estimate for the AP's location.

[0086] It is also possible to use the frame size and checksum of the frame/packet to estimate distance and accuracy. For instance, the larger the frame size, the more likely it is that the frame may become corrupted during transmission. Thus, if the client device received/sniffs a large frame (e.g., 500 bytes) from an AP, then it is likely that the AP is closer than an average distance for the data rate that packet/frame is being transmitted at. Conversely, if the frame is very small (e.g., 10 bytes or less), then the distance may be farther than the average distance. The average distance may be computed or otherwise determined as part of the development of the look-up table. For instance, a mean value or median value calculation may be performed on multiple data points to arrive at the average distance. Furthermore, the look-up table may be constructed using an analytical model for bit error rate and use that information to determine how far away a device could be so that a packet could be received at a certain data rate. Or, in addition or alternatively, the look-up table could be constructed using experimental data.

[0087] In a further alternative, the WLAN of interest may permit multiple APs to share a single frequency channel, such as in a spread-spectrum based architecture. However, depending on the implementation, the various APs and/or client devices using a particular frequency channel may need to adjust their data rates and/or power levels in order to share the channel while maintaining an acceptable noise or error rate. In this scenario, if there are multiple APs using the same channel and the data rate is relatively low (e.g., at 1 Mbps instead of 54 Mbps), then the distance estimation for a given transmitter may be increased. The amount of increase may be related to the number of APs in the same channel. By way of example only, the distance estimation may be increased by a certain percentage such as on the order of 5-20%.

[0088] FIG. 5 illustrates an alternative scenario **500** wherein there is a single AP **502** and a first client device **504** associated with the AP **502** at a first distance **506** from the AP **502**. The first client device **504** is stationary. In contrast, a second client device **508** moves from a first location at time T_1 to a second location at time T_2. At time T_1 the distance between the client device **508** and the AP **502** is shown by line **510**, while at time T_2 the distance between the client device **508** and the AP **502** is shown by line **512**.

[0089] In accordance with another aspect of the present invention, the system may compare the received signal strength indication ("RSSI") and data rate at time T_1 with the RSSI and data rate at time T_2. The packet decoding success rates at times T_1 and T_2 may be compared and evaluated with the RSSI and data rates to further improve the distance estimation. While only two time points are shown, any number of points may be employed. Thus, the client device **508** may be placed in a vehicle and data may be obtained continuously or at predetermined time increments. Furthermore, the rate of speed of the client device **508** may be factored into the analysis as well.

[0090] In a further example, the client device scanning or sniffing transmitted frames may include a receiver with multiple antennas and/or multiple receive chains. Such architectures may be used to provide spatial and/or temporal diversity and give a "stereo" effect which can improve the accuracy of the triangulation calculations. For instance, in one embodiment two separate receivers are located on either side of a vehicle. Both receivers may be electrically connected a single processing device (e.g., a laptop), and both may scan for data packets simultaneously. As with the moving example discussed with respect to FIG. 5, the difference in RSSI and packet decoding success rate for each receiver may improve the distance estimation. Of course, more than two receivers and/or antennas may be employed.

[0091] FIGS. 6A and 6B illustrate general architectures of wireless devices for use in accordance with the present invention. Specifically, FIG. 6A provides an exemplary GPS-enabled device **600** while FIG. 6B provides an exemplary device **602** which is not GPS enabled. As shown in FIGS. 6A and 6B, each device **600** and **602** may include a transceiver **604** which is operable to send and receive data packets over a Wi-Fi® or other type of WLAN using an antenna **606**. Although a single antenna **606** is shown, multiple antennas (and/or multiple receive chains) may be used for diversity purposes as explained herein.

[0092] Each device may also include a microprocessor or controller **608** and memory **610** for storing instructions and/or data. A user interface **612** may be provided along with one or more applications **614**. The applications **614** may be stored in an application memory (not shown) or may be stored in memory **610**. The key differences as shown between the devices **600** and **602** are the GPS receiver **616** and associated antenna **618** of the device **600**. The GPS receiver **616** may be implemented in hardware, software or some combination. The GPS receiver **616** is used to identify a location of the device **600**. Referring back to the earlier example of FIG. **3**, the client device **308** may be a GPS-enable device such as device **600**, while the client device **306** and/or the AP **302** may be configured without a GPS receiver such as device **602**.

[0093] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims. Furthermore, while particular processes are shown in a specific order in the appended drawings, such processes are not limited to any particular order unless such order is expressly set forth herein.

1. A computer-implemented method of estimating the location of a wireless device, the method comprising:

obtaining a packet of data transmitted from a first wireless device to a second wireless device;

determining whether one of the first and second wireless devices is a wireless access point;

determining the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and

assigning an estimated location to the wireless access point based upon the evaluation.

2. The method of claim **1**, wherein the predetermined criterion is stored in a look-up table and the evaluation includes identifying a distance in the look-up table associated with the determined data rate.

3. The method of claim **1**, wherein:

the transmitted data packet is obtained by a client device; and

the method further includes identifying a distance associated with the data rate, wherein the distance is used as a separation between the first wireless device and the client device.

4. The method of claim **3**, wherein the client device is at a known location and the method further comprises:

assigning a distance between the wireless access point and the client device to be the same as the distance between the first wireless device and the client device; and

triangulating a position of the wireless access device using the known location of the client device, the distance between the first wireless device and the client device and the distance between the wireless access point and the client device to obtain the estimated location.

5. The method of claim **4**, wherein the client device uses a GPS receiver to obtain the known location.

6. The method of claim **1**, wherein the predetermined criterion includes a worst-case distance estimate based upon at least one parameter.

7. The method of claim **6**, wherein the at least one parameter includes one or more of a channel propagation characteristic, a transmitter characteristic and a receiver characteristic.

8. The method of claim **1**, further comprising revising the estimated location of the wireless access point based upon multiple data packets sent or received by the wireless access point.

9. The method of claim 1, further comprising:

determining a position of the client device based upon the estimated location of the wireless access point; and

providing a location-based service to the client device based on the determined position.

10. A computer-implemented method of estimating confidence in a status of a wireless device, the method comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluating the one or more transmitted data packets to identify a frame type for each respective data packet;

identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assigning a confidence value to the identification of the wireless access point.

11. The method of claim **10**, wherein:

if the frame type of at least one of the respective data packets is a management frame, then identifying the first wireless device as a wireless access point; and

setting the confidence value for the identification of the wireless access point to a maximum confidence value.

12. The method of claim **11**, wherein:

if the frame type of at least one of the respective data packets is not the management frame, then evaluating whether the frame type of any of the respective data packets is a control frame;

if the frame type of at least one of the respective data packets is the control frame, then identifying the first wireless device as the wireless access point; and

setting the confidence value for the identification of the wireless access point to a value between the maximum confidence value and a minimum confidence value.

13. The method of claim **10**, wherein identifying the first wireless device or the second wireless device as the wireless access point further includes analyzing a number of frames transmitted or received by each device.

14. A computer-implemented method of estimating confidence in a location of a wireless device, the method comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

determining that the first or second wireless device is a wireless access point based upon the transmitted packets;

determining an estimated location of the wireless access point; and

assigning a confidence value to the estimated location.

15. The method of claim **14**, wherein the confidence value represents a percentage likelihood that the wireless access point is contained within a specified area of interest.

16. The method of claim **14**, wherein the estimated location is based on multiple data points.

17. The method of claim **16**, wherein a confidence code is applied to each data point.

18. The method of claim **17**, wherein the confidence code for each data point is calculated using a weighted function.

19. The method of claim **17**, wherein the confidence code for each data point represents a likelihood that that data point is valid or an outlier.

20. An apparatus including a processor operable to estimate the location of a wireless device, the processor executing a process to:

obtain a packet of data transmitted from a first wireless device to a second wireless device;

determine whether one of the first and second wireless devices is a wireless access point;

determine the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluate the determined data rate against a predetermined criterion; and

assign an estimated location to the wireless access point based upon the evaluation.

21. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating the location of a wireless device, the process comprising:

obtaining a packet of data transmitted from a first wireless device to a second wireless device;

determining whether one of the first and second wireless devices is a wireless access point;

determining the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and

assigning an estimated location to the wireless access point based upon the evaluation.

22. An apparatus including a processor operable to estimate confidence in a status of a wireless device, the processor executing a process to:

obtain one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluate the one or more transmitted data packets to identify a frame type for each respective data packet;

identify the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assign a confidence value to the identification of the wireless access point.

23. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating confidence in a status of a wireless device, the process comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluating the one or more transmitted data packets to identify a frame type for each respective data packet;

identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assigning a confidence value to the identification of the wireless access point.

24. An apparatus including a processor operable to estimate confidence in a location of a wireless device, the processor executing a process to:

obtain one or more packets of data transmitted from a first wireless device to a second wireless device;

determine that the first or second wireless device is a wireless access point based upon the transmitted packets;

determine an estimated location of the wireless access point; and

assign a confidence value to the estimated location.

25. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating confidence in a location of a wireless device, the process comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

determining that the first or second wireless device is a wireless access point based upon the transmitted packets;

determining an estimated location of the wireless access point; and

assigning a confidence value to the estimated location.

26. An apparatus for use in a wireless network, the apparatus comprising:

memory for storing information associated with a plurality of devices in the wireless network;

means for communicating with one or more of the plurality of devices in the wireless network; and

a processor operable to estimate a location of an access point device in the wireless network based upon data packet information sent to or received from the access point device;

wherein the processor is adapted to provide location based service information to one or more client devices associated with the access point device upon estimation of the location.

27. The apparatus of claim **26**, wherein the data packet information for a given data packet includes a data rate of the given data packet, the information stored in the memory includes distance estimates associated with different data rates, and the processor determines the location estimate of the access point device by comparing the data rate of the given data packet to the different data rates and distance estimates stored in the memory.

28. The apparatus of claim **26**, wherein the processor is operable to estimate the location of the access point device using the data packet information for multiple data packets sent to or received from the access point device, and wherein the processor is further operable to rank the data packet information for each of the multiple data packets to obtain approximate distances based upon each such packet.

29. The apparatus of claim **28**, wherein the processor estimates the location using a centroid of the approximate distances.

30. The apparatus of claim **28**, wherein the processor is further operable to assign a confidence in the estimated location of the access point device.

31. The apparatus of claim **30**, wherein the confidence represents a likelihood that the access point device is within a given area.

32. The apparatus of claim **30**, wherein the confidence is based upon at least one of spatial diversity of selected devices associated with the access point device, receiver characteristics of the selected devices, transmitter characteristics of the selected devices, and freshness of information stored in memory or the data packet information sent to or received from the access point device.

33. The apparatus of claim **26**, wherein the processor comprises a plurality of processing devices in a distributed architecture and the memory stores the information so that the information is accessible to one or more of the plurality of processing devices.

* * * * *

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 April 2010 (22.04.2010)

PCT

(10) International Publication Number
WO 2010/044872 A1

(51) International Patent Classification:
H04W 24/00 (2009.01)

(21) International Application Number:
PCT/US2009/005640

(22) International Filing Date:
14 October 2009 (14.10.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
61/196,167 15 October 2008 (15.10.2008) US

(71) Applicant *(for all designated States except US)*: **GOOGLE INC.** [US/US]; 1600 Amphitheatre Parkway, Mountain View, CA 94043 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **YOUSSEF, Adel, Amin** [EG/US]; 1607 Kennedy Drive, Milpitas, CA (US). **MISHRA, Arunesh** [IN/US]; 866 East Evelyn, Sunnyvale, CA 94086 (US). **LIANG, Sam** [US/US]; 840 Mesa Avenue, Palo Alto, CA 94306 (US). **CHU, Michael** [US/US]; 13050 Cumbra Vista Court, Los Altos, CA 94022 (US). **JAIN, Ravi** [US/US]; 1862 Edgewood Drive, Palo Alto, CA 94303 (US).

(74) Agents: **ZIDEL, Andrew T.** et al.; Lerner, David, Littenberg, Krumholz & Mentlik, LLP, 600 South Avenue West, Westfield, NJ 07090 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

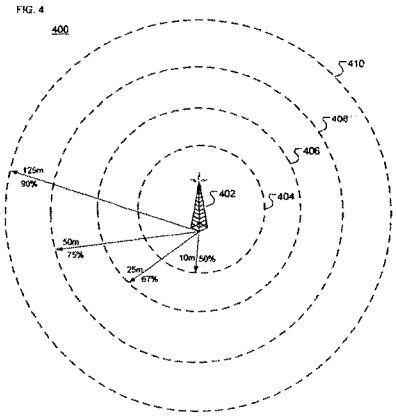
(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— *with international search report (Art. 21(3))*

(54) Title: WIRELESS NETWORK-BASED LOCATION APPROXIMATION

FIG. 4



(57) Abstract: The invention pertains to location approximation of devices, *e.g.*, access points ("APs") (102A, 102B, 102C) and client devices (104A, 104B, 104C) in a wireless network (100). Location estimates may be obtained by observation/analysis of packets (314) transmitted or received by APs. For instance, data rate information associated with a packet is used to approximate the distance between a device and the AP. This may be coupled with known positioning information to estimate an approximate location for the AP. Confidence information and metrics (404, 406, 408, 410) about whether a device is an AP and its location may also be determined. Accuracy of the location determination may be affected by factors including propagation and environmental factors, transmit power, antenna gain and diversity, etc. Location information database (112) of APs may employ measurements from various devices over time. Such information may identify locations of client devices and provide location-based services to them.

