AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES

JOINT HEARING

BEFORE THE

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

AND THE

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

OF THE

COMMITTEE ON ENERGY AND COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED ELEVENTH CONGRESS

SECOND SESSION

FEBRUARY 24, 2010

Serial No. 111–98

Printed for the use of the Committee on Energy and Commerce

energycommerce.house.gov

U.S. GOVERNMENT PRINTING OFFICE

76–010 WASHINGTON : 2012

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 ENERGY AND COMMERCE

HENRY A. WAXMAN, California, *Chairman*

JOHN D. DINGELL, Michigan
Chairman Emeritus
EDWARD J. MARKEY, Massachusetts
RICK BOUCHER, Virginia
FRANK PALLONE, JR., New Jersey
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
GENE GREEN, Texas
DIANA DEGETTE, Colorado
Vice Chairman
LOIS CAPPS, California
MICHAEL F. DOYLE, Pennsylvania
JANE HARMAN, California
TOM ALLEN, Maine
JAN SCHAKOWSKY, Illinois
HILDA L. SOLIS, California
CHARLES A. GONZALEZ, Texas
JAY INSLEE, Washington
TAMMY BALDWIN, Wisconsin
MIKE ROSS, Arkansas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
JOHN BARROW, Georgia
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
JOHN P. SARBANES, Maryland
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
BETTY SUTTON, Ohio
BRUCE L. BRALEY, Iowa
PETER WELCH, Vermont

JOE BARTON, Texas
Ranking Member
RALPH M. HALL, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
ED WHITFIELD, Kentucky
JOHN SHIMKUS, Illinois
JOHN B. SHADEGG, Arizona
ROY BLUNT, Missouri
STEVE BUYER, Indiana
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
JOHN SULLIVAN, Oklahoma
TIM MURPHY, Pennsylvania
MICHAEL C. BURGESS, Texas
MARSHA BLACKBURN, Tennessee
PHIL GINGREY, Georgia
STEVE SCALISE, Louisiana
PARKER GRIFFITH, Alabama
ROBERT E. LATTA, Ohio

SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION

BOBBY L. RUSH, Illinois
Chairman

JANICE D. SCHAKOWSKY, Illinois
Vice Chair
JOHN SARBANES, Maryland
BETTY SUTTON, Ohio
FRANK PALLONE, New Jersey
BART GORDON, Tennessee
BART STUPAK, Michigan
GENE GREEN, Texas
CHARLES A. GONZALEZ, Texas
ANTHONY D. WEINER, New York
JIM MATHESON, Utah
G.K. BUTTERFIELD, North Carolina
JOHN BARROW, Georgia
DORIS O. MATSUI, California
KATHY CASTOR, Florida
ZACHARY T. SPACE, Ohio
BRUCE L. BRALEY, Iowa
DIANA DEGETTE, Colorado
JOHN D. DINGELL, Michigan (ex officio)

CLIFF STEARNS, Florida
Ranking Member
RALPH M. HALL, Texas
ED WHITFIELD, Kentucky
GEORGE RADANOVICH, California
JOSEPH R. PITTS, Pennsylvania
MARY BONO MACK, California
LEE TERRY, Nebraska
MIKE ROGERS, Michigan
SUE WILKINS MYRICK, North Carolina
MICHAEL C. BURGESS, Texas

SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET

RICK BOUCHER, Virginia
Chairman

EDWARD J. MARKEY, Massachusetts
BART GORDON, Tennessee
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
BART STUPAK, Michigan
DIANA DEGETTE, Colorado
MICHAEL F. DOYLE, Pennsylvania
JAY INSLEE, Washington
ANTHONY D. WEINER, New York
G.K. BUTTERFIELD, North Carolina
CHARLIE MELANCON, Louisiana
BARON P. HILL, Indiana
DORIS O. MATSUI, California
DONNA M. CHRISTENSEN, Virgin Islands
KATHY CASTOR, Florida
CHRISTOPHER S. MURPHY, Connecticut
ZACHARY T. SPACE, Ohio
JERRY MCNERNEY, California
PETER WELCH, Vermont
JOHN D. DINGELL, Michigan (ex officio)

FRED UPTON, Michigan
Ranking Member
CLIFF STEARNS, Florida
NATHAN DEAL, Georgia
BARBARA CUBIN, Wyoming
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
VITO FOSELLA, New York
GEORGE RADANOVICH, California
MARY BONO MACK, California
GREG WALDEN, Oregon
LEE TERRY, Nebraska
MIKE FERGUSON, New Jersey

CONTENTS

	Page
Hon. Bobby L. Rush, a Representative in Congress from the State of Illinois, opening statement	1
Hon. Ed Whitfield, a Representative in Congress from the Commonwealth of Kentucky, opening statement	3
Prepared statement	5
Hon. Doris O. Matsui, a Representative in Congress from the State of California, opening statement	7
Hon. Cliff Stearns, a Representative in Congress from the State of Florida, opening statement	7
Hon. Kathy Castor, a Representative in Congress from the State of Florida, opening statement	9
Hon. Edward J. Markey, a Representative in Congress from the Commonwealth of Massachusetts, opening statement	10
Hon. Steve Scalise, a Representative in Congress from the State of Louisiana, opening statement	11
Hon. Anna G. Eshoo, a Representative in Congress from the State of California, opening statement	12
Hon. Lee Terry, a Representative in Congress from the State of Nebraska, opening statement	13
Hon. Rick Boucher, a Representative in Congress from the Commonwealth of Virginia, prepared statement	124
Hon. Joe Barton, a Representative in Congress from the State of Texas, prepared statement	128

WITNESSES

John B. Morris, Jr., General Counsel, Center for Democracy and Technology	14
Prepared statement	17
Lorrie Cranor, Associate Professor, Computer Science and Engineering and Public Policy, Carnegie Mellon University	32
Prepared statement	34
Jerry King, Chief Operating Officer, uLocate Communications, Inc.	69
Prepared statement	71
Tony Bernard, Vice President and General Manager, Useful Networks	76
Prepared statement	78
Michael Altschul, Senior Vice President and General Counsel, CTIA—The Wireless Association	87
Prepared statement	89
Anne Collier, ConnectSafely	96
Prepared statement	98

THE COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES

WEDNESDAY, FEBRUARY 24, 2010

HOUSE OF REPRESENTATIVES, SUBCOMMITTEE ON COMMERCE, TRADE, AND CONSUMER PROTECTION, JOINT WITH THE SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET, COMMITTEE ON ENERGY AND COMMERCE, WASHINGTON, DC.

The subcommittees met, pursuant to call, at 10:05 a.m., in Room 2141 of the Rayburn House Office Building, Hon. Bobby L. Rush [Chairman of the Subcommittee on Commerce, Trade, and Consumer Protection] presiding.

Present from Subcommittee on Commerce, Trade, and Consumer Protection: Representatives Rush, Sarbanes, Barrow, Matsui, Castor, Space, Braley, Stearns, Whitfield, Terry and Scalise.

Present from Subcommittee on Communications, Technology and the Internet: Representatives Boucher, Markey, Eshoo, Doyle, Matsui, Castor, Space, Stearns, Shimkus, Buyer and Terry.

Staff present: Michelle Ash, Chief Counsel; Marc Groman, FTC Detailee; Greg Guice, FCC Detailee; Will Cusey, Special Assistant; Daniel Hekier, Intern; Sarah Fisher, Special Assistant; David Kohn, Press Secretary; Amy Levine, Counsel; Timothy Robinson, Counsel; Ross Schulman, Intern; Will Carty, Minority Professional Staff; Sam Costello, Minority Legislative Analyst; Neil Fried, Minority Senior Counsel; Shannon Weinberg, Minority Counsel; and Brian McCullough, Minority Senior Professional Staff.

OPENING STATEMENT OF HON. BOBBY L. RUSH, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF ILLINOIS

Mr. RUSH. The subcommittee will now come to order. We are conducting a hearing this morning on the matter of the collection and use of location information for commercial purposes, and I want to welcome all the members of the committee who are present, those individuals who are present who are non-members, and I also want to welcome all the witnesses and those who are doing this from the perspective of interested parties who are in evidence. The chairman recognizes himself for 5 minutes for the purposes of an opening statement.

Today we are pleased to welcome six witnesses representing the wireless industry, software firms, a nonprofit advocacy group and an academic. We have got a lot of expertise in the realm of privacy, and this joint hearing, which is the fifth in our series of hearings on the general topic of consumer privacy, will focus on the collection and use of location information about individual consumers.

Local base applications and services are springing up each day like wildfire. Yesterday there was Facebook and in the not too distant future we will be encountering something more akin to a placebook. Location-based services and the applications that ride on these services utilize a number of different tracking technologies which can make it easy to track the whereabouts of an estimated 100 million individuals around the world. By the year 2013, it is estimated that the precise whereabouts of over 800 million individuals will be readily discernible at any given moment in time. Of that amount, nearly 180 million of these users will be North Americans. Virtually all location-based services are currently offered to subscribers for free and are subsidized by advertisers. A majority of these services generate, emit or connect terrestrial and satellite wireless signals. They connect independently or at premapped points on a network. These signals can then hone in on and find a wireless's wireless, handheld or low-wave device such as a cell phone or a GPS unit, and because these devices are typically always on our bodies or within arm's reach, there is very little guesswork for inquiring advertisers and other curious subscribers to know or deduce where an individual is located or where their daily movements are likely to be. In fact, advertisers even know the identity of that individual with the growing trend of behavioral advertising and how it intersects with privacy considerations at our joint hearing which our two committees held in June 2009.

To some extent, location-based services can be viewed as a subcategory of behavioral tracking in that they can quickly and cheaply, I might add, tell advertisers more than contextual advertising ever could about someone's preference, their habits and their patterns. Location-based services are in actuality inherently more invasive and threatening to consumer welfare and perhaps even more challenging to consumer privacy than behavioral advertising. Tracking a user's movements through a virtual world of business-to-consumer Web sites is, I am sure everyone will agree, bad enough. Location-based services on the other hand up the ante by making an individual's real-world location data accessible to intended and unintended recipients.

In closing, let me state clearly for the record, and especially for those interested consumer groups, interested entities and government regulators who have been monitoring our series of hearings that with the information we will obtain from today's hearing, we have now learned enough to take the next major step. As one of two co-chairs of these joint undertakings along with my friend, Congressman Boucher, on privacy, it is my intent that our next hearing on privacy will be a legislative hearing where we will discuss "the devil in the details" by commenting on a discussion draft of a comprehensive privacy bill. There is such a thing as TMI, and we need to stop gathering information now and get legislation on a privacy bill.

In the coming days, I and my staff will be working closely with Mr. Boucher, Mr. Whitfield in Mr. Radanovich's absence, Mr. Stearns and the minority staff to produce a draft of a bill, and I would like to thank each of our witnesses for your participation today and I look forward to hearing your testimony and to vigorously engage in our discussion today. I might again emphasize, I

really appreciate you taking the time out from your busy schedule to be with us here today to add your voices and your values and your expertise to this process.

We will now recognize now Mr. Whitfield for 5 minutes for the purposes of opening statement.

OPENING STATEMENT OF HON. ED WHITFIELD, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF KENTUCKY

Mr. WHITFIELD. Mr. Chairman, thank you very much for having this hearing on the collection and use of location information for commercial purposes. We certainly appreciate the panel for being here and giving us this expertise on this important subject.

Through the use of technologies including GPS, triangulation of cell phone positioning information or user-entered data, consumers now have access to what I call convenient information. Whether it is finding the nearest local restaurant in an unfamiliar city, navigating cars to intended designations or the knowledge that a first responder can find us by our GPS location if we are ever in trouble, many consumers find they can no longer live without these apps, as they are called. This new technology raises legitimate concerns about privacy. Obviously most people know that the application they download specifically for its location features will communicate that information for application functionality. What isn't as clear is how the data will be used, whether notice to the consumer is clear and whether user controls over the personal data are adequate. In addition to first-person privacy concerns, there are also privacy concerns for second persons, the people who may not use a service directly but who may be touched by a service by virtue of someone else's use, just as counterparties to phone calls or e-mails may find their identity revealed without their consent. For example, if someone forwards an e-mail to another person, so too can one's privacy location information be revealed if the user of the location-based social networking application shares that information.

Similarly, special situations arise in the employer-employee relationship. We can agree that there are benefits to a delivery service improving its delivery efficiency by using location tracking and positioning. The question is, what rights do the employees have and what policy does the employer communicate about its use of this technology. In one example last August, a New York City employee was terminated after the GPS on his city-provided phone revealed that he had been at home before his shift ended on 83 occasions according to an article in the New York Post. While this may have been justified, the fear of a Big Brother surveillance environment has clearly arrived and merits a serious discussion.

Another issue I might add that merits discussion concerns uniformity, in my view. Wireless carriers are generally prohibited from using location-based information for commercial purposes. However, application providers are not subject to this requirement. So I think that is an issue we also need to be focused on.

There are many questions raised by these technologies and how consumers interact with them. Most of these beneficial services were developed in the absence of legal mandates, and our top pri-

ority must be maintaining the appropriate balance between an environment that does not impede innovation but that does ensure consumers are fully aware of the information they trade for the use of these services. Thank you, Mr. Chairman.

[The prepared statement of Mr. Whitfield follows:]

Statement of the Honorable Ed Whitfield
Joint Subcommittee Hearing on Location Based Services
February 24, 2010

Thank you, Mr. Chairman, for calling today's hearing. It is a logical step in our path towards forming a basis for addressing today's pressing privacy issues and I commend you for holding this timely hearing.

For nearly a decade, location based services have held out the tantalizing promise of benefits to consumers ranging from instant coupons delivered to their cell phones to emergency services that help save their lives. A decade later, thanks in part to more cost efficient developments, consumers are finally realizing many of the promises of being "connected" whenever and wherever they want through the use of smart phones and wireless personal digital assistants.

Through the use of technologies including GPS, triangulation of cell phone positioning information, or user-entered data, consumers now have access to real time mapping services and social networks based on their immediate location. Unfortunately, like many technologies, the potential ramifications of using these services may be preceding the knowledge of its users. It therefore deserves our attention, particularly with regards to privacy issues.

The benefits of these technologies cannot be denied: information at our fingertips makes our lives easier and often safer, whether it is finding the nearest local restaurant in an unfamiliar city, navigating your car to its intended destination, or the knowledge that a first responder can find us by our GPS location if we are ever in trouble. Many consumers find they can no longer live without these "apps."

But just as there are concerns about the government possessing or gaining access to personal data about us in other contexts, similar, legitimate concerns also exist about private companies possessing or gaining access to our location data. Depending on how location data is used, there is certainly an argument such data could be considered "sensitive" information. The same concerns that have been expressed regarding the use of Internet behavior information to direct targeted adverting apply in this context: how will the information be used by the company gathering it, what does the consumer know about that information use, and did the consumer consent to the use or sharing of that information?

Obviously most people know the application they download specifically for its location features will need to communicate that information for application functionality. What isn't as clear is how the data will be used, whether notice to the consumer is clear, and whether user-controls over the personal data are adequate.

In addition to first person privacy concerns, there are also privacy concerns for second-persons – the people that may not use a service directly but who may be touched by a service by virtue of someone else's use. Just as counterparties to phone calls or emails

may find their identity revealed without their consent (for example, if someone forwards an email to another person), so too can one's private location information be revealed if the user of a location-based social networking application shares that information. For example, if I visit Chairman Rush's home, I can post my location and attach his name. In doing so, I will share information the Chairman might rather keep private and he has no control over that use of his information.

Similarly, special situation arise in the employer-employee relationship. We can agree there are benefits to a delivery service improving its delivery efficiency by using location tracking and positioning. The question is what rights do the employees have and what policy does the employer communicate about its use of the technology? In one example, last August, a New York City employee was terminated after the GPS on his city-provided phone revealed that he'd been at home before his shift ended on 83 occasions, according to the *New York Post*. While this may have been justified, the fear of a big brother surveillance environment has clearly arrived and merits serious discussion.

There are many questions raised by these technologies and how consumers interact with them. We need to delve further into theses issues to fully understand the implications and whether the market can address the issues on its own. Most of these beneficial services were developed in the absence of legal mandates, and our top priority must be maintaining the fine balance between an environment that does not impede innovation but that ensures consumers are fully aware of the information they trade for the use of these services.

Thank you Mr. Chairman, and I yield back.

Mr. RUSH. The Chair recognizes the gentlelady from California, Ms. Matsui, for 2 minutes.

OPENING STATEMENT OF HON. DORIS O. MATSUI, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. MATSUI. Thank you, Mr. Chairman. I want to thank you and Chairman Boucher for calling today's joint hearing. I would also like to thank our panelists for being with us this morning as we examine the collection of use of location-based commercial information.

Today, millions of Americans rely on different location-based services and applications for a variety of activities including social networking and navigation and mapping services, among many others. As both broadband expansion and the use of mobile devices continue to grow among consumers, the industry that provides location-based services and applications will only increase. In fact, according to one estimate, the use of these services and applications are expected to reach more than 80 million new users in North America alone over the next 3 years. As we all know, in today's economy information is everything to everyone, and as we know, mobile devices are everything to millions of consumers storing in many cases very personal information or even providing their physical location.

With ever-increasing technologies and applications emerging, it is essential that we properly protect the private and personal information of consumers. Simply put, privacy policies and disclosures should be clear and transparent. We should also understand the scope of information that is being collected, what it is used for, the length of time it is retained and its security. The more information that consumers have, the better. Ultimately, meaningful privacy safeguards should be in place while ensuring that we don't stifle innovation.

I thank both the chairmen for holding this important hearing today and I yield back the balance of my time.

Mr. RUSH. The Chair now recognizes the gentleman from Florida, Mr. Stearns, for 2 minutes.

OPENING STATEMENT OF HON. CLIFF STEARNS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Mr. STEARNS. Good morning, and let me welcome the witnesses and thank you, Mr. Rush and Mr. Boucher, the chair on the Telecom Committee, for having this hearing.

As technology continues to advance, obviously new issues surrounding consumer privacy will continue to confront us. My main concern continues to be protecting the privacy of American consumers without of course stifling innovation that is so critical to growing our economy, particularly now, and keeping America globally competitive.

Today's hearing focuses on the use of location-based services and applications which collect and use location data that allows a consumer to communicate, socialize, travel, play, dine and shop at great convenience than ever before. Location-based service technology is relatively new and as such it is important to examine the

privacy concerns that go along with this new technology. Location-based services present both an opportunity and a potential for all consumers. On the one hand, consumers could receive relevant information about commercial, educational and social opportunities just simply based upon their location, but on the other hand, consumer privacy could be undermined if multiple entities have access to a consumer's location and online activities.

So in order to maximize the consumer benefit of location-based services, the privacy policies of such services need to be transparent and provide a consumer with informed choice regarding whether to permit access to his or her location-based information. That is critical. In addition, we need to ensure that consumers are not lulled into a false sense of security regarding the privacy of their location-based information. Now, under section 222(f) of the Communications Act, wireless carriers are generally prohibited from using location-based information for commercial purposes without the express prior consent of the consumer. However, application providers are subject to no such requirement even though their applications are being downloaded on the devices of wireless carriers. This may falsely lead to consumers to the conclusion that application providers are subject to the same prohibitions as wireless carriers and that no action by consumers is necessary to ensure that their privacy is protected.

I hope our witnesses can address this very important issue but it seems to represent a gap in my mind in consumer privacy protection. So clear and transparent policies should be standard in regard to location-based services and applications. Real transparency should include a robust disclosure and notice to the consumer outside the privacy policy. These notices and disclosures must be presented in a clear and conspicuous manner so that the consumer knows first that information is being collected, second, how the information is being used, and third, what it is being used for, and possibly fourth, how to prevent the collection of this information.

Small businesses and consumers may greatly benefit from the delivery of location-based technology. I mean, for example, imagine that you are in a city and you have a desire to have Chinese food. Location-based application could give you some help right away and point you in the right direction to get it. It is a win-win situation. You get your Chinese food and the restaurant owner gets a customer that they may not otherwise have received. Conversely, if Congress makes it difficult for small businesses to reach or target potential consumers, small businesses could find it increasingly difficult to survive in the complex and constantly changing marketplace. If comprehensive privacy laws are to be developed by Congress, they must be competitively and technologically neutral and they must also be forward looking and adaptable. A proper regulatory framework will take into account the nature of rapidly changing technology. This is particularly true when it comes to a location-based technology that we are talking about today. Congress should not legislate in a way that is restrictive of technology development or that unfairly targets one industry over another.

Although there are certain numerous privacy concerns that must be taken into account, we must also keep in mind the tremendous benefit from these technologies ultimately to all the consumers.

The reality is that location-based service technology is the wave of the future. As such, this committee has a duty, a responsibility to ensure that consumers are protected and free to benefit from these new technologies.

Mr. Chairman, you and I have worked well in the past, Mr. Rush and I and Mr. Boucher, on a number of issues including privacy. Mr. Rush, you mentioned the idea of a privacy bill. I had met with Mr. Boucher, we talked, and I think Mr. Boucher has a draft bill. I understand that there is a possibility that we could get this draft bill. We have not seen it on this side. We urge you to give it to us. I think as a result of this hearing, we may have to look at ways to better inform consumers, as I mentioned earlier, on the location-based applications and services with more transparency. As I previously stated, there seems to be a gap in consumer privacy protection between the regulation of wireless carriers and the application providers. I think this needs to be fixed.

Thank you, Mr. Chairman.

Mr. RUSH. The Chair now recognizes the gentleman from Georgia, Mr. Barrow, for 2 minutes.

Mr. BARROW. I thank the Chair. I will waive an opening statement.

Mr. RUSH. The Chair now recognizes the gentlelady from Florida, Ms. Castor, for 2 minutes.

OPENING STATEMENT OF HON. KATHY CASTOR, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF FLORIDA

Ms. CASTOR. Thank you, Chairman Rush and Chairman Boucher, for calling this hearing.

Today's hearing provides a unique opportunity to learn more about a technology that has a potential to impact our lives in profound ways. I am looking forward to the testimony of our witnesses very much.

The mobile devices that we carry with us now, whether it is a basic cell phone or a smartphone like an iPhone or BlackBerry, are now practically indispensable to Americans. They are our lifelines in many respects. We rely on them to organize our day, keep in touch with our children and run our businesses, and the location-based technologies are generating new ways of interacting, and I am very fond of the function when I am traveling out of town to be able—you know, it used to be that you would reach into the glove box, take out the map and try to figure out—have interesting discussions with your spouse about where you should have turned. Now you can hit the map function and it will show you, and I can find my way to the soccer tournament or the business meeting where I am going.

So these location-based services are already very handy and they have the potential to help us with emergency services especially. They are enabling large companies and small to track their inventory, manage their workforce and do business more efficiently. A hundred million people already use these, but this is going to grow exponentially.

Such rapid proliferation of a technology as promising as LBS is awe-inspiring and bewildering. On one hand, the economic and social benefits that could be generated are potentially endless, but on

the other hand, we need to protect consumer privacy, and the need to protect consumer privacy is greater than ever but the law has not kept pace with this increased need. We are at a crossroads with telecommunications legislation. The Communications Act of 1934 requires phone companies to ask for permission before sharing consumer data including location information and companies are sharing best practices about how to protect sensitive information. Even so, we know that a large percentage of companies don't yet have privacy policies to prevent the sharing of sensitive location data with marketers and other interested parties. There are no comprehensive rules to guide these companies or courts when dealing with location information privacy concerns. So any proposed legislation needs to strike that balance, the right balance to further spur and encourage innovation without encroaching upon the privacy rights of consumers.

So thank you all, and I look forward to your testimony.

Mr. RUSH. The Chair now recognizes the gentleman from Illinois, Mr. Shimkus, for 2 minutes.

Mr. SHIMKUS. Thank you, Mr. Chairman. You are hearing a lot of the same from a lot of members. Location-based services would be great, especially when you are in areas that you don't know where things are. You can imagine traveling and being able to get to a place where you want to go, and I think a lot of people put the GPS in their baggage when they get a rental car, although a lot of rental cars have some of the applications now.