WO 2010/044872 A1

WIRELESS NETWORK-BASED LOCATION APPROXIMATION

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority to and claims the benefit of the filing date of United States Provisional Patent Application No. 61/196,167, filed October 15, 2008, entitled "Wireless Network-Based Location Approximation," the entire disclosure of which is hereby incorporated herein by reference.

BACKGROUND OF THE INVENTION

Field of the Invention

[0002] The present invention relates generally to approximating the location of electronic devices such as wireless access points ("APs") and client devices.

Description of Related Art

[0003] Wireless networks offer a wide variety of services using a number of different architectures. Client devices such as mobile phones, laptops and PDAs may connect to APs via cellular/PCS networks as well as wireless local area networks ("WLANs") such as IEEE 802.11, Bluetooth® or other Wi-Fi® networks.

[0004] Location-based services can leverage the physical location of a client device to provide an enhanced service or experience for a user. A location-based service may determine the location of the user by using one of several technologies for determining position, then use the location and possibly other information to provide personalized applications and services.

[0005] Conventional cellular/PCS networks may position their APs (e.g., base stations) in accordance with specific coverage criteria. The locations of these base stations may be placed at known locations. Client devices in such networks may include GPS-enabled handsets, which enable accurate determination of the location of the devices.

[0006] In contrast, WLANs networks may include APs which are relatively small or portable (e.g., mini base stations or wireless routers), and which may be placed at locations as needed. The exact locations of APs in this situation may not be known. For instance, a corporate wireless network may have a number of APs distributed across the corporate campus. So long as the APs provide adequate coverage, a general knowledge of their location such as which building they are in may suffice.

[0007] Another type of scenario where the specific location of the APs may not be known is in a building-wide (e.g., an airport terminal) or city-wide mesh or ad-hoc WiFi network. In such cases, users may access APs set up by one or more service providers.

[0008] In such cases, the APs and client devices themselves may not be GPS-enabled. Or the devices may be located indoors or in other environments where GPS does not operate. Thus, it may be difficult or impossible to offer location-based services without some way to determine the positions of the APs and/or the client devices.

BRIEF SUMMARY OF THE INVENTION

[0009] The present invention provides systems and methods for estimating AP locations as well as estimating the confidence and accuracy for such locations. Using such information, the locations of client devices may also be determined, which in turn enables the use of location-based services.

[0010] In accordance with an embodiment of the present invention, a computer-implemented method of estimating the location of a wireless device is provided. The method comprises obtaining a packet of data transmitted from a first wireless device to a second wireless device; determining whether one of the first and second wireless devices is a wireless access point; determining the data rate of the

transmitted data packet; if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and assigning an estimated location to the wireless access point based upon the evaluation.

[0011] In one alternative, the predetermined criterion is stored in a database such as in a look-up table. Here, the evaluation includes identifying a distance in the look-up table associated with the determined data rate. In one example, the transmitted data packet is obtained by a client device and the method further includes identifying a distance associated with the data rate, wherein the distance is used as a separation between the first wireless device and the client device. Here, if the client device is at a known location, then the method may further comprise assigning a distance between the wireless access point and the client device to be the same as the distance between the first wireless device and the client device; and triangulating a position of the wireless access device using the known location of the client device, the distance between the first wireless device and the client device and the distance between the wireless access point and the client device to obtain the estimated location. In this example, the client device may use a GPS receiver to obtain the known location.

[0012] In another alternative, the predetermined criterion includes a worst-case distance estimate based upon at least one parameter. In an example, the at least one parameter includes one or more of a channel propagation characteristic, a transmitter characteristic and a receiver characteristic.

[0013] In yet another alternative, the method further comprises revising the estimated location of the wireless access point based upon multiple data packets sent or received by the wireless access point.

[0014] In another alternative, the method further comprises determining a position of the client device based upon the estimated location of the wireless access point and providing a location-based service to the client device based on the determined position.

[0015] In accordance with another embodiment of the present invention, a computer-implemented method of estimating confidence in a status of a wireless device is provided. The method comprises obtaining one or more packets of data transmitted from a first wireless device to a second wireless device; evaluating the one or more transmitted data packets to identify a frame type for each respective data packet; identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and assigning a confidence value to the identification of the wireless access point.

[0016] In one alternative, if the frame type of at least one of the respective data packets is a management frame, then identifying the first wireless device as a wireless access point. In this case the method sets the confidence value for the identification of the wireless access point to a maximum confidence value. Optionally, if the frame type of at least one of the respective data packets is not the management frame, then the method evaluates whether the frame type of any of the respective data packets is a control frame. Here, if the frame type of at least one of the respective data packets is the control frame, then the method identifies the first wireless device as the wireless access point and sets the confidence value for the identification of the wireless access point to a value between the maximum confidence value and a minimum confidence value.

[0017] In another alternative, identifying the first wireless device or the second wireless device as the wireless

access point further includes analyzing a number of frames transmitted or received by each device

[0018] In accordance with another embodiment of the present invention, a computer-implemented method of estimating confidence in a location of a wireless device is provided. Here, the method comprises obtaining one or more packets of data transmitted from a first wireless device to a second wireless device; determining that the first or second wireless device is a wireless access point based upon the transmitted packets; determining an estimated location of the wireless access point; and assigning a confidence value to the estimated location.

[0019] In one alternative, the confidence value represents a percentage likelihood that the wireless access point is contained within a specified area of interest. In another alternative, the estimated location is based on multiple data points. In this case, a confidence code may be applied to each data point. In one example, the confidence code for each data point is calculated using a weighted function. In another example, the confidence code for each data point represents a likelihood that that data point is valid or an outlier.

[0020] In yet another embodiment of the present invention, an apparatus for use in a wireless network comprises memory for storing information associated with a plurality of devices in the wireless network, means for communicating with one or more of the plurality of devices in the wireless network and a processor. The processor is operable to estimate a location of an access point device in the wireless network based upon data packet information sent to or received from the access point device. The processor is adapted to provide location based service information to one or more client devices associated with the access point device upon estimation of the location.

[0021] In one alternative, the data packet information for a given data packet includes a data rate of the given data packet. Here, the information stored in the memory includes distance estimates associated with different data rates. The processor determines the location estimate of the access point device by comparing the data rate of the given data packet to the different data rates and distance estimates stored in the memory.

[0022] In another alternative, the processor is operable to estimate the location of the access point device using the data packet information for multiple data packets sent to or received from the access point device. The processor is further operable to rank the data packet information for each of the multiple data packets to obtain approximate distances based upon each such packet. In one example, the processor estimates the location using a centroid of the approximate distances. In another example, the processor is further operable to assign a confidence in the estimated location of the access point device. The confidence may represent a likelihood that the access point device is within a given area. Optionally, the confidence is based upon at least one of spatial diversity of selected devices associated with the access point device, receiver characteristics of the selected devices, transmitter characteristics of the selected devices, and freshness of information stored in memory or the data packet information sent to or received from the access point device.

[0023] In yet another alternative, the processor comprises a plurality of processing devices in a distributed architecture and the memory stores the information so that the information is accessible to one or more of the plurality of processing devices.

[0024] Each of the aforementioned methods and processes may be performed by a processor such as a CPU, microprocessor,

ASIC or other computing device. Furthermore, such methods and processes may be stored on a computer-readable recording medium (e.g., CD-ROM, DVD, Blue Ray disc, flash memory or the like) for execution by a processor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0025] FIG. 1 illustrates an exemplary wireless network in accordance with aspects of the present invention.

[0026] FIG. 2 illustrates aspects of a wireless network in accordance with aspects of the present invention.

[0027] FIG. 3 illustrates an exemplary configuration for estimating device location in accordance with aspects of the present invention.

[0028] FIG. 4 illustrates an exemplary confidence and positioning diagram in accordance with aspects of the present invention.

[0029] FIG. 5 illustrates an exemplary dynamic scenario for location estimation.

[0030] FIGS. 6A-B illustrate exemplary wireless devices for use with aspects of the present invention.

DETAILED DESCRIPTION

[0031] The aspects, features and advantages of the present invention will be appreciated when considered with reference to the following description of preferred embodiments and accompanying figures. The same reference numbers in different drawings may identify the same or similar elements. Furthermore, the following description does not limit the present invention; rather, the scope of the invention is defined by the appended claims and equivalents.

[0032] FIG. 1 provides an exemplary WLAN 100 which may have a number of APs 102 (e.g., 102A, 102B and 102C) as well as one or more client devices 104 (e.g., 104A, 104B and 104C) as shown. The APs 102 may include devices of different types from various manufacturers and may have different capabilities. Some APs 102 may be wireless routers that can

support dozens of client devices or more, while some APs may act as signal repeaters. The client devices 104 may also be of different types and have different capabilities. For instance, as shown client device 104A may be a PDA, 104B may be a laptop/notebook computer, and 104C may be a mobile phone.

[0033] The WLAN 100 may also include a server 110 that is in wired or wireless communication with some or all of the APs 102. A database 112 may be associated with the server 110. The database 112 may be used to store data related to the APs 102 and/or the client devices 104. For instance, the database 112 may maintain location-related records for the APs 102.

[0034] Each AP 102, each client device 104 and the server 110 may contain at least one processor, memory and other components typically present in a computer. FIG. 2 illustrates an alternative view 200 of a single AP 102, a single client device 104 and server 110 identifying such components. As shown, the AP 102 includes a processor 202 and memory 204. Components such as a transceiver, power supply and the like are not shown in any of the devices of FIG. 2.

[0035] Memory 204 stores information accessible by the processor 202, including instructions 206 that may be executed by the processor 202 and data 208 that may be retrieved, manipulated or stored by the processor. The memory may be of any type capable of storing information accessible by the processor, such as a hard-drive, ROM, RAM, CD-ROM, flash memories, write-capable or read-only memories. The processor 202 may comprise any number of well known processors, such as processors from Intel Corporation. Alternatively, the processor may be a dedicated controller for executing operations, such as an ASIC.

[0036] The instructions 206 may comprise any set of instructions to be executed directly (such as machine code) or indirectly (such as scripts) by the processor. In that regard, the terms "instructions," "steps" and "programs" may

be used interchangeably herein. The instructions may be stored in any computer language or format, such as in object code or modules of source code. The functions, methods and routines of instructions in accordance with the present invention are explained in more detail below.

[0037] Data 208 may be retrieved, stored or modified by processor 202 in accordance with the instructions 206. The data may be stored as a collection of data. For instance, although the invention is not limited by any particular data structure, the data may be stored in computer registers, in a relational database as a table having a plurality of different fields and records.

[0038] The data may also be formatted in any computer readable format such as, but not limited to, binary values, ASCII or EBCDIC (Extended Binary-Coded Decimal Interchange Code). Moreover, the data may include any information sufficient to identify the relevant information, such as descriptive text, proprietary codes, pointers, references to data stored in other memories (including other network locations) or information which is used by a function to calculate the relevant data.

[0039] Although the processor 202 and memory 204 are functionally illustrated in FIG. 2 as being within the same block, it will be understood that the processor and memory may actually comprise multiple processors and memories that may or may not be stored within the same physical housing or location. For example, some or all of the instructions and data may be stored on a removable CD-ROM and others within a read-only computer chip. Some or all of the instructions and data may be stored in a location physically remote from, yet still accessible by, the processor 202. Similarly, the processor 202 may actually comprise a collection of processors which may or may not operate in parallel. Data may be

distributed and stored across multiple memories 204 such as hard drives or the like.

[0040] In one aspect, AP 102 communicates with one or more client devices 104 and the server 110 via wireless network 210 (e.g., a Wi-Fi®-type network such as an 802.11g network or a Bluetooth®-type network). Each client device 104 and the server 110 may be configured similarly to the AP 102 with a processor 202, memory 204 and instructions 206, as well as one or more user input devices 212 and a user output device, such as display 214. Each client device 104 and the server 110 may be a general purpose computer, intended for use by a person, having all the components normally found in a personal computer such as a central processing unit ("CPU"), display, CD-ROM or DVD drive, hard-drive, mouse, keyboard, touch-sensitive screen, speakers, microphone, wireless modem and all of the components used for connecting these elements to one another.

[0041] Each device on the network 100 may transmit and receive data (packets) according to a known protocol in a segment (channel) of allotted portion the spectrum (frequency band). For instance, the IEEE 802.11 series of protocols specifies the format of various types of packets which may be transmitted in preset channels of the spectrum, such as the ISM band located in the 2.4 GHz frequency range or the public safety band located in the 4.9 GHz frequency range.

[0042] Depending upon their configuration, each AP may have a coverage area 106 such as coverage areas 106A, 106B and 106C as shown in FIG. 1. In many instances the coverage areas 106 of adjacent APs 102 may overlap, such as shown by overlap region 108. It should be understood that the coverage areas 106 in real-world implementations may be affected due to transmit power requirements, signal attenuation, multipath and other factors.