As legislators, I just want to continue to allow the development of this technology, at the same time ensuring consumer information is protected, and I know that is in the best interest of the industry. I know it is in the best interests of our citizens. So I look forward to hearing the testimony and looking forward to make sure that that happens. Yield back.

Mr. RUSH. The Chair now recognizes the gentleman from Massachusetts, Mr. Markey, for 2 minutes.

Mr. MARKEY. Thank you, Mr. Chairman, very much.

OPENING STATEMENT OF HON. EDWARD J. MARKEY, A REPRESENTATIVE IN CONGRESS FROM THE COMMONWEALTH OF MASSACHUSETTS

Mr. Chairman, back in 1999, I authored the privacy provisions that are now contained in section 222 of the Communications Act to safeguard the privacy of telecommunications customers and place new duties on telecommunications carriers to protect the confidentiality of proprietary information relating to other carriers, equipment makers and customers, and my law also included an opt-in, enabling customers to request the disclosure of their own personal telecommunications information to any person they may choose to designate but it would be their choice to opt in and so in that way I was trying to make sure that what you had in your hand was a telecommunications device and not a tracker, not something that could be used unless there was a warrant obtained by the police, you had given your permission for anyone to know what was going on with your device. And now what we have to do because of what has happened over the last 10 years is, we have to continue to update the laws just to make sure we fill in the gaps,

that we give people protection. You know, if you are leaving someplace and you are really planning on going to the New England Patriots-Jacksonville Jaguars game, no one should be able to track and see where you really went. If you went to the Patriots-Jaguars game, you know, it is none of their business. They shouldn't be able to do it unless you gave them permission or there is a warrant out, you have been able to get legally obtained permission to get access to that information. That is my feeling. And if it inhibits the business plan of a few software or telecommunications companies, well, that is just tough luck. They have no right to know that. And so that is my view on it, always has been, and I just think that this makes it possible for people to know just where you are, what seat you are sitting in at the Patriots-Jaguars game, you know, right down the row, oh, there is he right there. "I thought you said that you were going to be out shopping this afternoon."

So this is a very important set of rules we have to put in place, and in fact, it will create all new industries that are down here. Mr. King and others are down here. There are whole companies that can crop up to give you the protection that you need as long as we mandate it, and innovation is out there where you get to use the device, have the information that you need, but it is not voluntary. We can't make it voluntary because only some people will be protected because it will be dependent upon the good will of an individual company, individual application company as to whether or not you are voluntarily protected by them, and that is just not going to be good enough.

Thank you, Mr. Chairman.

Mr. RUSH. Thank you. The gentleman from Louisiana, Mr. Scalise, is recognized for 2 minutes.

OPENING STATEMENT OF HON. STEVE SCALISE, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF LOUISIANA

Mr. SCALISE. Thank you, Mr. Chairman. I am pleased that both subcommittees are once examining the balance between new technologies and privacy.

We can all agree that our privacy is important and we should continue to balance them as technology advances and develops in ways that provide tremendous benefits to consumers and in ways that were previously never imagined. A great example of this is the emergence of location-based technologies. Whereas 10 years ago many people did not even have cell phones, we can now use our mobile devices to find the closest restaurant or pull up directions to a destination, and in many cases, a message or coupon might be sent to us from the restaurant close by or for the destination we are trying to reach. These technologies and the applications that employ them are tremendous advancements and provide consumers with great benefits, not only convenience but also during instances when a person's location is needed for law enforcement personnel or during an emergency situation.

The technological advancements we are seeing today are impressive but as is most often the case, we are still learning about their capabilities and their implications. Even with these advancements, location-based technologies can also expose consumers to certain

risks such as having your location routinely tracked, which could lead to identity theft or stalking. As a father of two young children, I am also concerned about the effects these technologies could have on child safety. Therefore, we must continue to examine ways to ensure consumers don't have their personal information or safety compromised.

I look forward to hearing from our panelists today on what steps they are taking and what steps they think are needed to ensure that consumer protection and personal safety are not compromised. I also hope our panelists discuss what information is being collected on consumers and what is being done with that data and whether consumers even know their information is being collected. As I have stated before, the technology industry is one of the most advanced and competitive industries in our country. It is also one of the most beneficial both for consumers and for the economy. It is worth pointing out that the industry has evolved and grown on its own with little regulation from the federal government, some would say. Therefore, I hope we proceed carefully when stepping in or when drafting legislation in this area.

I hope today's hearing focuses on how we can protect consumers and their safety and what steps the industry will take or has already taken to do so. If self-regulation is not sufficient and privacy regulations move forward, they should be consistent across the industry and not be greater for one technology compared to another. Everyone involved should have to play by the same set of rules, and Congress should not pick winners or losers.

Again, I look forward to hearing the comments of our panelists today, particularly on self-regulation and whether parity is needed in the industry. It is important that we understand their positions and activities as well as all the implications of these popular technologies.

Thank you, and I yield back.

Mr. RUSH. The Chair now recognizes the gentlelady from California, Ms. Eshoo, for 2 minutes.

OPENING STATEMENT OF HON. ANNA G. ESHOO, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Ms. ESHOO. Thank you, Mr. Chairman, and to Chairman Boucher as well for convening this joint subcommittee hearing on the growing use of location-based technology and its implications on personal privacy. I support the continued effort to balance the needs of both promoting innovation and protecting the personal information of customers.

I have long advocated the use of location-based technology as a public safety tool. In fact, I am the author of the E911 legislation, so I can tell you that this technology is critical to first responders and to law enforcement. When they locate our citizens in distress by using geographical information, they literally can save thousands of lives, and they have.

So the use of this technology, however, has expanded beyond public safety and it is now widely used by consumers to complete everyday tasks to make their lives easier and more efficient including finding driving directions, restaurants or the nearest gas sta-

tion. So it is highly useful, very practical and we all use it. But it is also our job to look after the bests interests of the American people, so we have to ensure that the location of users is protected against any misuse from both corporate and government interests.

I look forward to hearing from the witnesses and I would like to especially welcome Anne Collier, who is with ConnectSafely, which is co-headquartered in Palo Alto, California, which is the heart of my district. So thank you to both of our chairmen and I look forward to hearing from the witnesses. Thank you.

Mr. RUSH. The Chair now recognizes the gentleman from Nebraska, Mr. Terry, for 2 minutes.

OPENING STATEMENT OF HON. LEE TERRY, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF NEBRASKA

Mr. TERRY. Thank you, Mr. Chairman, for holding this important hearing.

I agree with the necessity for balance. We should be examining these serious privacy concerns raised from the collection of location information going on today, but I believe that we must consider the great benefits these location-based services can provide our first responders in case of an emergency.

A colleague of ours, a good friend of mine, Todd Tiahrt from Kansas, has recently brought to my attention an issue that not only coincides with our topic of discussion today but an issue I believe must be addressed in any such discussion involving location information. On June 2, 2007, 18-year-old Kelsey Smith was abducted from a Target parking lot in Overland Park, Kansas. Law enforcement was quickly notified and they subsequently called her wireless provider to obtain Kelsey's ping data, or call information. They were denied. On June 6, 2007, 4 days after she had disappeared, Kelsey's body was found. She had been raped and murdered. Authorities had used the ping information to determine where her cell phone had traveled after 4 days of begging and pleading, so the time that they were able to ping, within 45 minutes after that found her dead. Law enforcement found her body.

Now, current law states that a telecommunications carrier may give call location information out to emergency service providers. However, telecom carriers are not required to give this information out to authorities and oftentimes telecom carriers are hesitant to provide the information due to potential liability. I believe it is time that we require telecom service providers to provide location or ping information when asked by law enforcement during cases of emergencies. I encourage my colleagues to look at Mr. Tiahrt's bill, join Mr. Rogers and me, and I think we are going to have discussion about this specific case and its implications.

Thank you for this opportunity. Yield back.

Mr. RUSH. The gentleman from Indiana, Mr. Buyer, is recognized for 2 minutes.

Mr. BUYER. I reserve my time for questioning. Thank you.

Mr. RUSH. The Chair thanks the gentleman. It is now my pleasure and honor to introduce our witnesses. We have six witnesses before us today, and I will introduce them beginning on my left. Mr. John B. Morris, Jr. is the general counsel for the Center for Democracy and Technology. Seated next to him is Ms. Lorrie

Cranor. She is an associate professor of computer science and engineering and public policy at the Carnegie Mellon University. Mr. Jerry King is the chief operating officer for a company called uLocate Communications Incorporated. Seated next to Mr. King is Mr. Tony Bernard. He is the vice president and the general manager of a corporation called Useful Networks. And next to Mr. Bernard is the senior vice president and general counsel for the CTIA–The Wireless Association. And last but not least, Ms. Anne Collier, who is with the organization ConnectSafely. Again, I want to welcome each and every one of you for appearing before us today, and I must note to you that it is the practice of this subcommittee to swear in witnesses. So I would like if you would please stand and raise your right hand.

[Witnesses sworn.]

Mr. RUSH. Let the record indicate and reflect that all the witnesses have answered in the affirmative.

Now I will recognize each one of the witnesses for 5 minutes. I want to note that our timer is technically incapacitated this morning so we are going to have to do it the old-fashioned way. We are going to have to guess. So each one of you are recognized for 5 minutes or thereabouts. So beginning with you, Mr. Morris, please, your opening statement.

TESTIMONY OF JOHN B. MORRIS, JR., GENERAL COUNSEL, CENTER FOR DEMOCRACY AND TECHNOLOGY; LORRIE CRANOR, ASSOCIATE PROFESSOR, COMPUTER SCIENCE AND ENGINEERING AND PUBLIC POLICY, CARNEGIE MELLON UNIVERSITY; JERRY KING, CHIEF OPERATING OFFICER, ULOCATE COMMUNICATIONS, INC.; TONY BERNARD, VICE PRESIDENT AND GENERAL MANAGER, USEFUL NETWORKS; MICHAEL ALTSCHUL, SENIOR VICE PRESIDENT AND GENERAL COUNSEL, CTIA—THE WIRELESS ASSOCIATION; AND ANNE COLLIER, CONNECTSAFELY

TESTIMONY OF JOHN B. MORRIS, JR.

Mr. MORRIS. Thank you very much, and thankfully, I was able to download an app yesterday onto my smartphone that is a 5-minute countdown timer, so I at least will be able to be on time.

Chairman Rush and members of the subcommittee, thank you very much for inviting us to testify on behalf of the Center for Democracy and Technology. We applaud the leadership of the subcommittee for examining the rapidly evolving area of commercial location-based services. We look forward to discussing the promises and the privacy risks of these services.

Over the past 18 months, location services have truly arrived in the online environment as more and more devices can obtain increasingly accurate information. Location has come to permeate the online experience and we are seeing an amazing array of new and innovative location-based products and services. But the easy availability of location information also raises a host of privacy concerns. Location can reveal very privacy information and can even put users at physical risk. Mobile location can reveal, often without user interaction, where a person is and what they are doing. It can reveal visits to potentially sensitive destinations like medical clin-

ics, courts, political rallies or, as I learned today, even New England Patriot games. And sadly, we have already seen location services abused in domestic violence cases.

Unfortunately, the legal standards for the protection of location information are woefully inadequate. Location technology simply has outpaced the existing statutory protections that Congressman Markey talked about, and they are inadequate both in the commercial context as well as with regard to standards for law enforcement access to location information. Congress must act to strengthen statutory protection of location, not only for the sake of protecting privacy but also to protect and to promote innovation in online services. Clear privacy rules are a prerequisite to the growth and success of this valuable part of our industry.

My written testimony describes several technical methods to determine location of a mobile device, but let me just highlight one critical fact. In the old days, say, 3 or 4 years ago, most location determinations involved a cellular carrier that provides the phone service to the device being located. But in the past few years that has all changed. While carriers are continuing to offer innovative location services, many other service providers also offer location service and they can do so wholly without the cooperation or even the knowledge of the cellular carrier. For example, Skyhook Wireless offers a service that can locate this device in this room based solely on the WiFi access points that are visible in this room, and through wireless Internet access, my device can send my location to any Web site or service on the Internet. Thus, anyone from mom-and-pop Web sites to Starbucks can offer location-based services wholly without the involvement of a cellular carrier. All a Web site really needs to do is to add a small portion of JavaScript code onto the Web site and they can enable location services on their Web site, which brings me back to the legal standards to protect the privacy of location information.

As Congressman Markey noted, commendably, Congress enacted the CPNI rules to protect customer proprietary network information and included location information. But as has been noted a number of times in your opening statements, those CPNI rules only apply to telecommunications carriers offering voice services, and today many of the new and innovative location services operate completely outside of the reach of the CPNI rules. And unfortunately, without a statutory mandate to protect location information, some location service providers have been slow to do so. Some in the industry are very closely attentive to privacy but others are not.

CDT believes that Congress can help protect location privacy in at least two ways. First, as Congress contemplates enacting baseline consumer privacy legislation, as has been discussed, we believe that location data should definitely be included as part of the broader framework governing sensitive user data. And second, and of relevance even to the Commerce Committee as well as the Judiciary Committee, whose room we are borrowing today, we believe it is vital for Congress to improve the standards for location access by government and law enforcement agencies. By clarifying the standard, there is an ongoing battle right now in courts about what the appropriate standard is for law enforcement access, and by

clarifying the standard, we can address some of the concerns that carriers have about access.

So all of these points were made in more detail in my written testimony and I hope to be able to answer any questions you might have about these issues. Thank you very much for the opportunity to testify.

[The prepared statement of Mr. Morris follows:]

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 **John B. Morris, Jr.**
General Counsel, and Director of CDT's Internet Standards,
Technology & Policy Project
Center for Democracy & Technology

before the House Committee on Energy and Commerce,
Subcommittee on Commerce, Trade, and Consumer Protection and
Subcommittee on Communications, Technology, and the Internet

THE PRIVACY IMPLICATIONS OF COMMERCIAL LOCATION-BASED SERVICES

February 24, 2010

Chairman Rush, Chairman Boucher, and Members of the Subcommittees:

On behalf of the Center for Democracy & Technology (CDT), I thank you for the opportunity to testify today. We applaud the Subcommittees' leadership and foresight in examining the burgeoning area of commercial location-based services, and we appreciate the opportunity to address the privacy implications of what is one of the fastest growing areas of online innovation. As a note of introduction, I am an attorney and serve as CDT's General Counsel, but I also have a technical background, and I direct CDT's Internet Standards, Technology & Policy Project. This Project seeks to address the fact that the work of technical standards bodies such as the Internet Engineering Task Force (IETF) often has important impact on civil liberties and other policy concerns. In particular, I have been involved for the past nine years with the IETF's efforts to address and protect the privacy of location information, and I am a co-author of four IETF standards documents addressing location privacy.[1]

The Promise and Risks of Location-Aware Technologies

The widespread consumer adoption of increasingly high-powered mobile devices has already spawned the Internet's next generation of location-based services and applications. As the accuracy of location data has improved and the expense of calculating and obtaining it has declined, location has become an increasingly common part of the online experience, and location-based services are an increasingly important market for U.S. companies.

---

[1] RFC 3693, "Geopriv Requirements" (with J. Cuellar, D. Mulligan, J. Peterson, J. Polk) (Internet Engineering Task Force 2004) (defining requirements for technical protocol to protect privacy of location information transmitted over the Internet); RFC 3694, "Threat Analysis of the Geopriv Protocol" (with M. Danley, D. Mulligan, J. Peterson) (Internet Engineering Task Force 2004) (analyzing risks and threats to privacy of location information on the Internet); RFC 4745, "Common Policy: A Document Format for Expressing Privacy Preferences" (with H. Schulzrinne, H. Tschofenig, J. Cuellar, J. Polk, J. Rosenberg) (Internet Engineering Task Force 2007) (defining protocol format for expression of privacy preferences concerning location information); RFC 5606, "Implications of 'retransmission-allowed' for SIP Location Conveyance" (with J. Peterson, T. Hardie) (Internet Engineering Task Force 2009).

The availability of location information paves the way for exciting new applications, ranging from uses that support essential services to those that address less weighty needs. For example, firefighters in Washington, D.C., use a customized version of Google Earth that displays the real-time location of fire trucks in the city. In its first year of use, this software has reportedly saved the city $3 million.[2] At the same time, millions of users rely on location technology to guide them to the closest coffee shop or to help them navigate through unfamiliar neighborhoods.

But the easy availability of location information also raises several different kinds of privacy concerns. The idea of "Big Brother" always watching the citizenry has long been a concern for many in this country. Ubiquitous availability of individualized location information on a mass scale is ripe for abuse. Location services can reveal very private information and even put users at physical risk. Ensuring that location information is subject to neither commercial nor government misuse – but is instead transmitted and accessed in a privacy-protective way – is essential to the long-term success of location-based applications and services.

Location data comes in a variety of forms and these forms vary in sensitivity. Web analytics programs, which analyze a Web site's traffic, have long leveraged the fact that IP addresses can be roughly correlated to metropolitan areas to calculate the approximate locations from which Web site visitors access individual sites. But as technology has developed, it has become possible to determine the near-exact location of most mobile device users. While this capability has existed for some years within cellular networks, it is only recently that the explosion of location-based technologies and applications has begun, with every new device locatable in multiple ways and an oc of applications developers incorporating location-based features into their products. With the popularity of iPhones, Blackberries, and the myriad other smartphones on the market, hundreds of millions of users are all now easily locatable, as are many users of laptops, as Mozilla's Firefox – the second-most popular Web browser[3] – has also recently become location-enabled.[4]

The collection and use of fixed device location (such as home or business addresses) has obvious privacy implications. However, especially troubling privacy concerns arise from the collection of "mobile location data," which identifies the whereabouts of an individual or his or her device in real or near-real time.[5] In this testimony, we focus on the risks raised by the increasing collection and use of mobile location data.

---

[2] *See* CNBC, *CNBC Original: Inside the Mind of Google* (Dec. 3, 2009), http://www.cnbc.com/id/33831099/.

[3] As of January 2010, Firefox had over 250 million users. *See* Erick Schonfeld, *Where Did Internet Explorer's Browser Share Go?*, TechCrunch.com (Feb. 2, 2010), http://techcrunch.com/2010/02/02/internet-explorer-browser-share/.

[4] *See Location-Aware Browsing*, http://www.mozilla.com/en-US/firefox/geolocation/ (last visited Feb. 21, 2010); *Mozilla Advances the Web with Firefox 3.5* (June 30, 2009), http://www.mozilla.com/en-US/press/mozilla-2009-06-30.html.

[5] In 2009, CDT worked with companies and other advocacy organizations in our Internet Privacy Working Group (IPWG) to establish a workable and specific vocabulary to describe how data is stored and used online. This definition for "mobile location data" originates in the set of definitions that was released through that collaboration. *See* Center for Democracy & Technology, *Threshold Analysis for Online Advertising Practices* 16 (Jan. 2009), http://www.cdt.org/privacy/20090128threshold.pdf.

Because individuals often carry their mobile devices with them, location data may be collected everywhere and at any time, often without user interaction, and it may describe both what a person is doing and where he or she is doing it. It can reveal visits to potentially sensitive destinations, like medical clinics, courts, political rallies, and union meetings. The ubiquity of location information has also increased the risks of stalking and domestic violence as perpetrators are able to use (or abuse) location-based services to gain access to location information about their victims.[6] And, as an increasing number of minors carry location-capable cell phones and devices, location privacy will become a child safety matter as well.

Beyond the risks to individuals' privacy, the lack of privacy protection also creates market risks for the very companies seeking to capitalize on location services. As my fellow witness, Professor Lorrie Cranor, can explain in far greater detail, research shows that people value their location privacy, are less comfortable sharing their location with strangers than with acquaintances, and want granular control over their location information.[7] At the end of the day, location-based services stand to be more successful if there is a framework of privacy giving users confidence that their information will be protected.

The sensitivity of location information clearly puts it at high risk for misuse by companies and governments alike. As location information begins to pervade the Web experience, standards, policy, and law must develop in ways that contribute to the protection of location privacy. CDT believes that Congress can help to protect location privacy in two ways:

- The disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties. As Congress contemplates enacting baseline consumer privacy legislation, such a requirement should be part of a broader framework governing sensitive user data.
- The standards for government and law enforcement access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.

---

[6] *See, e.g.*, "Tracing a Stalker," Dateline NBC (June 16, 2007), http://www.msnbc.msn.com/id/19253352/; "Albert Belle pleads guilty to stalking ex-girlfriend," Associated Press (July 26, 2006), http://sports.espn.go.com/mlb/news/story?id=2530911&campaign=rss&source=ESPNHeadlines.

[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.

Understanding Location-Aware Technologies

The location of mobile devices can be determined through a range of technologies. Some of these technologies require the participation of an underlying wireless carrier, while others work without the involvement or even knowledge of a telecommunications company. Although there are a number of variations, the most significant location determination technologies can be grouped into the following six categories[8]:

Carrier-controlled or -involved location technologies:

1. Cell tower-based calculations: Among the oldest forms of mobile location determination are calculations based on the location of cell towers and the signals received by the carrier at one or more towers. In its simplest form, if two or three cell towers can detect a mobile device at the same time, the carrier can triangulate from the towers to determine the approximate location of the phone. Carriers can, if needed, make calculations based on the strength and direction of a phone's signal as received at a single tower. This type of location determination does not require special hardware or computing power in the handset. The precision of this technique is relatively low, on the order of hundreds or thousands of meters, and is dependent upon the density of cell towers in the vicinity of the handset.

2. GPS: By receiving signals from the Global Positioning System (GPS) satellites, a handset can determine its own location, and can transmit it to the carrier. GPS produces higher precision locations (on the order of meters or tens of meters). In the context of emergency calls, mobile handsets in the U.S. are designed to transmit GPS information (if it is available) whenever a 911 call is placed (and handsets can be configured to transmit GPS data to the carrier when other telephone calls are placed). In this context, one part of the handset (the cellular voice circuitry) requests the location from the GPS chip in the handset, and passes the location on to the cellular carriers. One drawback of GPS-based positioning is that it can take 30 seconds or more (sometimes much more) for the GPS chip to make an initial location determination.

3. A-GPS: To address the potential slowness of GPS positioning, "Assisted-GPS" technology was developed, combining both of the above two location technologies. Using a number of methods, GPS data is combined with cell-tower based information to significantly speed up the initial location determination while taking advantage of the higher precision of GPS.

Location technologies independent of carriers:

4. WiFi database lookup: The location of WiFi-capable devices (including nearly all laptops and smartphones) can be determined using a database to identify WiFi access points in the vicinity of the particular device. Both Google and Skyhook have developed databases of WiFi access points and their

[8] For a more detailed explanation of the various leading location determination technologies, see "Location Technologies Primer," TechCrunch (June 4, 2008), http://techcrunch.com/2008/06/04/location-technologies-primer/.

locations. When an application (such as Web browser or location-aware application) needs the location of the device, it sends a query to (for example) a Google database, and Google returns the location based on nearby WiFi access points. This lookup process takes place without the involvement or even knowledge of any cellular carrier used by the device (and indeed, by using this approach, devices that have *no* cellular capabilities can be located).

5. Cell tower database lookup: This approach is similar to a WiFi database lookup, except that the lookup is to a database of cellular tower locations. As with its WiFi access point database, Google has amassed a database of the locations of cell towers. When a device is accessing the Internet over a cellular data network, it can send a query to Google containing the cell tower ID that the device is connected to, and Google is able to return an approximate location. As with WiFi database lookups, this approach does *not* need the involvement of any carrier, even though locations are determined based on the locations of the carrier's cell towers.[9]

6. GPS: Finally, applications (including Web browsers such as Firefox and Apple's Safari) running on a mobile device can receive location information directly from a GPS chip in the device, *without* any involvement or knowledge of a carrier. The GPS information can in turn be sent to anyone on the Internet through the mobile data connection. And, because mobile Web browsers can connect to any Web site on the Internet, *any* Web page can include code that requests the user's location from the device.