[0043] As discussed above, it is desirable to provide location-based services to client devices. While some client devices may include a GPS receiver or some other tool to determine and/or communicate the device's location, many client devices may not have such equipment or capabilities. Thus, in accordance with one aspect of the present invention, the location of a given client device may be determined based upon the location(s) of one or more APs, either alone or in conjunction with other network-related information.

[0044] In such a scenario, one important issue is that in many instances the specific location of an AP 102 may not be known. Therefore, in accordance with another aspect of the present invention, systems and methods are provided to estimate an AP's location using data rate information between the AP and one or more client devices. FIG. 3 illustrates an exemplary configuration 300 with a single AP 302 having a coverage area 304. A first client device 306 and a second client device 308 are located within the coverage area 304.

[0045] In the present example, the client device 306 may be "associated" with the AP 302, transmitting packets to and receiving packets from the AP 302. Here, the client device 306 is not GPS enabled and is not otherwise configured to determine its location. In contrast, the client device 308 may include a GPS receiver or other means of performing geolocation.

[0046] In this example, the client device 306 is located a first distance 310 from the AP 302, while the client device 308 is located a second distance 312 from the AP. And the client device 306 is located a third distance 316 from the client device 308. The client device 308 performs geolocation using its GPS receiver or by other means to accurately determine its location.

[0047] Furthermore, the client device 308 may be configured to observe or capture data packets such as frame 314

transmitted to or from the AP 302. By way of example, the client device 308 may be a laptop having a wireless transceiver that can operate in a "sniffer" or "monitor" mode, thereby handling transmitted frames 314 without requiring the client device 308 to be associated with the AP 302.

[0048] In accordance with one embodiment, the client device 308 receives and captures the frame(s) 314. The client device 308 may analyze the frame 314, such as with an analyzer program executed by its processor. Alternatively, the server 110 may execute the analyzer program. The analyzer program may parse different portions of the frame 314 and perform error checking on the frame 314. As part of the analysis, it is determined which device (e.g., AP 302 or client device 306) transmitted the frame 314, as well as the data rate at which the transmitter sent the frame 314. The data rate may be identified by data in the frame 314 itself or may be otherwise identifiable. For example, the data rate is the rate of transmission from the AP 302 to the client device 306 or from the client device 306 to the AP 302. Alternatively, if the client device 308 is associated with the AP 302 and is communicating with the AP 302 (as opposed to merely sniffing packets), then the data rate may be the rate transmitted from the AP 302 to the client device 308 or from the client device 308 to the AP 302.

[0049] Using this information, the client device 308 or the server 110 may estimate the distance of the client device 308 relative to the AP 302 and/or the client device 306. For instance, the data rate may be used as an estimate of channel quality to indicate the physical separation between client device 308 and the AP 302 or between the client device 308 and the client device 306. In one example, a look-up table may be used to estimate the distance. An exemplary look-up table is provided below.

Rate	Distance
5 Mbps	250 meters
10 Mbps	125 meters
54 Mbps	30 meters

[0050] As shown in this example, the higher the data rate, the shorter the distance. However, the distance may be adjusted by various parameters as will be discussed below. The distances in the look-up table may be approximated using a worst-case estimate based on various channel parameters such as propagation characteristics, transmit power, antenna gain, receiver sensitivity and other radio characteristics for both the transmitter and receiver, as well as terrain type, etc.

[0051] In accordance with another aspect, so long as the client device 308 is able to capture and properly decode a packet containing a transmitted frame, then it is determined that the distance between the client device 308 and the transmitting entity (e.g., AP 302 or client device 306) must fall within the worst-case estimate. If the client device 308 is not associated with the AP 302, then some platforms may not provide or process certain frames. In the case where client device 308 is associated with the AP 302, then more information about the AP 302 may be available which can be used to improve the accuracy of the AP's location. For instance, in addition to the frames that client device 308 observes between the AP 302 and the client device 306, client device 308 also has frames transmitted to itself by the AP 302. These frames also have data rate information associated with them, so this is another opportunity to obtain an estimate of the distance between the AP 302 and the client device 308.

[0052] Thus, in one alternative the frame(s) observed between AP 302 and client device 306 provide a first estimate or multiple estimates which can be used to determine a first

approximate distance 312, while the frame(s) received by the client device 308 from AP 302 provide a first estimate or multiple estimates which can be used to determine a second approximate distance 312. In this case, weights or rankings may be applied to the first and second approximate distances to arrive at a resultant distance 312. Of course, it should be understood that there may be other client devices within the area 304 in communication with the AP 302. In that situation, there may be even more approximate distances 312 calculated/weighted to arrive at an even more accurate resultant distance 312.

[0053] If the packet cannot be decoded or is decoded with uncorrectable errors, then the distance approximation may not be performed. Alternatively, if the packet cannot be decoded properly, it may be inferred that the distance 312 between AP 302 and client device 308 is greater than the distance 310 between the AP 302 and the client device 306.

[0054] The above look-up table may be supplemented or otherwise parameterized based upon additional factors besides distance. For instance, the table can be parameterized based upon the transmit power values of the transmitter. Or if the transmit power values are unknown, a certain distribution of common transmit power values can be used as an approximation. The table can also be parameterized based upon the environment where the packet/frame was captured. For example, in a dense urban environment, one may expect a high multipath coefficient. On the other hand, in a rural environment, one may expect the propagation pattern to be very symmetric, leading to larger distances for the same data rate. The table could also be parameterized based upon the receiver's radio characteristics, such as the sensitivity, antenna gain and any diversity metrics (e.g., multiple antennas) which may be applicable.

[0055] Calibration or otherwise updating of the look-up table may be done based on the power, radio sensitivity and/or vendor information of the various devices. For instance, different radios may have very different RF characteristics. Some APs are operable to transmit at higher power than others. Thus, at the same data rate, a higher power AP may be located farther away than a lower power AP.

[0056] Similarly, it may be beneficial to evaluate the sensitivity of the receiver of the client device 308. By way of example, a dedicated sniffer/scanner may have a much higher gain antenna/receive chain than the radio receiver on a laptop, which in turn may have a higher gain than the radio on a cellular phone.

[0057] Vendor and model information for a given device and its radio/receiver may be determined based upon the device's MAC address (e.g., using the object identifier ("OID")) and frames transmitted by the device. This in turn may be used to evaluate the power and sensitivity of the radio/receiver.

[0058] Once the packet containing a frame is properly decoded, the frame may be examined to determine whether it was sent by the AP 302 or the client device 306 (or some other entity). This information may provide additional insight into the specifications of the particular AP 302 or client device 306. For instance, if the frame information identifies the AP 302 as being of a specific type, then that may indicate the power level(s) at which the AP 302 operates.

[0059] If the decoded frame was sent by the AP 302, then the distance determined using the look-up table gives an accurate upper bound on the separation between the client device 308 and the AP 302. This is coupled with the location of the client device 308 provided by its self-geolocation. Thus, starting with the client device 308 at a center point of a circle similar to the coverage area 304, the AP 302 can be

determined to be within a radius of the circle, where the radius is the distance identified by the look-up table.

[0060] If the decoded frame was sent by the client device 306, then the distance determined using the look-up table identifies the maximum separation between the client device 306 and the client device 308. Similarly, the distance determined using the data rate (and possibly other information) in the look-up table also provides the maximum separation between the client device 306 and the AP 302. Using the geometrical principal known as the Triangle Inequality, the maximum separation between the AP 302 and the client device 308 is no more than twice the distance determined using the look-up table.

[0061] As discussed above, because the client device 308 has a GPS receiver or can otherwise determine its position using geolocation, the location of client device 308 is known. Thus, in accordance with another aspect of the invention, the location of the AP 302 is determined by triangulating using the distance between the client devices 306 and 308 and the distance between the AP 302 and the client device 308.

[0062] This process may be repeated by analyzing multiple packets sent between the AP 302 and the client device 306 (or other client devices falling within the coverage area 304. Multiple estimates of the location of the AP 302 may be made by the client device 308 and/or other client devices having geolocation capabilities.

[0063] Alternatively, an estimate of the location of the AP 302 may be performed using a centroid (mean location) of multiple points associated with the AP 302. These points may correspond to locations obtained by the same or different client devices 308 using the AP 302 at the same or different times. A coverage radius of the AP 302 may also be estimated so that most or all the points in a collection are covered.

[0064] Once a given packet/frame has been captured and decoded by the client device 308, then the location estimation process for the AP 302 may be done by the client device 308, the AP 302 or other entity such as server 110 of FIG. 1. By way of example only, the look-up table may be stored in database 112. This database may be accessible only to the server 110, to some or all of the APs 102, and/or to some or all of the client devices 104. Alternatively, the database 112 may be a distributed database spread among various nodes of the wireless network, including some of the APs 102 and/or the server 110.

[0065] Returning to FIG. 3, once the location of the AP 302 has been estimated, then that information may be used to provide location-based services to the client device 306. For instance, this may be done relying solely on the location of the AP 302, and that location estimate is used when offering location-enabled features to the user of the client device 306. Alternatively, the location of the client device 306 itself may be determined using the processes discussed above with regard to the AP 302. Here, for example, once the AP 302 location has been estimated, the Triangle Inequality or other geolocation technique (e.g., time difference of arrival ("TDOA"), angle of arrival ("AOA"), etc.) may be used to estimate the location of the client device 306. As above, repeated measurements may be used to determine the location before or during offering location-enabled services to the user of the client device 306.

[0066] In accordance with other aspects of the present invention, the confidence of the location of an AP may be estimated. The confidence determination may include an evaluation as to whether the transmitting entity is in fact an AP. And the confidence determination may evaluation the relative accuracy of the physical location for that transmitting entity.

[0067] In one evaluation, it is important to determine whether the device of interest is really an AP. This may be done by evaluating different types of frames sent to (or received from) the device of interest. Depending upon the protocol of the WLAN, there may be management frames, control frames, data frames, etc. which are sent and received by devices in the network. In the example of FIG. 3, if the client device 308 decodes a management frame such as a beacon frame, then it is determined that the transmitting entity is the AP 302. However, if the decoded frame is a control frame such as a "Request To Send" ("RTS"), "Clear to Send" ("CTS"), "Acknowledgement" ("ACK"), "Power Save - Poll" ("PS-POLL"), or "Contention Free - End" ("CF-END"), then the transmitter may or may not be the AP 302.

[0068] Another indicator of whether the device of interest is the AP 302 is the number of frames it transmits. For example, a high number of frames such as control frames sent over a short period of time (e.g., 100 control frames sent in 2 minutes) may suggest that the device is an AP. Similarly, a high number of frames received may also suggest that the device is an AP.

[0069] Data and metrics concerning the device of interest may be obtained by various client devices 308 at the same or different periods of time. Such information may be stored in a database such as database 112. These various indicators are analyzed to provide some value of confidence that the device is an AP. By way of example only, the confidence may be expressed as a percentage value (e.g., 90%) that the device of interest is an AP. An exemplary algorithm may rely on a number of factors to obtain confidence levels/values. For instance, spatial, temporal and/or platform diversity of GPS measurements would be relevant. Also, the types of frames that are used in the measurement, such as data frames, management frames and/or control frames may affect the

confidence. And the source of the measurement may be a relevant factor, such as if it is a trusted party providing the readings versus uploading them through an Open API implementation.

[0070] In another evaluation, the confidence in the location of the AP 302 is determined. Here, the confidence may be expressed as a percentage, e.g., that it is 90% likely that the device of interest is within a certain radius/area). Factors affecting this analysis include spatial diversity of the different client devices which interact with the AP. In addition, whether the client devices are of different types may be relevant to the evaluation. For instance, the antenna gain and overall robustness of the receiver may impact the accuracy of the measurements taken. Here, the data taken by a high quality receiver with multiple spatially diverse antennas having high gain may be given a higher weight in the analysis than data taken from a receiver with a single, low gain antenna.

[0071] Furthermore, the accuracy of the GPS or other geolocation measurements may affect the accuracy calculation. Here, for instance, a differential GPS receiver may be determine the client device 308's position to within a meter or less, while a non-differential GPS receiver may determine the position to within 5-25 meters or more. In addition, while the accuracy of a GPS measurement outdoors with a clear view of the sky may be close to optimum, performance degradations may occur in urban canyon environments where fewer satellites are "visible" and especially when the GPS receiver is located indoors. In the latter case, the GPS receiver may be unable to fix a location at all. Also the "freshness" of the data collected may be relevant to the confidence determination. Here, more recent data may be given a higher weight in the analysis than older data. As above, an exemplary algorithm may rely on a number of additional

factors to obtain accuracy. For instance, spatial, temporal and/or platform diversity of GPS measurements would be relevant. Also, the types of frames that are used in the measurement, such as data frames, management frames and/or control frames may affect the confidence. And the source of the measurement may be a relevant factor, such as if it is a trusted party providing the readings versus uploading them through an Open API implementation.

[0072] In accordance with another aspect of the present invention, processes to determine the accuracy of AP locations are provided. In one embodiment, the measurements taken by various client devices determine a confidence that a given AP is within a certain area. One or more data points represented the expected position of the given AP may be calculated based upon the various factors discussed herein. A "confidence code" may be applied to each data point.