Many smart phones can take advantage of all six of these location determination technologies,[10] and most new wireless devices – including cell phones, smart phones, e-book readers, laptops, netbooks, and even the new iPad – have at least one of these capabilities (and usually two or more). Moreover, as GPS and WiFi capabilities have been built into an increasing number of these devices, location information has become increasingly accurate.[11]

---

[9] For a discussion of how Google is able to automatically determine the location of cell towers, see "Google enables Location-aware Applications for 3rd Party Developers" (June 6, 2008), http://googlemobile.blogspot.com/2008/06/google-enables-location-aware.html.

[10] It is important to note that these six arrangements describe only how a device location can be determined, not how that location is used or later transmitted. The carrier-independent technologies result in the device knowing its own location. That location may then be used locally by applications on the device (such as Web browsers of mobile apps) or sent to a Web site or remote server. In the latter case, for handsets connected to a cellular network, the location may be transmitted as content over a cellular data connection. But this does not mean that the carrier is involved in locating the device, or that the carrier is even aware that the content contains the device's location. The positioning of the device and the transmission of its location to effectuate a particular application or service on the device can be entirely separate processes.

[11] One small study of the accuracy of these location-determining technologies on the 3G iPhone (the first mobile device to successfully integrate all of the primary location technologies) found that cellular network positioning yielded a median error of 600 meters, WiFi positioning yielded a median error of 74 meters, and GPS yielded a median error of 8 meters. *See* Paul A Zandbergen, *Accuracy of iPhone Locations: A Comparison of Assisted GPS, WiFi, and Cellular Positioning*, Transactions in GIS, Volume 13, Issue s1 (July 2009), http://gisandscience.com/2009/07/15/accuracy-of-iphone-locations-a-comparison-of-assisted-gps-wifi-and-cellular-positioning/.

In the past, telecommunications carriers served as gatekeepers of location information – data about a cell phone user's location was primarily calculated within a carrier's netw using the signals sent by the phone to the carrier's service antennas (as described as "cell tower-based calculations" above). As discussed more fully below, laws to protect users' location information were accordingly focused on the role of the carrier and offered a baseline of protection for how the carrier could share and use that information. But location information is now collected by a much broader spectrum of companies.

Consider the example of Yelp, a service used to find and rate businesses located near the user (allowing someone to find out "how good is that dry cleaner that I drive by every day?").[12] A consumer who uses the Yelp application on the location-enabled Apple iPod Touch provides her location information to Yelp entirely independently from any cell carrier – the iPod Touch is not a cellular device, and only has WiFi connectivity.[13]

The amount of location data that is sent independently from any cellular carrier is very significant and rapidly growing. As of July 2009, 3300 location-based applications were offered through application stores for mobile devices.[14] And in May 2009, Skyhook Wireless, the company that provides WiFi positioning for Apple products, AOL, and others, was receiving 250 million location requests *every day.*[15]

Moreover, the range of companies that potentially have access to location data is not limited to telecommunications carriers, location providers like Skyhook Wireless, application developers, or Web sites. From the user perspective, the number of possible uses for location data is ever-growing and the number of companies handling location information is continuously expanding as well: handset vendors, operating system vendors, advertisers, advertising networks, and analytics companies may also have access to precise, sensitive information about where users are located.

Existing Legal Standards For Access to and Protection of Location Information Are Woefully Inadequate

Although Congress has in the past sought to protect electronic communications, including location information, the technology has far outpaced the statutory protections, both regarding use of location in the commercial context, as well as protection of location from unwarranted government access. Clear privacy rules for location are a pre-requisite to the growth and success of new location-based services.

Although the focus of this hearing is on *commercial* use of location information, it is important to look at the inadequacy of legal protection in both the commercial and governmental contexts. Users want and demand a level of privacy around their location with respect to commercial entities – but they also seek locational privacy vis-à-vis the

---

[12] *See* Yelp, Inc. *Yelp: Version 4.0.0* (iPhone application), http://itunes.apple.com/us/app/yelp/id284910350?mt=8 (last visited Feb. 21, 2010).

[13] *See iPod Touch: Features*, http://www.apple.com/ipodtouch/features/ (last visited Feb. 21, 2010).

[14] *See* Skyhook Wireless, *Location Aware App Report: From the Apple, Blackberry, Android, Nokia and Palm App Stores* (July 2009), http://www.locationrevolution.com/stats/skyhookjulyreport.pdf.

[15] *See* Jenna Wortham, *Cellphone Locator System Needs No Satellite*, New York Times (May 31, 2009), http://www.nytimes.com/2009/06/01/technology/start-ups/01locate.html.

government. Thus, to promote and facilitate innovation and market acceptance of location-based services in the *commercial* context, it is important that Congress also act to protect location information in the law enforcement investigative context as well. Thus, before discussing the legal standards governing commercial use of location, we briefly address the inadequacies in the government context.

The Electronic Communications Privacy Act Should be Updated to Protect Location Information from Inappropriate Disclosure to Government

A lack of clear rules about law enforcement access to location information held by service providers has left location technology without sound legal footing. 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[16] 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] Finally, the Electronic Communications Privacy Act (ECPA),[19] while it sets a 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 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] But a plurality of courts have required a higher level of proof – probable cause – for law enforcement access to this prospective location information.[22] Just this month, the federal court of appeals in Philadelphia heard oral argument on the question of what

---

[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.*

[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).

standard should apply to stored location data, the first but probably not the last case to present that issue at the appellate level.[23]

Uncertainty about the privacy afforded to location information could restrain consumer adoption of location-based services. 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 the Digital Privacy and Surveillance Working Group – has convened technology and communications companies, privacy advocates and academics in an effort to arrive at consensus proposals to update ECPA. We plan to unveil those proposals in the coming weeks, including one that, if adopted, would bring clarity and simplicity to the law governing law enforcement access to location information.

Statutory Protection of Location Information in the Commercial Context is Also Inadequate

Just as technology has bypassed ECPA and other statutes on government access to information, technology has also bypassed statutes intended to protect location privacy in the commercial context. Foremost among these statutes are the CPNI rules, protecting "customer proprietary network information," including location. Although the CPNI rules continue to provide important protections, they are less and less relevant, and taken together, they and other laws do not provide sufficient protection for location information.

CPNI Rules

Starting with the Telecommunications Act of 1996, with subsequent amendments, Congress has prohibited a telecommunications carrier from disclosing 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."[24] With this minimal standard, Congress prohibited carriers from releasing location information on a solely discretionary basis.

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

- First, the CPNI rules simply do not apply to the most innovative and burgeoning types of location technologies, applications, and services. The CPNI rules do not cover *any* of the "location technologies independent of carriers" described above as technologies 4 through 6, because there is no telecommunications carrier involved in the location determination or location-based service. The WiFi-only iPod Touch example described above starkly

[23] *See* Brock Meeks, "Privacy Battle Over Cell Phone Tracking Data Hits Appeals Court," Center for Democracy & Technology (Feb. 12. 2010), http://www.cdt.org/blogs/brock-meeks/privacy-battle-over-cell-phone-tracking-data-hits-appeals-court.

[24] 47 U.S.C. § 222.

illustrates the limits of the CPNI rules, but even when location data is transmitted over a cellular network, the carrier is increasingly not directly involved in the location transaction. When an iPhone or Android user installs a location-based application, the location data transmitted by the resulting service is largely invisible to the telecommunications carrier over which the service is provided. The CPNI rules simply do not reach the location transaction.

- Second, 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,[25] Commissioner Copps explained the effect of the Order on the protection of location information under the CPNI rules:

  > [C]onsider a cutting-edge device like Apple's much-anticipated iPhone, which allows a user to communicate via IP-based Wi-Fi technology as well as traditional CMRS [Commercial Mobile Radio Service] service. Under our precedent, a consumer who uses the CMRS features of the device to place a phone call can be secure in the knowledge that our Title II CPNI rules require the carrier to protect his or her call and location information. But what about when that very same consumer uses that very same device just moments later to send an email via Wi-Fi, to call up a map of his or her location via a browser, or even to place a VoIP call to another Internet user? Because *those* services—which the customer can be excused for thinking of as functionally identical to the CMRS call—are now classified as Title I information services, the carrier appears to be entirely free, under our present rules, to sell off aspects of the customer's call or location information to the highest bidder.[26]

  In light of the Wireless Broadband Order, as Commissioner Copps explained, it appears quite possible that even carrier-provided location based services that run over the wireless *data* network are not protected by the CPNI rules. Although Congress and then the FCC did extend CPNI rules to cover IP-enabled "interconnected" VoIP services,[27] 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.

When first enacted almost 15 years ago, the CPNI rules were groundbreaking, and provided important protections for the primary wireless service used by Americans at

---

[25] *Appropriate Regulatory Treatment for Broadband Access to the Internet Over Wireless Networks*, Declaratory Ruling, WT Docket No. 07-53, FCC 07-30, 2, ¶ 2 (rel. Mar. 23, 2007), http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-30A1.pdf ("Wireless Broadband Order").

[26] Statement of Commissioner Copps, Wireless Broadband Order, at 1, http://fjallfoss.fcc.gov/edocs_public/attachmatch/FCC-07-30A3.pdf.

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

that time – voice. Now that our society is moving away from voice and to data, and our online interactions provide a far more robust window into our personal lives, the protections offered by the CPNI rules have been left behind.

Federal Trade Commission Act and State Attorneys General

Under its authorizing statute,[28] the Federal Trade Commission is empowered to challenge unfair and deceptive trade practices. Under this broad authority, the FTC has established some general precedents about what constitutes a deceptive or unfair privacy practice online – deviating from a stated privacy policy or failing to secure personal information are two examples. More specific authority has also been granted to the agency to deal with particular privacy issues, including spam, credit reporting, financial privacy, children's privacy, and telemarketing.

The FTC has a strong track record of pursuing bad actors engaged in egregiously deceptive or unfair practices – the agency's efforts in the spyware area provide good examples. However, the FTC has been hesitant to use its unfairness jurisdiction to address questionable privacy practices, and it lacks several important tools – including rulemaking authority and civil penalty authority – that are necessary for the agency to successfully protect consumers from privacy threats, including those related to location privacy. 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 do not live up to their privacy policies or that engage in other unfair or deceptive trade practices. To date, however, little attention has been paid at the state level to location privacy concerns.

ECPA

ECPA covers entities providing "remote computing services," defined as "the provision to the public of computer storage or processing services by means of an electronic communications system." This definition may cover providers of location-based services, who receive location data from a user, process it, and deliver value-added results to the user. In the absence of consent, remote computing services are prohibited from divulging the contents of communications they receive, but only if the communications are maintained "solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computing processing." That caveat, uncertainty about the scope of the definition of "remote computing service," and the ease with which subscriber consent can be obtained as part of terms of service, render ECPA unresponsive to user privacy concerns or, at the very least, leave consumers with the kind of ambiguity that provides little foundation for user confidence.

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

The Privacy Practices of Companies Collecting Location are Uneven at Best and Inadequate at Worst

In the face of inadequate statutory protection for location information, it is perhaps not surprising that the privacy practices of companies collecting location, and the granularity of controls they offer, range widely in terms of the level of protection that they provide. CTIA–The Wireless Association has, commendably, issued best practices to govern the provision of location-based services,[29] and CTIA has indicated that it is committed to maintaining its guidelines as technology evolves. However, the primary adherents to those self-regulatory guidelines are wireless carriers – which, as noted above, are far from alone in offering the newest location-based services, and are already bound by the CPNI rules.

Because of the sensitivity of location information, the users of location-based services deserve a robust set of protections to help manage the associated privacy risks. The list of possible protections is long: providing clear notice of when location information is being collected, offering robust user choice about when location can be collected, providing access to stored data (for example, showing maps of where the user has been), providing the ability to broadcast "fake" location, sending reminders to users that their location is being shared, applying de-identification techniques,[30] encrypting location information in transit and storage, and many others. Some providers of location-based services, such as Loopt (which provides location-based social networking) have fully integrated these kinds of protections into their products.[31] Others have included strong consent mechanisms, but failed to incorporate more comprehensive user control tools.[32] Still others have failed to incorporate even the most basic of protections – privacy policies.

Weak privacy protections put users at risk in two important ways. First, data collected about users may be retained long after the moment of data collection, and often long after the original location service has been provided. Whether the location information is stored by location providers like Skyhook Wireless and Google, by the developers of applications downloaded to the device, by location-aware Web sites, or by advertisers and analytics companies, this data may be shared, sold, or put to unpredictable uses far in the future. The second type of risk derives from services that share consumer location with acquaintances or with the public at large. While these technologies offer exciting new opportunities for Internet users, products built with defaults that do not protect privacy may place the uninformed user in dangerous situations.

---

[29] CTIA-The Wireless Association, "Best Practices and Guidelines for Location-Based Services," http://files.ctia.org/pdf/CTIA_LBS_BestPracticesandGuidelines_04_08.pdf.

[30] For example, when Google maps began collecting traffic data from location-enabled cell phones, it took steps to delete the starting and ending points of users' journeys. *See* Tom Krazit, *Google Maps adds traffic data from your cell phone* (Aug. 25, 2009), http://news.cnet.com/8301-30684_3-10317223-265.html.

[31] *See* Loopt, *Loopt: Privacy & Security*, http://www.loopt.com/about/privacy-security (last visited Feb. 22, 2010).

[32] *See* Alissa Cooper, *The Dawn of the Location-Enabled Web*, Center for Democracy & Technology (July 6, 2009), http://www.cdt.org/policy/dawn-location-enabled-web-0.

Unfortunately, many location-based products and services have not adequately addressed these risks:

- Many companies that offer applications for mobile devices collect real-time location data from their customers but offer no assurances for how that data will be protected: often their privacy policies fail to detail how location data will be used, shared, or sold. For example, the privacy policy for Foursquare, a location-based social networking service in which users "check-in" at their present locations and share these locations with friends through Facebook and Twitter, does not specifically describe how the location information Foursquare receives will be used, shared, or protected – in fact, it does not even mention the word "location," and the policy itself is not accessible before or during the application sign-up process.[33] Many other location-based services lack privacy policies all together.[34] Privacy policies alone offer little in the way of privacy protection, but their existence represents an important – and necessary – step toward promoting accountability: without a privacy policy, it is exceptionally difficult to even begin to evaluate a company's practices vis-à-vis user privacy.

- Services that publish user locations to friends or to the world vary considerably with respect to the privacy controls they offer. Two different products offered by Google illustrate this variation well. Google Latitude, released in February 2009, is a location-aware application that allows a user's cell phone location to be overlaid on Google Maps and shared with friends. Latitude was designed with privacy in mind. A user's location information is shared on an opt-in basis and only with friends the user has designated, location logs are by default delete and users who have enabled location-sharing receive periodic emails reminding them that the service is turned on.[35] In contrast, Google's Buzz for Mobile, released just a few weeks ago (one year after Latitude), has proven to be a privacy disaster. Buzz serves as a Gmail-integrated feed to which users can post thoughts, articles, photos, and similar updates. If the user has location services enabled on his or her mobile device, then every comment the user makes via Buzz Mobile by default includes his or her current location. If a user hasn't taken steps to make a Buzz private then the comment is tossed into the public "buzzstream," allowing anyone, anywhere in the world to track where the user is at any given time.[36] One could use Buzz to check out who is hanging out at the corner bar, attending a protest rally or visiting a particular medical facility. A new Web site, pleaserobme.com, was posted to highlight the risks inherent in making

---

[33] *See* Foursquare Labs, Inc., *Foursquare Labs, Inc. Privacy Policy* (Nov. 13, 2009), http://foursquare.com/legal/privacy.

[34] *See* Nick Doty, *Who's Using the W3C Geolocation API?* http://npdoty.name/location/services (last visited Feb. 21, 2010).

[35] *See e.g.*, *Google Latitude*, *http://www.google.com/latitude/intro.html* (last visited Feb. 21, 2010); Ryan Singel, *Google Latitude to Cops: 'I Don't Remember,'* Wired (March 5, 2009), http://www.wired.com/epicenter/2009/03/googles-latitud/; Robin Wauters, *Google Warns Latitude Users That They Might Be Sharing Their Location*, TechCrunch (Feb. 18, 2010), http://techcrunch.com/2010/02/18/google-warns-latitude-users-that-they-might-be-sharing-their-location/.

[36] *See* Leslie Harris, *Buzz or Bust*, The Huffington Post (Feb. 17, 2010), http://www.huffingtonpost.com/leslie-harris/buzz-or-bust_b_466133.html.

> such public announcements about location. The Web site provides a live feed of posts by Twitter and other users who have publicly announced that they are somewhere other than at home.[37]

As CDT has noted in its recent submission to the FTC on privacy, notice, choice and security comprise an incomplete framework for privacy protection. Privacy in the 21st century must be grounded in the full set of Fair Information Practice principles, including individual access, data minimization, and accountability. In the absence of this comprehensive framework,[38] many questions remain around the uses of location data and whether customers are being tracked against their will, whether location data is being protected throughout its lifecycle, and whether the entities that handle location data are giving sensitive location data the respect it deserves in terms of minimizing data collection and data uses and maximizing transparency, security,[39] and user control and consent.[40]

Given the privacy interests at stake, we would expect location controls to be better than other kinds of technological controls on the Web.[41] Unfortunately, the market has clearly not provided the protections users need for their location data.

Technical Standards Could Help Protect Location Privacy, but the Mobile Applications Industry Has Been Reluctant to Adopt Such Standards

CDT has worked since 2001 within the Internet Engineering Task Force (IETF) – the leading technical standards setting body for the Internet – on the development of a location privacy standard named "Geopriv."[42] One goal of Geopriv was to change the

---

[37] *See* Barry Borsboom, Boy van Amstel, and Frank Groeneveld, *Please Rob Me*, www.pleaserobme.com (last Visited Feb. 21, 2010).

[38] Center for Democracy & Technology, Refocusing the FTC's Role in Privacy Protection: Comments of the Center for Democracy & Technology In regards to the FTC Consumer Privacy Roundtable (Nov. 2009), http://www.cdt.org/files/pdfs/20091105_ftc_priv_comments.pdf

[39] Firefox has taken an important step toward protecting the security of location information. It establishes an SSL connection with its location provider, Google, in order to protect the location data being exchanged between the browser and the location provider. *See Location-Aware Browsing*, http://www.mozilla.com/en-US/firefox/geolocation/ (last visited Feb. 21, 2010).

[40] Important but often overlooked aspects of user control include: giving users the ability to obscure location or present a location other than their actual one - just as annonymization tools allow PC users to blur who or where they are, applications and devices should allow users to obscure their location; and allowing users to generate a whitelist of trusted sites that can always obtain the user's location and a blacklist of untrusted sites that cannot ever access it.

[41] Location-enabled browsers have so far offered pretty strong baselines for consent to location sharing. On the iPhone, for example, each Web site that wants to use location has to first obtain the user's permission not once, but twice. Those permissions are reset every 24 hours. However, the privacy controls offered by the iPhone still lack granularity. *See* Alissa Cooper, *The Dawn of the Location-Enabled Web*, Center for Democracy & Technology (July 6, 2009), http://www.cdt.org/policy/dawn-location-enabled-web-0.

[42] *See* Geopriv Working Group Charter, http://www.ietf.org/html.charters/geoprivcharter.html. For more information about this standard, see John Morris and Jon Peterson, "Who's Watching You Now?," IEEE Security and Privacy Magazine, Vol. 5, Issue 1 (January/February 2007), http://www.cdt.org/publications/20070100ieee.pdf; Alissa Cooper and John Morris, "Binding Privacy Rules to Location on the Web," Proceedings of the 2nd International Workshop on Location and the Web, LOCWEB '09 (Boston, Mass., Apr. 04, 2009), http://www.cdt.org/privacy/LocWebFinal.pdf.

historic reliance on privacy policies set by service providers, and to allow users to specify the rules that would govern use and retention of location information about the

Unfortunately, in a 2008 effort spearheaded by the leading browser vendors (including Opera, Mozilla, and Apple), a different standards body rejected the IETF approach and instead opted to continue to leave it up to individual service providers to issue privacy policies governing location. This other body, the World Wide Web Consortium (W3C), has far more influence over "applications layer" services (including most location services) than does the IETF. When W3C declined to follow the standards set by the IETF, it instead developed its own location standard that urges developers to respect privacy, but includes no technical steps that would help force developers to do so.[43] The W3C process is on going, and CDT is working to improve the W3C standard, but it is very unlikely that the W3C will change course to adopt the more privacy-protected approach created by the IETF.

Although the W3C standard does have good language urging developers to protect privacy, the experience in the marketplace ranges widely. A researcher at the University of California at Berkeley, Nick Doty, has sought to identify Web sites that are implementing the W3C location standard. Of the sites he has been able to identify, about one-third of them have *no privacy policy whatsoever*, and many of the rest are silent in their privacy policies about the handling of location information.[44]

This standards development issue is *not* one that Congress should directly seek to address – technical development is best left in the hands of industry and standards bodies, not governments. However, the failure of the W3C member companies to tr' strong action to protect location privacy highlights the kinds of privacy gaps that res. from allowing the marketplace to wholly dictate how privacy protections (or lack thereof) will evolve. The appropriate response from Congress should be to pass baseline privacy legislation that specially protects sensitive information such as location. If the United States adopts strong requirements to protect location privacy, the technology community will respond with standards and products that meet the legal requirements.

The Role of Congress

CDT believes that there are at least three specific measures needed to protect the privacy of location information, the first two of which would benefit from Congressional action:

- First, the disclosure of precise location information in a commercial context must only be made with specific, informed, opt-in consent in which a user has the ability to selectively disclose location only to trusted parties. As Congress contemplates enacting baseline consumer privacy legislation, such a requirement should be part of a broader framework governing sensitive user data.

---

[43] *See* W3C Geolocation Working Group Overview, http://www.w3.org/2008/geolocation/.

[44] *See* Nick Doty, Who's Using the W3C Geolocation API?, http://npdoty.name/location/services (last vis' ' Feb. 21, 2010).

- Second, the standards for government access to location information must be amended to make clear that a probable cause warrant is required for the government to obtain location information.
- Third, location-based services and applications should follow technical standards that give users clear control over the use of their location information and that require the transmittal of privacy rules with the location information itself.

Conclusion

CDT would like to thank the Subcommittees again for holding this important and forward-looking hearing. We believe that Congress has a critical role to play in ensuring that privacy of location information is protected as location-based services increasingly become ubiquitous. CDT looks forward to working with the Members of both Subcommittees as they pursue these issues further.

For more information, contact John Morris, jmorris@cdt.org, or Alissa Cooper, acooper@cdt.org, or at (202) 637-9800.

Mr. RUSH. The Chair recognizes Professor Cranor for 5 minutes for opening statement.

TESTIMONY OF LORRIE CRANOR

Ms. CRANOR. Chairmen Boucher and Rush, I thank you for the opportunity to testify today. My name is Lorrie Cranor. I am an associate professor of computer science and of engineering and public policy at Carnegie Mellon University. I have been asked to testify about privacy issues associated with the use of location information for commercial purposes.

Location-based services use a variety of technologies to acquire a user's location based on the current position of cell phone, computer or other device. These technologies typically use triangulation to locate the device based on signals from GPS satellites, cell towers or WiFi access points, often within a few hundred feet. Cellular providers can obtain location information of mobile phones in that manner even when the phones are not being used to place a call. The Internet address of a user's computer can also be used to determine an approximate geographic location, typically at a city level.

In April 2009, we conducted a survey at CMU to understand consumers' perceptions of location-sharing services. We asked participants about the degree of harm or benefit they associated with each of 24 scenarios. Participants rated finding people in an emergency as the scenario with the most significant benefit. Other highly beneficial scenarios included being able to track one's children and relatives, finding information based on one's location, and checking to see if people are OK. On the risk side, participants had significant privacy concerns. They saw great harm in scenarios involving stalking or revealing one's home address. They were also concerned about being found by people one wants to avoid or when one wants to be alone, having others intrude on one's personal space and being tracked by the government, and also receiving location-based ads.