[0073] The confidence code may be calculated using a weighted function. The weights used by the weighted function may be obtained based on information of the collected data such as size of the collection (e.g., the cardinality or number of points in the collection), platform information of the client devices, temporal and/or spatial diversity of the points corresponding to the client devices, etc. One or more estimates of the location of the AP may be adjusted based on the calculated confidence code. A Monte Carlo-type analysis may also be performed.

[0074] In order to provide more accurate estimation of AP locations and coverage regions, several factors can be taken into account to analyze the accuracy of such estimations. The factors may include the number of points, platform information of corresponding client devices, temporal diversity of the points, spatial diversity of the points, etc. For example, the estimated location for a given AP will be more accurate when using more points for the estimation.

[0075] More variety of platforms of client devices indicates more users for the AP, and may increase the accuracy of the estimation. With regard to temporal diversity, points spanning multiple distinct times may contribute to a more accurate estimation than points spanning fewer distinct times. Also, with regard to spatial diversity, more accurate estimation can be achieved by using points spread in a larger space than points clustered in a smaller area. A weight function can be used to calculate a confidence code based on the above information. Accordingly, the estimated location and coverage radius for the given AP can be adjusted based on the confidence code.

[0076] In one example, the confidence code represents the likelihood that a particular data point is valid or an outlier. For instance, this may be expressed as a percentage (e.g., 90% likely that the data point is valid), as a ranking (e.g., a 4 on a scale of 1-5, with 1 being the lowest confidence and 5 being the highest confidence), or some other relative indicator. The confidence code may then be used to discard outliers. Once this is done, the system may compute a "best circle" representing the likely position of the AP of interest.

[0077] In an alternative, multiple circles may be provided as shown in the confidence and positioning diagram 400 of FIG. 4. In this example, AP 402 may be placed in the center of multiple concentric circles 404, 406, 408 and 410. Each circle may be associated with both an area and a confidence value. For instance, the innermost circle 404 may indicate that there is a 50% likelihood that the AP 402 is within 10 meters of the epicenter of that circle. The next smallest circle 406 may be used to indicate that there is a 67% likelihood of the AP 402 being within 25 meters of the epicenter of that circle. The next circle 408 may be used to indicate that there is a 75% likelihood of the AP 402 being

within 50 meters of the epicenter of that circle. And the outermost circle 410 may be used to indicate that there is a 90% chance of the AP 402 being within 125 meters of the epicenter of that circle. In one example, an $O(n^2)$ algorithm may be used to detect outliers. This may be done as follows. First, the centroid of a given number of points may be computed. Then for each point, its distance to the centroid may be computed. If the distance for a given point exceeds a threshold, then the point may be marked or otherwise identified as an outlier. The process may be refined by removing some/all outliers and repeating the above. This may be repeated until there are no more outliers or the algorithm converges.

[0078] As discussed herein, the location of a given AP may be based on a number of measurements taken by one or more client devices. The raw data collected by a client device may be processed locally or sent to a central repository (e.g., server 110 of FIG. 1) for processing. Regardless of which device performs the calculations, each distance and/or each location estimate may be stored in a database, for instance as part of a location table. The location table may store, for one or more APs, a unique identifier for the AP (such as a MAC address, IP address or SSID), a location estimate (e.g., latitude and longitude coordinates and/or height), a time the location estimate was obtained/calculated, a coverage radius for the AP, a confidence for the location estimate (e.g., 90% likely to be within 50 meters of the specific position), equipment type (e.g., transceiver make/model) and/or RSSI information. If multiple location measurements are made, some or all of them may be stored in the location table. Calculated locations and associated estimates such as discussed above with regard to FIG. 4 may also be stored in the location table.

[0079] The server 110 may provide AP location information from the location table to users upon request. In addition, when a location is needed for a given client device, the server 110 may obtain relevant data for one or more APs from the location table and either provide them to the client device or perform location calculations for the client device's position.

[0080] By way of example, a client device without geolocation capabilities may perform a scanning or sniffing operation to obtain a list of all APs that can be observed by the client device. This list may then be evaluated against a database of APs such as the aforementioned location table to determine the specific or estimated locations of the observed APs. Given the (likely) AP locations, a location of the client device may be estimated as set forth above.

[0081] In accordance with other aspects of the present invention, the client devices may be stationary or may be moving. In either situation, the data rate between a given client device and a serving AP may change. This may be due to a number of factors such as multipath interference, error rates, etc. For example, a client device may use a maximum data rate (e.g., 54 Mbps) at first to communicate with an AP. If there is no ACK control frame received from the AP, then the client device may drop or back off its data rate to 24 Mpbs or less until it receives the ACK. Thus, in one example, changes in the data rate between a given client device and the AP may be used to refine the distance estimate. As different measurements may occur at different data rates, there may be multiple distance estimates and/or location estimates for a given AP. Statistical processing may be used to arrive at an average distance or most likely location estimate for a given confidence level. In the case where the client device includes a GPS receiver, if that device captures multiple frames relating to an AP, then it may also obtain multiple GPS

measurements and use the data rate as a bounding factor. Such measurements of GPS signals and/or frames may be aggregated in a localization process to obtain a more accurate estimate for the AP's location.

[0082] It is also possible to use the frame size and checksum of the frame/packet to estimate distance and accuracy. For instance, the larger the frame size, the more likely it is that the frame may become corrupted during transmission. Thus, if the client device received/sniffs a large frame (e.g., 500 bytes) from an AP, then it is likely that the AP is closer than an average distance for the data rate that packet/frame is being transmitted at. Conversely, if the frame is very small (e.g., 10 bytes or less), then the distance may be farther than the average distance. The average distance may be computed or otherwise determined as part of the development of the look-up table. For instance, a mean value or median value calculation may be performed on multiple data points to arrive at the average distance. Furthermore, the look-up table may be constructed using an analytical model for bit error rate and use that information to determine how far away a device could be so that a packet could be received at a certain data rate. Or, in addition or alternatively, the look-up table could be constructed using experimental data.

[0083] In a further alternative, the WLAN of interest may permit multiple APs to share a single frequency channel, such as in a spread-spectrum based architecture. However, depending on the implementation, the various APs and/or client devices using a particular frequency channel may need to adjust their data rates and/or power levels in order to share the channel while maintaining an acceptable noise or error rate. In this scenario, if there are multiple APs using the same channel and the data rate is relatively low (e.g., at 1 Mbps instead of 54 Mbps), then the distance estimation for a

given transmitter may be increased. The amount of increase may be related to the number of APs in the same channel. By way of example only, the distance estimation may be increased by a certain percentage such as on the order of 5-20%.

[0084] FIG. 5 illustrates an alternative scenario 500 wherein there is a single AP 502 and a first client device 504 associated with the AP 502 at a first distance 506 from the AP 502. The first client device 504 is stationary. In contrast, a second client device 508 moves from a first location at time T_1 to a second location at time T_2. At time T_1 the distance between the client device 508 and the AP 502 is shown by line 510, while at time T_2 the distance between the client device 508 and the AP 502 is shown by line 512.

[0085] In accordance with another aspect of the present invention, the system may compare the received signal strength indication ("RSSI") and data rate at time T_1 with the RSSI and data rate at time T_2. The packet decoding success rates at times T_1 and T_2 may be compared and evaluated with the RSSI and data rates to further improve the distance estimation. While only two time points are shown, any number of points may be employed. Thus, the client device 508 may be placed in a vehicle and data may be obtained continuously or at predetermined time increments. Furthermore, the rate of speed of the client device 508 may be factored into the analysis as well.

[0086] In a further example, the client device scanning or sniffing transmitted frames may include a receiver with multiple antennas and/or multiple receive chains. Such architectures may be used to provide spatial and/or temporal diversity and give a "stereo" effect which can improve the accuracy of the triangulation calculations. For instance, in one embodiment two separate receivers are located on either side of a vehicle. Both receivers may be electrically connected a single processing device (e.g., a laptop), and

both may scan for data packets simultaneously. As with the moving example discussed with respect to FIG. 5, the difference in RSSI and packet decoding success rate for each receiver may improve the distance estimation. Of course, more than two receivers and/or antennas may be employed.

[0087] FIGS. 6A and 6B illustrate general architectures of wireless devices for use in accordance with the present invention. Specifically, FIG. 6A provides an exemplary GPS-enabled device 600 while FIG. 6B provides an exemplary device 602 which is not GPS enabled. As shown in FIGS. 6A and 6B, each device 600 and 602 may include a transceiver 604 which is operable to send and receive data packets over a Wi-Fi® or other type of WLAN using an antenna 606. Although a single antenna 606 is shown, multiple antennas (and/or multiple receive chains) may be used for diversity purposes as explained herein.

[0088] Each device may also include a microprocessor or controller 608 and memory 610 for storing instructions and/or data. A user interface 612 may be provided along with one or more applications 614. The applications 614 may be stored in an application memory (not shown) or may be stored in memory 610. The key differences as shown between the devices 600 and 602 are the GPS receiver 616 and associated antenna 618 of the device 600. The GPS receiver 616 may be implemented in hardware, software or some combination. The GPS receiver 616 is used to identify a location of the device 600. Referring back to the earlier example of FIG. 3, the client device 308 may be a GPS-enable device such as device 600, while the client device 306 and/or the AP 302 may be configured without a GPS receiver such as device 602.

[0089] Although the invention herein has been described with reference to particular embodiments, it is to be understood that these embodiments are merely illustrative of the principles and applications of the present invention. It

is therefore to be understood that numerous modifications may be made to the illustrative embodiments and that other arrangements may be devised without departing from the spirit and scope of the present invention as defined by the appended claims. Furthermore, while particular processes are shown in a specific order in the appended drawings, such processes are not limited to any particular order unless such order is expressly set forth herein.

INDUSTRIAL APPLICABILITY

[0090] The present invention enjoys wide industrial applicability including, but not limited to, network services and applications for wireless devices.

CLAIMS

1. A computer-implemented method of estimating the location of a wireless device, the method comprising:

obtaining a packet of data transmitted from a first wireless device to a second wireless device;

determining whether one of the first and second wireless devices is a wireless access point;

determining the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and

assigning an estimated location to the wireless access point based upon the evaluation.

2. The method of claim 1, wherein the predetermined criterion is stored in a look-up table and the evaluation includes identifying a distance in the look-up table associated with the determined data rate.

3. The method of claim 1, wherein:

the transmitted data packet is obtained by a client device; and

the method further includes identifying a distance associated with the data rate, wherein the distance is used as a separation between the first wireless device and the client device.

4. The method of claim 3, wherein the client device is at a known location and the method further comprises:

assigning a distance between the wireless access point and the client device to be the same as the distance between the first wireless device and the client device; and

triangulating a position of the wireless access device using the known location of the client device, the distance between the first wireless device and the client device and the distance between the wireless access point and the client device to obtain the estimated location.

5. The method of claim 4, wherein the client device uses a GPS receiver to obtain the known location.

6. The method of claim 1, wherein the predetermined criterion includes a worst-case distance estimate based upon at least one parameter.

7. The method of claim 6, wherein the at least one parameter includes one or more of a channel propagation characteristic, a transmitter characteristic and a receiver characteristic.

8. The method of claim 1, further comprising revising the estimated location of the wireless access point based upon multiple data packets sent or received by the wireless access point.

9. The method of claim 1, further comprising:

determining a position of the client device based upon the estimated location of the wireless access point; and

providing a location-based service to the client device based on the determined position.

10. A computer-implemented method of estimating confidence in a status of a wireless device, the method comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluating the one or more transmitted data packets to identify a frame type for each respective data packet;

identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assigning a confidence value to the identification of the wireless access point.

11. The method of claim 10, wherein:

if the frame type of at least one of the respective data packets is a management frame, then identifying the first wireless device as a wireless access point; and

setting the confidence value for the identification of the wireless access point to a maximum confidence value.

12. The method of claim 11, wherein:

if the frame type of at least one of the respective data packets is not the management frame, then evaluating whether the frame type of any of the respective data packets is a control frame;

if the frame type of at least one of the respective data packets is the control frame, then identifying the first wireless device as the wireless access point; and

setting the confidence value for the identification of the wireless access point to a value between the maximum confidence value and a minimum confidence value.

13. The method of claim 10, wherein identifying the first wireless device or the second wireless device as the wireless access point further includes analyzing a number of frames transmitted or received by each device.

14. A computer-implemented method of estimating confidence in a location of a wireless device, the method comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

determining that the first or second wireless device is a wireless access point based upon the transmitted packets;

determining an estimated location of the wireless access point; and

assigning a confidence value to the estimated location.

15. The method of claim 14, wherein the confidence value represents a percentage likelihood that the wireless access point is contained within a specified area of interest.

16. The method of claim 14, wherein the estimated location is based on multiple data points.

17. The method of claim 16, wherein a confidence code is applied to each data point.

18. The method of claim 17, wherein the confidence code for each data point is calculated using a weighted function.

19. The method of claim 17, wherein the confidence code for each data point represents a likelihood that that data point is valid or an outlier.

20. An apparatus including a processor operable to estimate the location of a wireless device, the processor executing a process to:

obtain a packet of data transmitted from a first wireless device to a second wireless device;

determine whether one of the first and second wireless devices is a wireless access point;

determine the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluate the determined data rate against a predetermined criterion; and

assign an estimated location to the wireless access point based upon the evaluation.

21. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating the location of a wireless device, the process comprising:

obtaining a packet of data transmitted from a first wireless device to a second wireless device;

determining whether one of the first and second wireless devices is a wireless access point;

determining the data rate of the transmitted data packet;

if one of the first and second wireless devices is the wireless access point, then evaluating the determined data rate against a predetermined criterion; and

assigning an estimated location to the wireless access point based upon the evaluation.

22. An apparatus including a processor operable to estimate confidence in a status of a wireless device, the processor executing a process to:

obtain one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluate the one or more transmitted data packets to identify a frame type for each respective data packet;

identify the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assign a confidence value to the identification of the wireless access point.

23. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating confidence in a status of a wireless device, the process comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

evaluating the one or more transmitted data packets to identify a frame type for each respective data packet;

identifying the first wireless device or the second wireless device as a wireless access point based upon the identified frame type for at least one of the data packets; and

assigning a confidence value to the identification of the wireless access point.

24. An apparatus including a processor operable to estimate confidence in a location of a wireless device, the processor executing a process to:

obtain one or more packets of data transmitted from a first wireless device to a second wireless device;

determine that the first or second wireless device is a wireless access point based upon the transmitted packets;

determine an estimated location of the wireless access point; and

assign a confidence value to the estimated location.

25. A computer-readable recording medium recorded with a computer program for use by a processor to perform a process of estimating confidence in a location of a wireless device, the process comprising:

obtaining one or more packets of data transmitted from a first wireless device to a second wireless device;

determining that the first or second wireless device is a wireless access point based upon the transmitted packets;

determining an estimated location of the wireless access point; and

assigning a confidence value to the estimated location.

26. An apparatus for use in a wireless network, the apparatus comprising:

memory for storing information associated with a plurality of devices in the wireless network;

means for communicating with one or more of the plurality of devices in the wireless network; and

a processor operable to estimate a location of an access point device in the wireless network based upon data packet information sent to or received from the access point device;

wherein the processor is adapted to provide location based service information to one or more client devices associated with the access point device upon estimation of the location.

27. The apparatus of claim 26, wherein the data packet information for a given data packet includes a data rate of the given data packet, the information stored in the memory includes distance estimates associated with different data rates, and the processor determines the location estimate of the access point device by comparing the data rate of the

given data packet to the different data rates and distance estimates stored in the memory.

28. The apparatus of claim 26, wherein the processor is operable to estimate the location of the access point device using the data packet information for multiple data packets sent to or received from the access point device, and wherein the processor is further operable to rank the data packet information for each of the multiple data packets to obtain approximate distances based upon each such packet.

29. The apparatus of claim 28, wherein the processor estimates the location using a centroid of the approximate distances.

30. The apparatus of claim 28, wherein the processor is further operable to assign a confidence in the estimated location of the access point device.

31. The apparatus of claim 30, wherein the confidence represents a likelihood that the access point device is within a given area.

32. The apparatus of claim 30, wherein the confidence is based upon at least one of spatial diversity of selected devices associated with the access point device, receiver characteristics of the selected devices, transmitter characteristics of the selected devices, and freshness of information stored in memory or the data packet information sent to or received from the access point device.

33. The apparatus of claim 26, wherein the processor comprises a plurality of processing devices in a distributed architecture and the memory stores the information so that the

information is accessible to one or more of the plurality of processing devices.

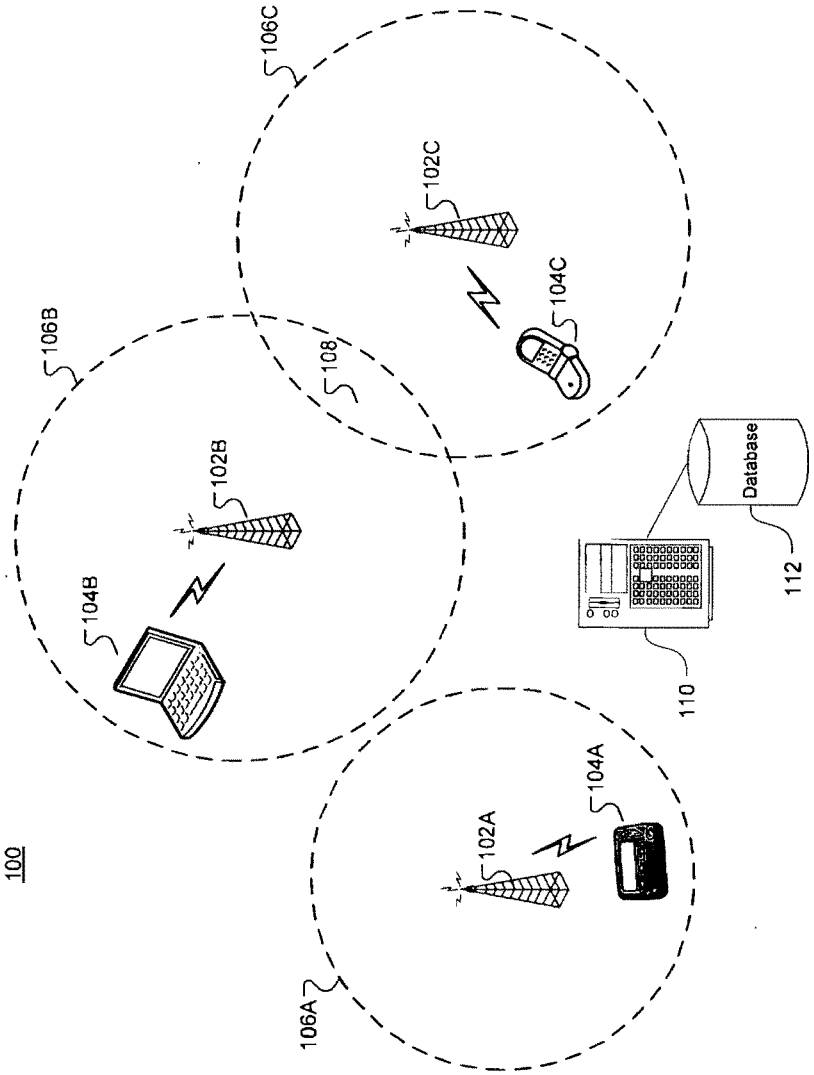

100
106A
106B
106C
102A
102B
102C
104A
104B
104C
108
110
112
Database

FIG. 1

FIG. 2

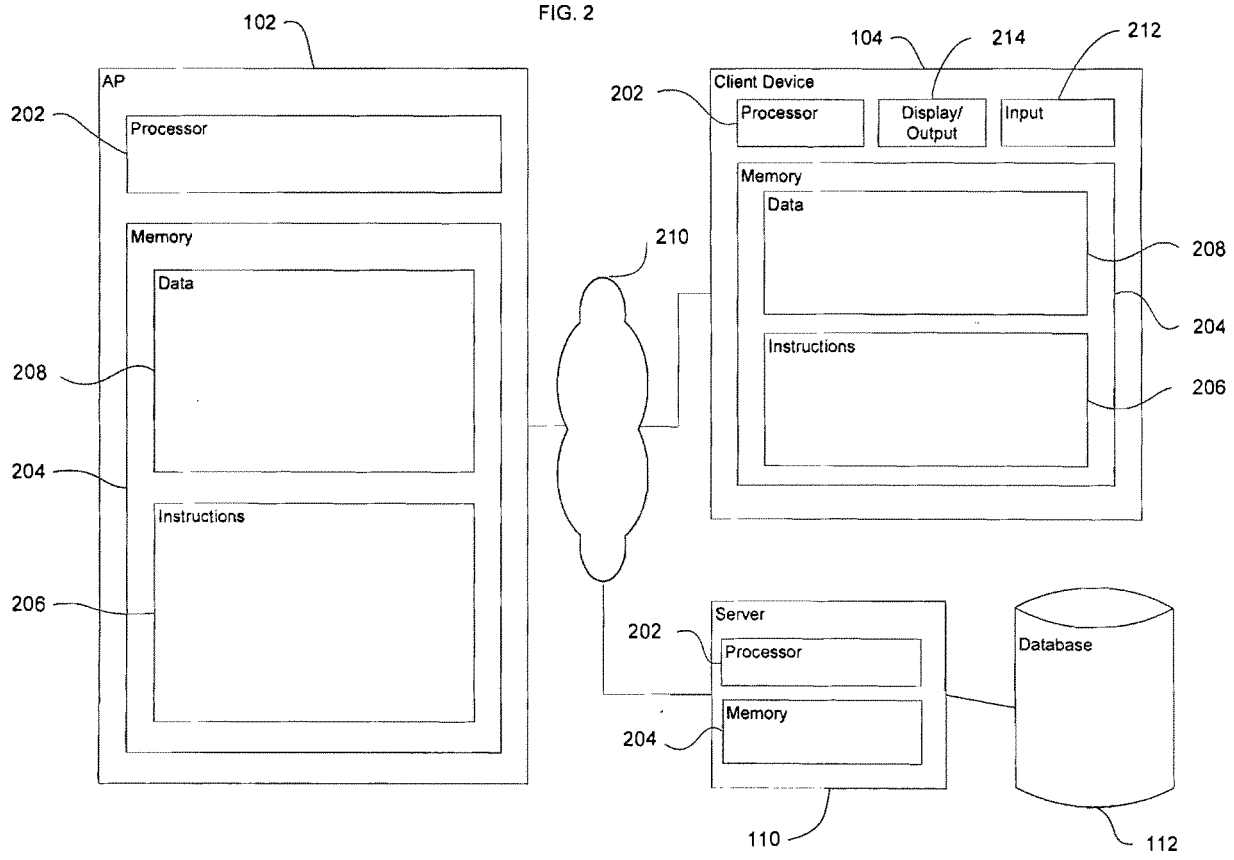

102
AP
202
Processor
Memory
Data
208
204
Instructions
206
210
104
214
212
Client Device
202
Processor
Display/
Output
Input
Memory
Data
208
204
Instructions
206
Server
202
Processor
Memory
204
110
Database
112

FIG. 3

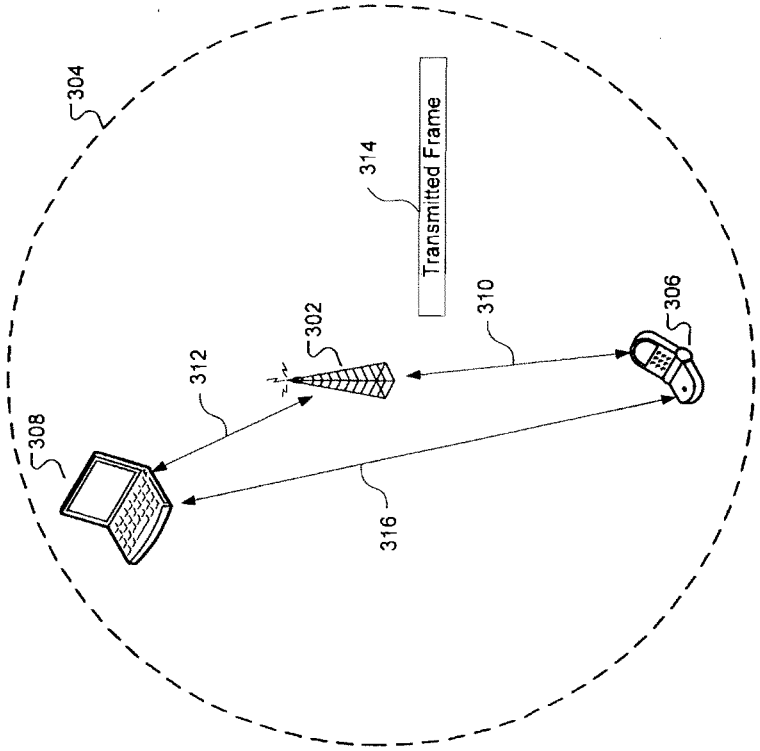


FIG. 4

400

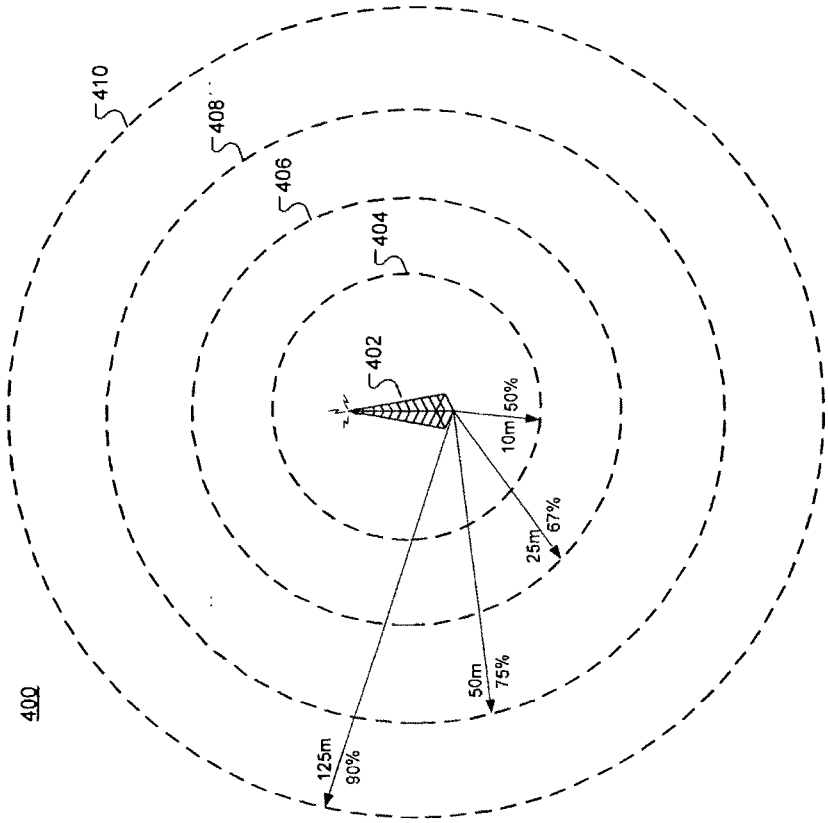


FIG. 5

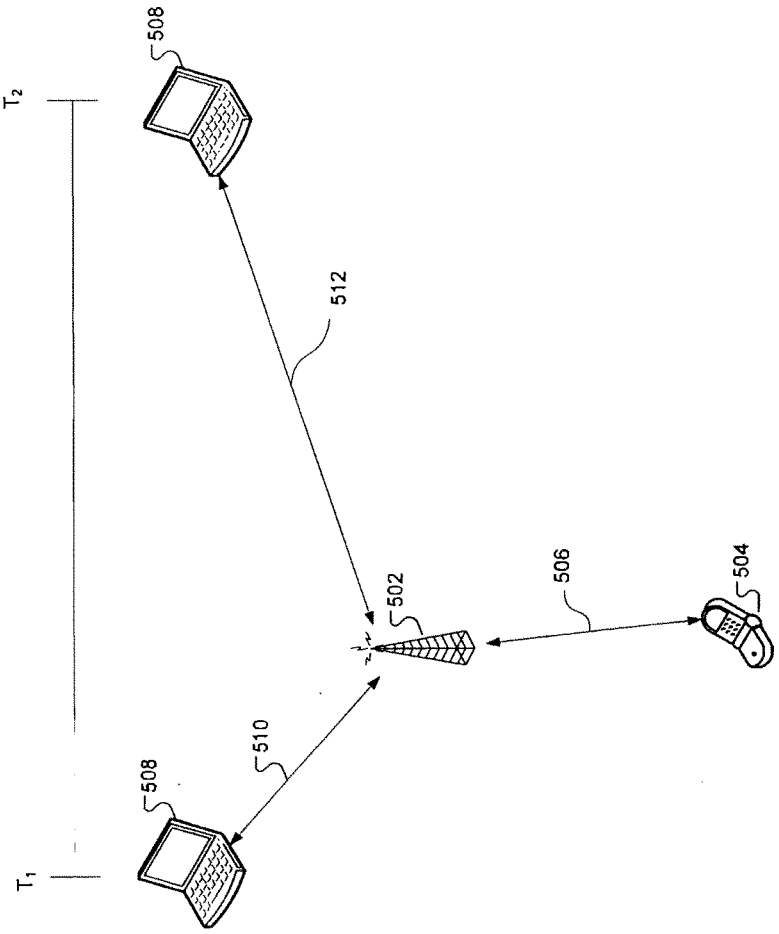


FIG. 6A

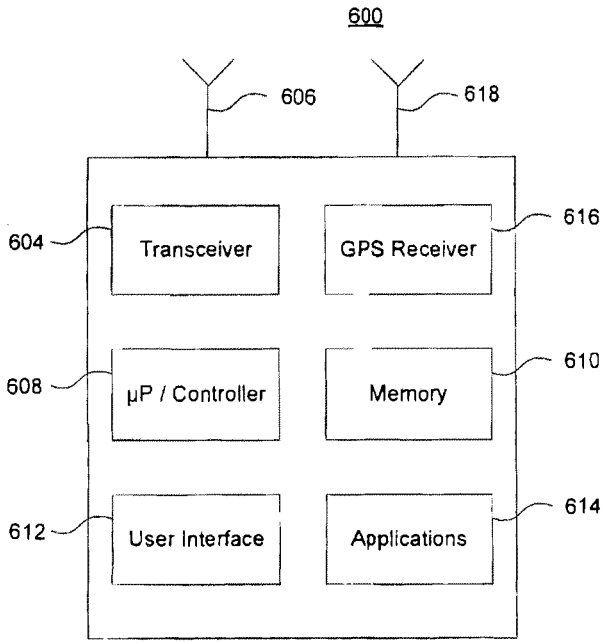
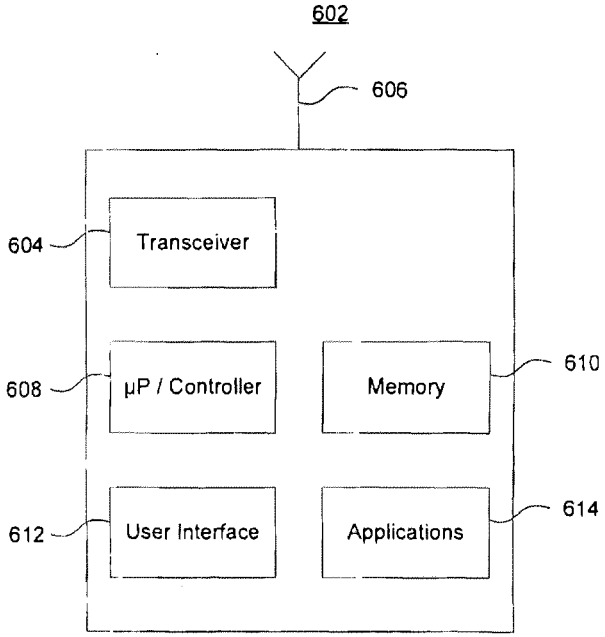

600
606
618
604
Transceiver
GPS Receiver
616
608
µP / Controller
Memory
610
612
User Interface
Applications
614

FIG. 6B


602
606
604
Transceiver
608
µP / Controller
Memory
610
612
User Interface
Applications
614

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 09/05640

A. CLASSIFICATION OF SUBJECT MATTER
IPC(8) - H04W 24/00 (2009.01)
USPC - 455/456.1
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
USPC - 455/456.1

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
USPC - 455/404.2, 440, 456.1 (keyword limited - see terms below)

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
PubWEST(PGPB,USPT,EPAB,JPAB); Google. Search Terms Used: mobile, wireless, cellular, estimate, determine, approximate, find, detect, location, area, distance, access point, base station, wireless router, signal repeater, frame, confidence, value, point, number, trust, parameter, level, request to send, RTS, clear to send, CTS, acknowledgment, ack

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X — Y	US 2005/0124355 A1 (Cromer et al.) 09 June 2005 (09.06.2005), entire document, especially; Fig. 2, 3, 4a, 4b, para. [0003], [0004], [0007], [0014]-[0019]	1, 6-9, 20, 21, 26-29, 33 2-5, 10-19, 22-25, 30-32
Y	US 2008/0113672 A1 (Karr et al.) 15 May 2008 (15.05.2008), [0103], [0104], [0107], [0113], [0114], [1030]	2-5, 10-19, 22-25, 30-32
Y	US 2004/0157624 A1 (Hrastar) 12 August 2004 (12.08.2004), Fig. 8a, 8b, para. [0084], [0085]	12, 13
A	US 6,249,252 B1 (Dupray) 19 June 2001 (19.06.2001), entire document	1 - 33

☐ Further documents are listed in the continuation of Box C. ☐

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 November 2009 (29.11.2009)	11 DEC 2009
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US, Commissioner for Patents P.O. Box 1450, Alexandria, Virginia 22313-1450 Facsimile No. 571-273-3201	Authorized officer: Lee W. Young PCT Helpdesk: 571-272-4300 PCT OSP: 571-272-7774

Form PCT/ISA/210 (second sheet) (July 2009)

Gadget Lab
Hardware News and Reviews
Previous post
Next post

iPhone's Location-Data Collection Can't Be Turned Off

By Brian X. Chen April 25, 2011 | 2:09 pm | Categories: Phones

Apple claims turning Location Services to 'Off' will cease all collection of geodata on iOS devices. Independent tests show otherwise. Photo: Jon Snyder/Wired.com

The iPhone continues to store location data even when location services are disabled, contrary to Apple's previous claims.

The Wall Street Journal did independent testing on an iPhone and found that even after turning off location services, the device was still collecting information on nearby cell towers and Wi-Fi access points.

This discovery challenges some of Apple's claims. As Wired.com reported last week, the company explained in a detailed letter last year that it deliberately collects geodata to store in a comprehensive location database to improve location services. In the letter, Apple noted that customers can disable location-data collection by turning off Location Services in the settings menu.

"If customers toggle the switch to 'Off,' they may not use location-based services, and no location-based information will be collected," Apple said in the letter (.pdf).

That doesn't appear to be the case from *WSJ*'s testing, as well as multiple independent reports from customers who had the same results.

The controversy surrounding Apple's location-tracking stems from a discovery by two data scientists, who found that a file stored on iPhones and iPads ("consolidated.db") contains a detailed history of geodata accompanied with time stamps.

Apple claimed in its letter last year that the geodata is stored on the device, then anonymized and transmitted back to Apple every 12 hours, using a secure Wi-Fi connection (if one is available).

Although it's thorough, Apple's explanation does not address why the stored geodata continues to live on the device permanently after it's transmitted to Apple, nor does it address why geodata collection appears to persist even when Location Services is turned off.

Google does similar geodata collection for its own location-services database. However, it notifies Android users clearly in a prompt when geodata collection will occur, and it also gives users a way to opt out. Also, Android devices do not permanently store geodata after transmitting it to Google.

Meanwhile, a MacRumors.com reader claims he sent an e-mail to CEO Steve Jobs asking him to explain why Apple tracks geodata, threatening to switch to an Android device.

"Maybe you could shed some light on this for me before I switch to a Droid," the reader wrote. "They don't track me."

The CEO shot back a terse reply, defending his company and attacking his competitor Google, according to the reader: "Oh yes they do. We don't track anyone. The info circulating around is false."

Apple has not commented on the authenticity of the e-mail.

The purported e-mail is similar in nature to many e-mails that Jobs has sent to customers in the past: It's concise and still manages to pull off some word play. Jobs would be accurate to claim that Apple is not tracking customers directly — but instead it is using iPhones to gather information about nearby cell towers and Wi-Fi stations, occasionally combined with GPS data. In other words, Apple is tracking geodata from mobile devices, as Google is also doing.

Apple has not commented on the location-tracking issue since the story broke last week.

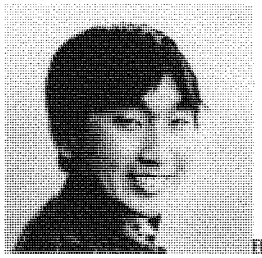
While the collected geodata doesn't reveal specific addresses for locations you've visited, it can still leave a pretty rich trail of a user's movements. Combine this data with other pieces of information on the iPhone, like your messages and photos, and you've got a device that knows more about you than you do yourself, says *The Atlantic*'s Alexis Madrigal.

Madrigal tested an iPhone forensics program called Lantern, which stitches together contacts, text messages and geodata into a neat interface that reconstructed a timeline of his life.

"Immediately after trying out Lantern, I enabled the iPhone's passcode and set it to erase all data on the phone," Madrigal said. "This thing remembers more about where I've been and what I've said than I do, and I'm damn sure I don't want it falling into anyone's hands."

See Also:

- Why You Should Care About the iPhone Location-Tracking Issue
- Why and How Apple Is Collecting Your iPhone Location Data
- iPhone Tracks Your Every Move, and There's a Map for That



Brian is a Wired.com technology reporter focusing on Apple and Microsoft. He recently wrote a book about the always-connected mobile future called *Always On* (publishing June 7, 2011 by Da Capo).
Follow @bxchen and @gadgetlab on Twitter.

Tags: Apple, iPhone, privacy, Security
Post Comment | Permalink

and 1 other liked this.

Login
Add New Comment

Real-time updating is **enabled**. (Pause)

Sort by popular now
Showing 38 comments

THE WALL STREET JOURNAL.
WSJ.com

APRIL 26, 2011, 4:13 PM ET

The Unique ID Android Uses in Collecting Location

In tests last week, a security analyst found that Google Inc.'s Android phones were collecting and transmitting location data, along with a unique phone identifier, back to Google.

So what is that phone identifier, and what does Google do with it?

Basically, it's a string of numbers and letters associated with your phone. The ID is created when the phone is booted up for the first time. A user can change the ID by performing a "factory reset" of the device, which wipes out the data on the phone.

Google says the identifier is associated only with the location data, not with other user information. Indeed, the analyst doing the research, Samy Kamkar, did not see the ID transmitted with other information, such as email or calendar data.

Mr. Kamkar found that the identifier — called a "platform key" — is similar to another ID on the phone, something known as an Android ID.

The numbers are created when the phone is first booted up, and the Android ID can be used by application developers to do things like keep track of scores in games. But having the phone's Android ID doesn't mean that an app developer would also be able to get the platform key.

Google has said it uses location data to, among other things, determine the rate at which traffic is moving to provide traffic information on Google Maps. It uses this data only if users agree to allow location services when they set up the phone.