We then evaluated 89 location-sharing applications and systems to determine the types of privacy protections that each one offered. We found that most of these applications provided fairly limited privacy concerns, and about a third of them did not even provide readily accessible privacy policies on their Web site. Some location-sharing applications had generic privacy policies that don't explicitly mention location. Others mention that they provide privacy controls but in order to see what controls are provided, a consumer has to actually use the service. Most of the applications with privacy controls required users to click multiple screens to reach the privacy settings.

Some of the privacy controls that allow users to specify that their location information should be shared only with their friends rather than with the general public turn out to actually have exceptions. For example, many services have a simple privacy switch. It looks very simple. It says on and off. But in one service we examined, text positioned four paragraphs below the switch mentions that there are actually two exceptions in which location information will be shared even when the privacy switch is not set to share information.

Our research at Carnegie Mellon has explored offering fine-grained and expressive privacy controls. The Locaccino system we developed allows users to specify location-sharing rules based on time, location and the person making a location request. For example, I have set up a rule that allows students to find my location when I am on campus so they can determine if I am in my office or teaching in another building. Another rule allows my family members to locate me at all times and locations. And another rule allows people I work with to locate me between 8 a.m. and 6 p.m. on weekdays. Locaccino is not being used for advertising, but a similar approach could be used to control when and where location information is used for location-based advertising.

Our research suggests that Internet users are definitely concerned about their location privacy but that most currently available location-sharing services do not do a good job informing them about how their location information will be used or provide users with expressive location privacy controls and privacy protective default settings. Thus, additional privacy protections may be necessary.

While the CTIA best practices offer a useful framework that requires notice and consent about location use, they do not specify form, placement, manner of delivery or content of notices nor do they provide enforcement. Thus, while users may opt in to a service by signing up for it, they may not realize what they are getting themselves into. As the Web site pleaserobme.com suggests, users may not think through the implications of broadcasting their location information to the public or even be aware that a service makes their location information public. Indeed, the CTIA best practices do not discuss what should happen when location information is disclosed publicly.

Even when users understand and are comfortable with the commercial use of their location data, the use of this data without a warrant by law enforcement has troubling implications. Due to the way cellular technology works, the widespread use of cell phones enables large-scale round-the-clock surveillance of citizens. It is important that the storage of individual location data be minimized and that protections be put in place to limit when it can be disclosed.

Finally, it is important to realize that techniques to deidentify personal information may not be effective when it comes to location information. Even when a person is not identified by name, her location trails may be used to identify her. Since most of us go to a particular location for work each weekday and a particular location to sleep each evening, with only a few days of location trails information combined with other publicly available information, it becomes possible to identify most people. Thus, users who try to hide behind made-up names may still unwittingly be identifying themselves when they make their location information public. Thus, it is important that privacy be considered from the beginning in the design of location-based services and that users of these services are fully informed about the privacy implications of their use.

Thank you for inviting me to testify today. I look forward to answering your questions.

[The prepared statement of Ms. Cranor follows:]

Written Testimony of
Lorrie Faith Cranor
Associate Professor of Computer Science and of Engineering & Public Policy,
Carnegie Mellon University

United States House of Representatives, Energy and Commerce Committee
Subcommittee on Communications, Technology and the Internet, and
Subcommittee on Commerce, Trade, and Consumer Protection
Hearing on
The Collection and Use of Location Information for Commercial Purposes
February 24, 2010

Chairmen Boucher and Rush, Ranking Members Stearns and Radanovich, and members of the committees, I thank you for the opportunity to testify about privacy issues associated with the use of location information for commercial purposes.

My name is Lorrie Faith Cranor. I am an associate professor of computer science and of engineering & public policy at Carnegie Mellon University. I am also the director of the CyLab Usable Privacy and Security Laboratory at Carnegie Mellon. I am a member of USACM, the U.S. Public Policy Council of the leading professional society for computer scientists.

I have been conducting privacy research for over a decade. I have studied Internet users' privacy concerns, how they make decisions about privacy, and their use and comprehension of privacy policies.[1] Along with my colleagues and students, I have developed technologies and standard approaches for communicating about privacy online, including a search engine that provides information about website privacy policies[2] and a privacy "nutrition label."[3] I have also been involved in a Carnegie Mellon University project to develop a location-sharing service that allows

---

[1] http://cups.cs.cmu.edu/#privacy-decision

[2] http://privacyfinder.org/

[3] http://cups.cs.cmu.edu/privacyLabel/

users to control when, where, and with whom to share their location information.[4] We have used this system as a platform for our privacy research.[5]

I have been asked to testify about privacy issues associated with the use of location information for commercial purposes. I will first provide a brief overview of how location-based services work. Then I will discuss consumer perceptions of risks and benefits of location-sharing technology. Next, I will discuss privacy controls in location-sharing applications. Finally, I will discuss some of the policy implications of my research findings in this area. Much of my testimony here is based on a paper I co-authored last summer with Janice Tsai, Patrick Gage Kelley, and Norman Sadeh, which I have included as an appendix to my written testimony.[6]

Locating Technologies

Location-based services (LBS) offer a wide range of functionality, including: providing maps and local information to users, allowing users to share their locations with their friends, allowing people to track other people such as their employees or children, using player location information in electronic games, and providing location-based advertisements. These services use a variety of technologies to acquire a user's location based on the current location of the user's cell phone, computer, or other device. Some devices, such as smart phones, may use more than one locating technology. The following are locating technologies in common use today:

- **Global Positioning System (GPS)** locates a user through a device that triangulates a location based on signals it receives from a constellation of satellites. GPS is often unavailable indoors.

---

[4] http://www.locaccino.org/

[5] http://www.locaccino.org/science

[6] J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-Sharing Technologies: Privacy Risks and Controls. TPRC 2009, August 2009. http://cups.cs.cmu.edu/LBSprivacy/

- **Wireless positioning** locates a user by listening for signals of nearby WiFi access points and sending information about detected signals to a service that maintains a database of access point locations.
- **Cellular identification** locates a user by triangulating their position based on the cell towers within signal range of their mobile phone. Cellular providers can obtain location information of mobile phones in this manner even when the phones are not being used to place a call.
- **IP location** locates a user by looking up the Internet address of the user's device in a database that maps IP addresses to geographic locations. Internet addresses can be shared by multiple computers and may change over time. This technique typically provides only city-level location information.

Consumer Perceptions of Risks and Benefits of Location-Sharing Technology

In April 2009 we conducted an online survey to understand consumer perceptions of the risks and benefits associated with location-sharing services. Our non-random survey sample consisted of 587 respondents recruited through notices on websites that offered the opportunity to win a $75 gift card.

We showed survey participants a screen-shot of an online location-sharing service and asked them to list some benefits and some risks of using this technology. Then we described 14 scenarios that focused on benefits of location sharing and 10 scenarios that focused on risks of location sharing. For each scenario we asked participants to provide numeric ratings for the degree of harm or benefit they associated with each scenario. Participants rated finding people in an emergency as the scenario with the most significant benefit. Other highly beneficial scenarios included being able to track one's children, finding information based on one's location, checking to see if people are ok, and tracking relatives. Participants saw only limited benefit to using location-sharing technologies to meet new people

based on their location. On the risks side, participants saw great harm in scenarios involving stalking or revealing one's home address. They were also concerned about being found by people one wants to avoid, having others intrude on one's personal space, being found when one wants to be alone, being tracked by the government, and receiving location-based ads.

Overall, we found that most of our participants did not expect that location-sharing technologies would be all that beneficial to them, and they have significant concerns about their privacy when sharing their locations online.

Privacy Controls in Location-Sharing Applications

In August 2009 we evaluated 89 location-sharing applications and systems to determine the types of privacy protections each offered. Overall, we found that most of these applications provided fairly limited privacy controls and about a third of them did not provide readily accessible privacy policies on their websites. We reviewed the websites for these applications again in February 2010 and found similar results for the 84 services still in existence at that time. Privacy policies are notoriously difficult for consumers to understand, and many location-sharing services do not provide prospective users with a clear picture of how their location information will be used and shared before they sign up for the service. However, reading the fine print reveals that many location-sharing services store users' profile and location information indefinitely.

Some location-sharing applications have generic privacy policies that don't explicitly mention their use and sharing of location information. Others mention that they provide privacy controls, but in order for a consumer to see what controls are provided they have to actually sign up for and use the service. Only 18 of the 84 services examined in February 2010 mentioned privacy controls or security on the front page of their website (where they typically describe the benefits of their service and try to convince people to sign up for it).

We found that 76% of the applications had some form of privacy controls. However, most of these required users to visit or click multiple screens to reach the privacy settings. Most commercial systems had fairly basic privacy controls that allowed them to control whether their location would be made available publicly or would be made available only to designated friends. Some also had "invisible" modes where a user could prevent their location from being made available to anyone (other than the service provider itself). Few allowed people to choose to provide some locations on a less granular level such as neighborhood or city rather than street address or provided other fine-grained controls.

Some of the privacy controls that allow users to specify that their location information should be shared only with their friends rather than with the general public turn out to have exceptions. For example, many services have a simple privacy switch that can be set to "on" or "off." But in one service we examined, text positioned four paragraphs below the switch mentions "two exceptions" in which location information will be shared publicly even when the privacy switch is set not to share this information.

Our research at Carnegie Mellon University has explored the possibility of offering users more fine-grained and expressive privacy controls than typically found in commercial location-sharing systems. The Locaccino system, developed as part of our research, allows users to specify location-sharing rules based on time, location, and the person making a location request. For example, I have setup a rule that allows students to find my location when I am on campus so that they can determine whether I am in my office or teaching in another building. Another rule allows my family members to locate me at all times and locations. And another rule allows people I work with to locate me between 8 am and 6 pm on weekdays. Locaccino is not being used for advertising, but I could imagine a similar approach being used to control when and where location information is used for location-based advertising.

Our research has demonstrated that people have nuanced privacy preferences, and that providing them with the ability to control location sharing based on time and location offers substantial benefit over simpler privacy controls.[7] Of course, these more expressive privacy controls could become confusing and burdensome to users if not designed carefully to be easy and quick to use, with well-chosen, privacy protective default settings. We are currently exploring approaches to reduce user burden when using expressive privacy controls.[8]

Discussion

Our research suggests that Internet users are concerned about their location privacy, but that currently available location-sharing services do not, for the most part, do a good job informing them about how their location information will be used or provide users with expressive location privacy controls and privacy-protective default settings. Thus additional protections may be necessary.

While the CTIA Best Practices and Guidelines for LBS providers[9] offer a useful framework that requires notice and consent about location use and disclosure, they do not specify "form, placement, manner of delivery or content of notices," nor do they provide enforcement mechanisms or assurances that all LBS providers will follow them. Thus, while users may explicitly "opt-in" to a service by

---

[7] M. Benisch, P. G. Kelley, N. Sadeh, T. Sandholm, L. F. Cranor, P. Hankes Drielsma, J. Tsai. The Impact of Expressiveness on the Effectiveness of Privacy Mechanisms for Location Sharing. CMU-ISR Tech Report 08-141. http://reports-archive.adm.cs.cmu.edu/anon/isr2008/CMU-ISR-08-141.pdf

[8] P. Kelley, P. Hankes Drielsma, N. Sadeh, L. Cranor. User Controllable Learning of Security and Privacy Policies. *AISec 2008.* http://patrickgagekelley.com/file_download/1/aisec14-kelley.pdf

[9] Best practices and guidelines for location-based services. Version 3.18.08. CTIA Wireless Association (April 2 2008). http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.

signing up for it, they may still not realize what they are getting themselves into. Users remain somewhat confused about the extent to which their location information may be shared and how they can control that.[10] And as the website Pleaserobme.com suggests, users may not fully think through the implications of broadcasting their location information to the public, or even be aware that a service makes their location information public.[11] Indeed, the CTIA Best Practices do not discuss the possibility that location information might be made public or recommend additional steps to be taken to notify users.