Mr. Kamkar has a controversial past. In 2005, when he was 19, he created a computer worm that caused MySpace to crash. He pled guilty to a felony charge of computer hacking and agreed to not use a computer for three years. Since 2008, he has been doing independent computer security research and consulting.

The Journal hired an independent consultant, Ashkan Soltani, to review Mr. Kamkar's findings. Mr. Soltani confirmed the conclusions.

Copyright 2008 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

1.15% APY | A HIGH-YIELD SAVINGS ACCOUNT FROM AMERICAN EXPRESS | LEARN MORE NOW | PERSONAL SAVINGS from American Express

Accounts offered by American Express Bank, FSB. Member FDIC

Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

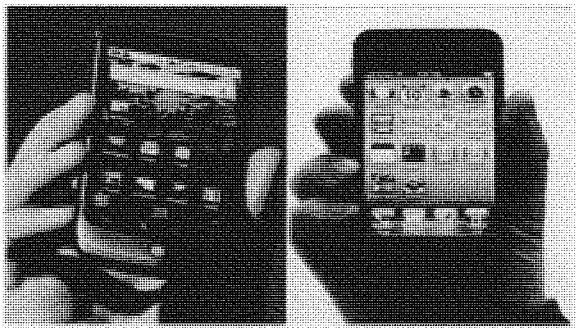
See a sample reprint in PDF format. Order a reprint of this article now

THE WALL STREET JOURNAL.
WSJ.com

TECHNOLOGY | APRIL 22, 2011

Apple, Google Collect User Data

By JULIA ANGWIN And JENNIFER VALENTINO-DEVRIES



WSJ.com Senior Technology Editor Julia Angwin reports Apple's iPhone and Google's Android regularly transmit user location data back to those companies, based on data analyzed by The Wall Street Journal.

Apple Inc.'s iPhones and Google Inc.'s Android smartphones regularly transmit their locations back to Apple and Google, respectively, according to data and documents analyzed by The Wall Street Journal—intensifying concerns over privacy and the widening trade in personal data.

Google and Apple are gathering location information as part of their race to build massive databases capable of pinpointing people's locations via their cellphones. These databases could help them tap the $2.9 billion market for location-based services—expected to rise to $8.3 billion in 2014, according to research firm Gartner Inc.

More

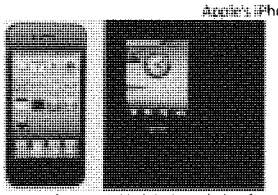
How to Avoid Mobile Trackers

Security Analyst Samy Kamkar's Website

In the case of Google, according to new research by security analyst Samy Kamkar, an HTC Android phone collected its location every few seconds and transmitted the data to Google at least several times an hour. It also transmitted the name, location and signal strength of any nearby Wi-Fi networks, as well as a unique phone identifier.

Google declined to comment on the findings.

Until last year, Google was collecting similar Wi-Fi data with its fleet of StreetView cars that map and photograph streets



There are ways for users to block the transmission of location information by Android devices and iPhones-although doing so limits important smartphone functions such as maps. WSJ's Jennifer Valentino explains.

What They Know

A Wall Street Journal investigation into the world of digital privacy.

Stalkers Exploit Cellphone GPS

Google Agonizes on Privacy

Facebook in Privacy Breach

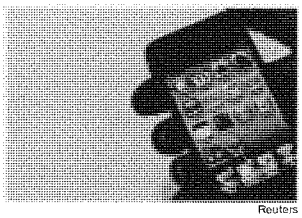
Read More: The Complete Series

Journal Community

How concerned are you that the iPhone tracks and stores your location?

- Very
- Somewhat
- Not at all
- Don't have an iPhone

SUBMIT VOTE **View Results »**



Reuters

Apple's iPhone.

world-wide. The company shut down its StreetView Wi-Fi collection last year after it inadvertently collected e-mail addresses, passwords and other personal information from Wi-Fi networks. The data that Mr. Kamkar observed being transmitted on Android phones didn't include such personal information.

Apple, meanwhile, says it "intermittently" collects location data, including GPS coordinates, of many iPhone users and nearby Wi-Fi networks and transmits that data to itself every 12 hours, according to a letter the company sent to U.S. Reps. Edward Markey (D-Mass.) and Joe Barton (R-Texas) last year. Apple didn't respond to requests for comment.

The Google and Apple developments follow the Journal's findings last year that some of the most popular smartphone apps use location data and other personal information even more aggressively than this—in some cases sharing it with third-party companies without the user's consent or knowledge.

Apple this week separately has come under fire after researchers found that iPhones store unencrypted databases containing location information sometimes stretching back several months.

Google and Apple, the No. 1 and No.3 U.S. smartphone platforms respectively according to comScore Inc., previously have disclosed that they use location data, in part, to build giant databases of Internet WI-Fi hotspots. That data can be used to pinpoint the location of people using Wi-Fi connections.

Cellphones have many reasons to collect location information, which helps provide useful services like local-business lookups and social-networking features. Some location data can also help cellphone networks more efficiently route calls.

Google also has said it uses some of the data to build accurate traffic maps. A cellphone's location data can provide details about, for instance, how fast traffic is moving along a stretch of highway.

The widespread collection of location information is the latest frontier in the booming market for personal data. Until recently, most data about people's behavior has been collected from personal computers: That data generally can be tied to a city or a zip code, but it is tough to be more precise. The rise of Internet-enabled cellphones, however, allows the collection of user data tied with much more precision to specific locations.

This new form of tracking is raising questions from government officials and privacy advocates. On Wednesday, Rep. Markey sent a follow-up letter to Apple asking why the company is storing customer-location data on its phones.

"Apple needs to safeguard the personal location information of its users to ensure that an iPhone doesn't

become an iTrack," Rep. Markey said in a statement.

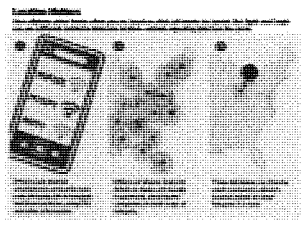
Google previously has said that the Wi-Fi data it collects is anonymous and that it deletes the start and end points of every trip that it uses in its traffic maps. However, the data, provided to the Journal exclusively by Mr. Kamkar, contained a unique identifier tied to an individual's phone.

Mr. Kamkar, 25 years old, has a controversial past. In 2005, when he was 19, he created a computer worm that caused MySpace to crash. He pled guilty to a felony charge of computer hacking in Los Angeles Superior Court, and agreed to not use a computer for three years. Since 2008, he has heen doing independent computer security research and consulting. Last year, he developed the "evercookie"—a type of tracking file that is difficult to be removed from computers—as a way to highlight the privacy vulnerabilities in Web-browsing software.

The Journal hired an independent consultant, Ashkan Soltani, to review Mr. Kamkar's findings regarding the Android device and its use of location data. Mr. Soltani confirmed Mr. Kamkar's conclusions.

Transmission of location data raises questions about who has access to what could he sensitive information about location and movement of a phone user.

Location Matters



Federal prosecutors in New Jersey are investigating whether smartphone applications illegally obtained or transmitted information such as location without proper disclosures, the Journal reported in April, citing people familiar with the matter.

A spokeswoman for the Office of the Privacy Commissioner of Canada said the office "had concerns" about using cellphones to collect Wi-Fi data and has expressed those concerns to Google. "The whole issue of the tracking capabilities of new mobile devices raises significant privacy issues," she said.

The business of collecting location information began in 2003, when Boston-based Skyhook Inc. launched and began the practice of "wardriving"—cruising around in cars to collect information about Wi-Fi hotspots. Comparing the names and signal strengths of nearby Wi-Fi hotspots against a database allows for a cellphone's location to be determined within 100 feet, in many cases, Skyhook says.

"For the first four or five years, people thonght we were nuts," said Ted Morgan, Skyhook's founder and CEO. "We invented this whole concept of driving aronnd and scanning for Wi-Fi and tuning these algorithms."

In 2007, Google began building its own Wi-Fi database, using the StreetView cars. Last year, Apple switched from using Skyhook and began creating its own database of Wi-Fi points for use on its newest phones, although it still uses Skyhook data for older phones and Macintosh computers.

Skyhook's Mr. Morgan says the company attempts to protect users' privacy by collecting data via cellphone only when a person requests location from its servers—for instance when they are actively looking at a map. Each time a user requests location, the information is encrypted and gathered without any identifying user numbers, Mr. Morgan says. That means Skyhook can't follow a person from one location to the next, he says.

EXPERIENCE WSJ PROFESSIONAL

Editors' Deep Dive: Privacy Battles Transform Legal Landscape

COMMUNICATIONS DAILY
Washington Revs Up Internet Legislation

THE LEGAL INTELLIGENCER

Google seems to be taking a different approach, to judge from the data captured by Mr. Kamkar. Its location data appears to be transmitted regardless of whether an app is running, and is tied to the phone's unique identifier.

In its letter to Congress last year, Apple said that it only collects location data from people who use apps that require

Online Behavioral Advertising and 'Do Not Track Me'

DOW JONES NEWS SERVICE

Despite Uproar, Consumers Give Up Privacy

Access thousands of business sources not available on the free web. Learn More

More Tech News

IPhones Power Apple's Growth

Amazon Glitch Hobbles Websites

Facebook Seeking Friends in Beltway

location. It doesn't specify how often a person must use the app for intermittent collection to occur.

Apple also said in the letter that it collects Wi-Fi and GPS information when the phone is searching for a cellular connection. Apple said the data it transmits about location aren't associated with a unique device identifier, except for data related to its mobile advertising network

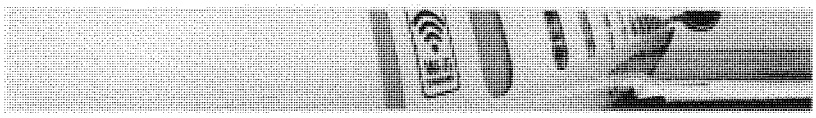
Apple gathers the data to help build a "database with known location information," the letter says. "This information is batched and then encrypted and transmitted to Apple over a Wi-Fi Internet connection every twelve hours (or later if the device does not have Wi-Fi Internet access at that time)," the company wrote in the July letter to Congress.

The letter, which is available on Rep. Markey's website, became newsworthy this week in light of findings from two researchers who uncovered a file on iPhones that keeps a record of where the phone has been and when it was there. The file is unencrypted and stored by default.

The discovery of this location file touched off a furor among iPhone owners who could see for the first time a trove of location data about themselves stored on their phones. The researchers, Alasdair Allan and Pete Warden, said that they had no evidence that the file was being transmitted to Apple.

Write to Julia Angwin at julia.angwin@wsj.com

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com



Dow Jones Reprints: This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers, use the Order Reprints tool at the bottom of any article or visit www.djreprints.com

See a sample reprint in PDF format. Order a reprint of this article now

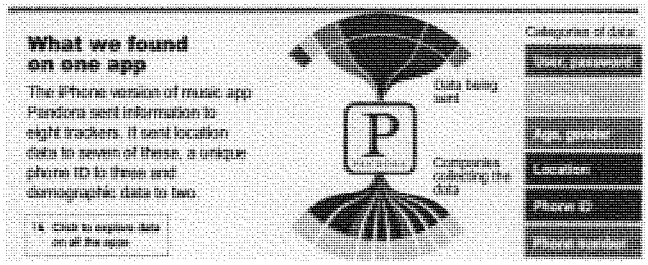
THE WALL STREET JOURNAL.
WSJ.com

WHAT THEY KNOW | DECEMBER 17, 2010

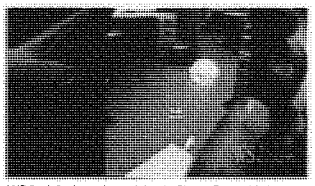
Your Apps Are Watching You

A WSJ Investigation finds that iPhone and Android apps are breaching the privacy of smartphone users

By SCOTT THURM and YUKARI IWATANI KANE



Few devices know more personal details about people than the smartphones in their pockets: phone numbers, current location, often the owner's real name—even a unique ID number that can never be changed or turned off.



WSJ's Julia Angwin explains to Simon Constable how smartphone apps collect and broadcast data about your habits. Many don't have privacy policies and there isn't much you can do about it.

These phones don't keep secrets. They are sharing this personal data widely and regularly, a Wall Street Journal investigation has found.

An examination of 101 popular smartphone "apps"—games and other software applications for iPhone and Android phones—sbowed that 56 transmitted the phone's unique device ID to other companies without users' awareness or consent. Forty-seven apps transmitted the phone's location in some way. Five sent age, gender and other personal details to outsiders.

The findings reveal the intrusive effort by online-tracking companies to gather personal data about people in order to flesh out detailed dossiers on them.

Among the apps tested, the iPhone apps transmitted more data than the apps on phones using Google Inc.'s Android operating system. Because of the test's size, it's not known if the pattern holds among the hundreds of

thousands of apps available.

Apps sharing the most information included TextPlus 4, a popular iPhone app for text messaging. It sent the phone's unique ID number to eight ad companies and the phone's zip code, along with the user's age and gender, to two of them.

Both the Android and iPhone versions of Pandora, a popular music app, sent age, gender, location and phone identifiers to various ad networks. iPhone and Android versions of a game called Paper Toss—players try to throw paper wads into a trash can—each sent the phone's ID number to at least five ad companies. Grindr, an iPhone app for meeting gay men, sent gender, location and phone ID to three ad companies.

More

What Can You Do? Not Much

What Settings to Look For

How One App Sees Location Without Asking

Unique Phone ID Numbers Explained

The Journal's Cellphone Testing Methodology

Complete Coverage: What They Know

"In the world of mobile, there is no anonymity," says Michael Becker of the Mobile Marketing Association, an industry trade group. A cellphone is "always with us. It's always on."

iPhone maker Apple Inc. says it reviews each app before offering it to users. Both Apple and Google say they protect users by requiring apps to obtain permission before revealing certain kinds of information, such as location.

"We have created strong privacy protections for our customers, especially regarding location-based data," says Apple spokesman Tom Neumayr. "Privacy and trust are vitally important."

The Journal found that these rules can be skirted. One iPhone app, Pumpkin Maker (a pumpkin-carving game), transmits location to an ad network without asking permission. Apple declines to comment on whether the app violated its rules.

Smartphone users are all but powerless to limit the tracking. With few exceptions, app users can't "opt out" of phone tracking, as is possible, in limited form, on regular computers. On computers it is also possible to block or delete "cookies," which are tiny tracking files. These techniques generally don't work on cellphone apps.

The makers of TextPlus 4, Pandora and Grindr say the data they pass on to outside firms isn't linked to an individual's name. Personal details such as age and gender are volunteered by users, they say. The maker of Pumpkin Maker says he didn't know Apple required apps to seek user approval before transmitting location. The maker of Paper Toss didn't respond to requests for comment.

Journal Community

Do you think apps should tell you when they collect and send information about the mobile

- Yes, every time
- Yes, but only when I first install the app
- Only if sending data to other companies
- No, this doesn't bother me

View Results »

This poll has closed, please click above for results.

Many apps don't offer even a basic form of consumer protection: written privacy policies. Forty-five of the 101 apps didn't provide privacy policies on their websites or inside the apps at the time of testing. Neither Apple nor Google requires app privacy policies.

To expose the information being shared by smartphone apps, the Journal designed a system to intercept and record the data they transmit, then decoded the data stream. The research covered 50 iPhone apps and 50 on phones using Google's Android operating system. (Methodology available here.)

The Journal also tested its own iPhone app; it didn't send information to outsiders. The Journal doesn't have an Android phone app.

Among all apps tested, the most widely shared detail was the unique ID number assigned to every phone. It is effectively a "supercookie," says Vishal Gurbuxani, co-founder of Mobclix Inc., an exchange for mobile advertisers.

On iPhones, this number is the "UDID," or Unique Device Identifier. Android IDs go by other names. These IDs are set by phone makers, carriers or makers of the operating system, and typically can't be blocked or deleted.

"The great thing about mobile is you can't clear a UDID like you can a cookie," says Meghan O'Holleran of Traffic Marketplace, an Internet ad network that is expanding into mobile apps. "That's how we track everything."

Ms. O'Holleran says Traffic Marketplace, a unit of Epic Media Group, monitors smartphone users whenever it can. "We watch what apps you download, how frequently you use them, how much time you spend on them, how deep into the app you go," she says. She says the data is aggregated and not linked to an individual.

More From the Series

- **A Web Pioneer Profiles Users by Name**
- **Web's New Goldmine: Your Secrets**
- **Personal Details Exposed Via Biggest Sites**
- **Microsoft Quashed Bid to Boost Web Privacy**
- **On Cutting Edge, Anonymity in Name Only**
- **Stalking by Cellphone**
- **Google Agonizes Over Privacy**
- **On the Web, Children Face Intensive Tracking**
- **'Scrapers' Dig Deep for Data on Web**
- **Facebook in Privacy Breach**
- **Insurers Test Data Profiles to Identify Risky Clients**
- **Shunned Profiling Technology on the Verge of Comeback**
- **Race Is On to 'Fingerprint' Phones, PCs**
- **The Tracking Ecosystem**

Follow **@whattheyknow** on Twitter

Complete Coverage: What They Know

The main companies setting ground rules for app data-gathering have hig stakes in the ad business. The two most popular platforms for new U.S. smartphones are Apple's iPhone and Google's Android. Google and Apple also run the two biggest services, by revenue, for putting ads on mobile phones.

Apple and Google ad networks let advertisers target gronps of users. Both companies say they don't track individuals based on the way they use apps.

Apple limits what can be installed on an iPhone by requiring iPhone apps to be offered exclusively through its App Store. Apple reviews those apps for function, offensiveness and other criteria.

Apple says iPbone apps "cannot transmit data about a user without obtaining the user's prior permission and providing the user with access to information about how and where the data will be used." Many apps tested by the Journal appeared to violate that rule, by sending a user's location to ad networks, without informing users. Apple declines to discuss bow it interprets or enforces the policy.

Phones running Google's Android operating system are made by companies including Motorola Inc. and Samsnng Electronics Co. Google doesn't review the apps, which can be downloaded from many vendors. Google says app makers "bear the responsibility for how they handle user information."

Google requires Android apps to notify users, before they download the app, of the data sources the app intends to access. Possible sources include the phone's camera, memory, contact list, and more than 100 others. If users don't like what a particnlar app wants to aceess, they can choose not to install the app, Google says.

"Our focus is making sure that users have control over what apps they install, and notice of what information the app accesses," a Google spokesman says.

Neither Apple nor Google requires apps to ask permission to access some forms of the device ID, or to send it to outsiders. When smartphone users let an app see their location, apps generally don't disclose if they will pass the location to ad companies.

Lack of standard practices means different companies treat the same information differently. For example, Apple says that, internally, it treats the iPhone's UDID as "personally identifiable information." That's because, Apple says, it can be combined with other personal details about people—such as names or email addresses—that Apple has via the App Store or its iTunes music services. By contrast, Google and most app makers don't consider device IDs to be identifying information.

A growing industry is assembling this data into profiles of cellphone users. Mobclix, the ad exchange, matches more than 25 ad networks with some 15,000 apps seeking advertisers. The Palo Alto, Calif., company collects phone IDs, encodes them (to obscure the number), and assigns them to interest categories based on what apps people download and how much time they spend using an app, among other factors.

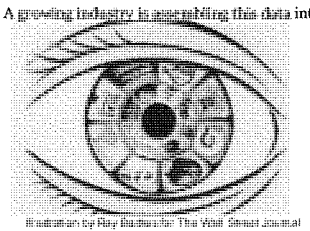


Illustration by Ray Bachmann/The Wall Street Journal

By tracking a phone's location, Mobclix also makes a "best guess" of where a person lives, says Mr. Gurbuxani, the Mobclix executive. Mobclix then matches that location with spending and demographic data from Nielsen Co.

In roughly a quarter-second, Mobclix can place a user in one of 150 "segments" it offers to advertisers, from "green enthusiasts" to "soccer moms." For example, "die hard gamers" are 15-to-25-year-old males with more than 20 apps on their phones who use an app for more than 20 minutes at a time.

Mobclix says its system is powerful, but that its categories are broad enough to not identify individuals. "It's about how you track people better," Mr. Gurbuxani says.

Some app makers have made changes in response to the findings. At least four app makers posted privacy policies after being contacted by the Journal, including Rovio Mobile Ltd., the Finnish company behind the popular game Angry Birds (in which birds battle egg-snatching pigs). A spokesman says Rovio had been working on the policy, and the Journal inquiry made it a good time to unveil it.

Free and paid versions of Angry Birds were tested on an iPhone. The apps sent the phone's UDID and location to the Chillingo unit of Electronic Arts Inc., which markets the games. Chillingo says it doesn't use the information for advertising and doesn't share it with outsiders.

Apps have been around for years, but burst into prominence when Apple opened its App Store in July 2008. Today, the App Store boasts more than 300,000 programs.

Other phone makers, including BlackBerry maker Research in Motion Ltd. and Nokia Corp., quickly built their own app stores. Google's Android Market, which opened later in 2008, has more than 100,000 apps. Market researcher Gartner Inc. estimates that world-wide app sales this year will total $6.7 billion.

Many developers offer apps for free, hoping to profit by selling ads inside the app. Noah Elkin of market researcher eMarketer says some people "are willing to tolerate advertising in apps to get something for free." Of the 101 apps tested, the paid apps generally sent less data to outsiders.

Ad sales on phones account for less than 5% of the $23 billion in annual Internet advertising. But spending on mobile ads is growing faster than the market overall.

Central to this growth: the ad networks whose business is connecting advertisers with apps. Many ad networks offer software "kits" that automatically insert ads into an app. The kits also track where users spend time inside the app.

Some developers feel pressure to release more data about people. Max Binshtok, creator of the DailyHoroscope Android app, says ad-network executives encouraged him to transmit users' locations.

Mr. Binshtok says he declined because of privacy concerns. But ads targeted by location bring in two to five times as much money as untargeted ads, Mr. Binshtok says. "We are losing a lot of revenue."

Other apps transmitted more data. The Android app for social-network site MySpace sent age and gender, along with a device ID, to Millennial Media, a big ad network.

In its software-kit instructions, Millennial Media lists 11 types of information about people that developers may

transmit to "help Millennial provide more relevant ads." They include age, gender, income, ethnicity, sexual orientation and political views. In a re-test with a more complete profile, MySpace also sent a user's income, ethnicity and parental status.

A spokesman says MySpace discloses in its privacy policy that it will share details from user profiles to help advertisers provide "more relevant ads." My Space is a unit of News Corp., which publishes the Journal. Millennial did not respond to requests for comment on its software kit.

App makers transmitting data say it is anonymous to the outside firms that receive it. "There is no real-life I.D. here," says Joel Simkhai, CEO of Nearby Buddy Finder LLC, the maker of the Grindr app for gay men. "Because we are not tying [the information] to a name, I don't see an area of concern."

Scott Lahman, CEO of TextPlus 4 developer Gogii Inc., says his company "is dedicated to the privacy of our users. We do not share personally identifiable information or message content." A Pandora spokeswoman says, "We use listener data in accordance with our privacy policy," which discusses the app's data use, to deliver relevant advertising. When a user registers for the first time, the app asks for email address, gender, birth year and ZIP code.

Google was the biggest data recipient in the tests. Its AdMob, AdSense, Analytics and DoubleClick units collectively heard from 38 of the 101 apps. Google, whose ad units operate on hoth iPhones and Android phones, says it doesn't mix data received by these units.

Google's main mobile-ad network is AdMob, which it bonght this year for $750 million. AdMob lets advertisers target phone users by location, type of device and "demographic data," including gender or age group.

A Google spokesman says AdMob targets ads based on what it knows about the types of people who use an app, phone location, and profile information a user has submitted to the app. "No profile of the user, their device, where they've been or what apps they've downloaded, is created or stored," he says.

Apple operates its iAd network only on the iPhone. Eighteen of the 51 iPhone apps sent information to Apple.

Apple targets ads to phone users based largely on wbat it knows about them through its App Store and iTunes music service. The targeting criteria can include the types of songs, videos and apps a person downloads, according to an Apple ad presentation reviewed by the Journal. The presentation named 103 targeting categories, including: karaoke, Christian/gospel music, anime, business news, health apps, games and horror movies.

People familiar with iAd say Apple doesn't track what users do inside apps and offers advertisers broad categories of people, not specific individuals.

Apple has signaled tbat it has ideas for targeting people more closely. In a patent application filed this past May, Apple outlined a system for placing and pricing ads based on a person's "web history or search history" and "the contents of a media library." For example, home-improvement advertisers might pay more to reach a person who downloaded do-it-yourself TV shows, the document says.

The patent application also lists another possible way to target people with ads: the contents of a friend's media library.

How would Apple learn who a cellphone user's friends are, and what kinds of media they prefer? The patent says Apple could tap "known connections on one or more social-networking websites" or "publicly available information or private databases describing purchasing decisions, brand preferences," and other data. In September, Apple introduced a social-networking service within iTunes, called Ping, that lets users share music preferences with friends. Apple declined to comment.

Tech companies file patents on blue-sky concepts all the time, and it isn't clear whether Apple will follow through on these ideas. If it did, it would be an evolution for Chief Executive Steve Jobs, who has spoken out

against intrusive tracking. At a tech conference in June, he complained about apps "that want to take a lot of your personal data and suck it up."

—Tom McGinty and Jennifer Valentino-DeVries contributed to this report.

Write to Scott Thurm at scott.thurm@wsj.com and Yukari Iwatani Kane at yukari.iwatani@wsj.com

Copyright 2011 Dow Jones & Company, Inc. All Rights Reserved
This copy is for your personal, non-commercial use only. Distribution and use of this material are governed by our Subscriber Agreement and by copyright law. For non-personal use or to order multiple copies, please contact Dow Jones Reprints at 1-800-843-0008 or visit www.djreprints.com

SUBMISSIONS FOR THE RECORD NOT PRINTED DUE TO VOLUMINOUS NATURE, PREVIOUSLY PRINTED BY AN AGENCY OF THE FEDERAL GOVERNMENT, OR OTHER CRITERIA DETERMINED BY THE COMMITTEE, LIST OF MATERIAL AND LINKS CAN BE FOUND BELOW:

http://info.publicintelligence.net/GoogleWiFiSpy.pdf

○