Even when users understand and are comfortable with the commercial uses of their location data, the use of this data without a warrant by law enforcement has troubling implications. Due to the way cellular technology works, the widespread use of cell phones enables large-scale round-the-clock surveillance of citizens. It is important that the storage of individual location data be minimized and that protections be put in place to limit when it can be disclosed to the government.

Finally, it is important to realize that techniques to de-identify or anonymize personal information may not be all that effective when it comes to location information. Even when a person is not identified by name or other commonly-used identifier, her location trails over time may be used to identify her. Since most of us go to a particular location for work each weekday and a particular location to sleep each evening, with only a few days of location trails information combined with

---

[10] L. Jedrzejczyk and B. A. Price and A. K. Bandara and B. Nuseibeh. I Know What You Did Last Summer: risks of location data leakage in mobile and social computing. http://computing-reports.open.ac.uk/2009/TR2009-11.pdf

[11] Pleaserobme.com is a website that displays publicly available location information from Twitter and Foursquare that indicates individuals who are not at home. The site creators write that their goal is to raise awareness of the risks associated with making personal location information available publicly. http://pleaserobme.com/why

other publicly available information it becomes possible to identify most people.[12] Thus, users who try to hide behind made-up names may still unwittingly be identifying themselves when they make their location information public. In addition, services that attempt to de-identify their users by removing their names before disclosing their location information may not be effectively anonymizing this data. Thus, it is important that privacy be considered from the beginning in the design of location-based services, and that users of these services are fully informed about the privacy implications of their use.

Thank you for inviting me to testify today. I look forward to answering your questions.

---

[12] P. Golle and K. Partridge. On the anonymity of home/work location pairs. Pervasive, 2009. http://xenon.stanford.edu/~pgolle/papers/commute.pdf

Appendix

J. Tsai, P. Kelley, L. Cranor, and N. Sadeh. Location-Sharing Technologies: Privacy Risks and Controls. TPRC 2009. Updated February 2010.
http://cups.cs.cmu.edu/LBSprivacy/

Location-Sharing Technologies: Privacy Risks and Controls

Janice Y. Tsai, Patrick Gage Kelley, Lorrie Faith Cranor, Norman Sadeh

Carnegie Mellon University
Pittsburgh, PA
jytsai@andrew.cmu.edu, pkelley@cs.cmu.edu,
lorrie@cs.cmu.edu, sadeh@cs.cmu.edu
Updated February 2010

Abstract. Due to the ability of cell phone providers to use cell phone towers to pinpoint users' locations, federal E911 requirements, the increasing popularity of GPS-capabilities in cellular phones, and the rise of cellular phones for Internet use, a plethora of new applications have been developed that share users' real-time location information online [27]. This paper evaluates users' risk and benefit perceptions related to the use of these technologies and the privacy controls of existing location-sharing applications. We conducted an online survey of American Internet users (n = 587) to evaluate users' perceptions of the likelihood of several location-sharing use scenarios along with the magnitude of the benefit or harm of each scenario (e.g. being stalked or finding people in an emergency). We find that although the majority of our respondents had heard of location-sharing technologies (72.4%), they do not yet understand the potential value of these applications, and they have concerns about sharing their location information online. Most importantly, participants are extremely concerned about controlling who has access to their location. Generally, respondents feel the risks of using location-sharing technologies outweigh the benefits. Respondents felt that the most likely harms would stem from revealing the location of their home to others or being stalked. People felt the strongest benefit were being able to find people in an emergency and being able to track their children. We then analyzed existing commercial location-sharing applications' privacy controls (n = 89). We find that while location-sharing applications do not offer their users a diverse set of rules to control the disclosure of their location, they offer a modicum of privacy.

1 Introduction

By 2009, at least 87% of the U.S. population owned cellular phones [3]. The proliferation of mobile devices and mobile Internet devices (including laptops) along with federal E911 requirements and the ubiquity of GPS-capabilities in mobile devices has spurred the development of location-sharing applications [27]. These technologies, also referred to as *mobile location* technologies, *social mobile* applications or simply *location-based services* (LBS), typically allow users to share their real-time or historical location information online.

Despite the increased availability of these location-sharing applications, we have not yet seen wide adoption [11, 23]. It has been suggested that the reason for this lack of adoption may be users' privacy concerns regarding the sharing and use of their location information [5, 14, 17, 23]. To explore these concerns regarding location-sharing technologies, we examine the use of LBS and research related to user's perceptions and use of location-sharing technologies in Section 1. Next, we investigate and enumerate the privacy controls offered by existing applications in Section 2. In Section 3, we present the results of an online survey to determine the magnitude of users' expected risks and benefits associated with these applications. Finally, in Section 4 we evaluate the ability of existing location-sharing technologies to address user's perceived risks and provide recommendations for controls to address users' privacy concerns.

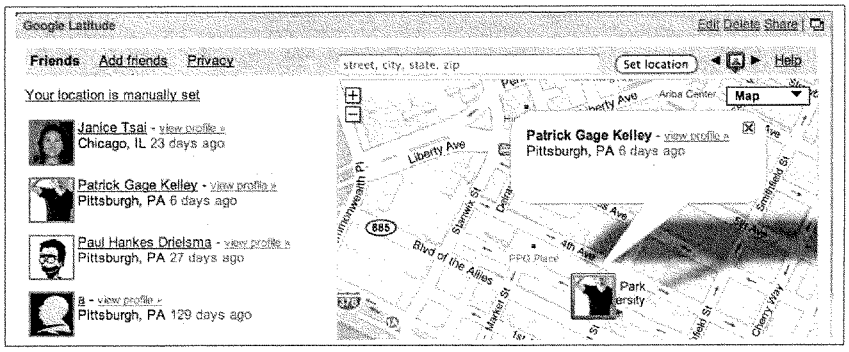


Fig. 1: The web interface for Google Latitude

1.1 Locating Technologies

The location-information shared by LBS may be text-based (e.g. "Andrew has been located at 5000 Forbes Ave., Pittsburgh, PA"), or it may be map-based, where the user's location is represented as a dot on a map as illustrated in Figure 1 and Figure 2. To display location information, users can manually enter a street address or longitude and latitude coordinates. Today, location information is more frequently acquired through automated means.

The following locating technologies are typically used to determine users' locations:

- **GPS:** The Global Positioning System (GPS), locates a user through a device that is in communication with a constellation of satellites. Triangulation by multiple satellites locates the device, making GPS the most accurate method for finding locations [27]. However, drawbacks include the lack of user-accessible GPS capabilities in most personal cell phones and the scarce availability of built-in GPS technology in commercial laptops. Additionally, GPS can be battery intensive and inconsistent or unavailable indoors.
- **Wireless positioning:** As urban areas become blanketed with both personal and public WiFi access points, users can be mapped according to the location of these access points. Through the process of "war-driving" access points, and mapping each broadcasting point to a GPS location [20], researchers and companies such as Skyhook Wireless[1] have created large databases with high location accuracy. While these locations are not always as precise as GPS, more people have wireless devices and location information can be pinpointed indoors.
- **Cellular identification:** At any given time, a mobile phone is likely in signal range of upwards of three cell phone towers, allowing a location to be triangulated if the locations of the cell towers are known. Some companies have partnered with telecom companies to use cellular data. One such company, AirSage[2] analyzes wireless signaling data to model traffic patterns.

[1] Skyhook Wireless. http://www.skyhookwireless.com/
[2] AirSage. http://www.airsage.com

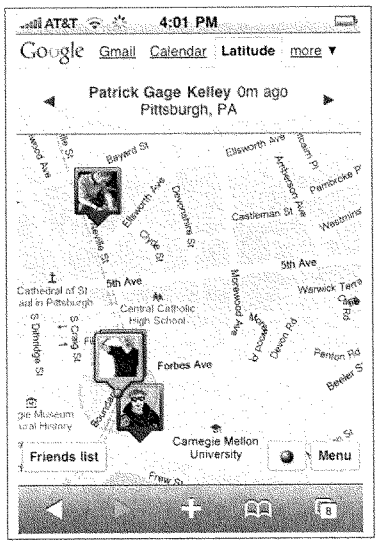


Fig. 2: The iPhone interface for Google Latitude

Loopt, a location-sharing service also leverages a cellular partnership with AT&T to provide always-on location information based on a user's iPhone [13].

- **IP Location:** Devices connected to an Internet network are provided with an IP address. IP addresses are limited in number; and based on the range, can be associated geographically [26]. (See the IP-to-Country Database.[3]) IP location is mostly used as a fallback when none of the above methods are available. The resolution of such lookups is commonly mapped to an area as large as a city.

1.2 Development Platforms for Locating-Technologies

Locating technologies are available for mobile phones, laptops, and internet-enabled mobile devices. There are three common ways for applications to pull location information:

- **Installed Software:** Users download and install software onto their cell phones or computers. Software determines the user's approximate location by one of the methods listed above and stores that data in a database or sends it to a location-sharing application. This transmission of coordinates may be automatic (e.g. a location ping is sent every 5 minutes) or it may require a "push" action to be initiated by the user (e.g. the user clicks a "Find me now" button).

[3] IP-to-Country Database. http://ip-to-country.webhosting.info/

- **Web browser:** In lieu of requiring the user to run a separate piece of software, several companies have developed location-finding web browser plug-ins. Applications that use this technology allow users to visit a website to be located, typically according to the users' wireless or IP location, based on an installed plug-in, such as Skyhook's web toolbar Loki.[4]
- **Location Broker:** APIs, (e.g. Yahoo!'s FireEagle[5] and Google Latitude[6]) allow developers to create applications that pull the user's location from a central provider. This allows application developers to entirely avoid any of the location lookup technologies, relying on a third party to provide location information.

1.3 Industry Best Practices

The worldwide revenues from mobile marketing are projected to reach $24 billion in 2013 [2]. It is understandable that the mobile or wireless industry would want to spur the adoption of location-sharing technologies. LBS may detect users' locations and offer them advertisements for businesses or services nearby. To address users' privacy concerns, CTIA, the International Association for the Wireless Telecommunications Industry,[7] issued Best Practices and Guidelines for LBS providers. These guidelines are meant to help LBS providers protect user privacy and rely on two of the Fair Information Principles (FIPs), *user notice* and *consent* .

The guidelines include the following [1]:

- **Notice:** First, LBS providers must inform users about how their location information will be used, disclosed and protected so that a user can make an informed decision whether or not to use the LBS or authorize disclosure.
- **Consent:** Second, once a user has chosen to use an LBS, or authorized the disclosure of location information, he or she should have choices as to when or whether location information will be disclosed to third parties and should have the ability to revoke any such authorization.

The CTIA guidelines do not specify the "form, placement, manner of delivery or content of notices" [1]. Generally, providers provide their statements regarding notice and consent in their posted privacy policies or terms of service.

1.4 Location Privacy Studies

Researchers have conducted studies to examine the usage of location-sharing applications and the privacy concerns raised by these applications. These studies have employed the experience sampling method (ESM) where users have carried devices to simulate location requests [4, 10, 19]. Other small laboratory experiments have involved small groups of participants who are members of existing social groups where people requesting locations were provided with automatic location disclosures [5, 9], or users responded via SMS with location information [16, 29]. Field studies

[4] Loki. http://loki.com/
[5] FireEagle. http://fireeagle.yahoo.net/
[6] Google Latitude. http://www.google.com/latitude/apps/badge
[7] The CTIA Wireless Association. http://www.ctia.org/

have been conducted by the authors and their colleagues, where we deployed a location-sharing application in a college campus community[30].

Research has shown that the primary dimensions of privacy concern surrounding the disclosure of this information include *context* and *use* [5, 6]. The willingness to share one's location and the level of detail shared depends highly on *who* is requesting this information [10, 21] (or knowing who is requesting this information [30]), and the *social context* of the request [9, 19]. Due to users' varied privacy concerns and preferences depending on the situation [21] or activity in which the user may be engaged [16], privacy controls need to be flexible [4, 28] and include a mechanism to provide plausible deniability [29].

In addition to the context of a location request, it is users' own perceptions of the *use* of one's location information that impacts their privacy concerns [6, 10]. For example, a user may be more concerned with an acquaintance requesting his or her location because they are unsure of *why* that information is being requested compared to users' lack of concern when sharing location information with people nearby to find restaurant recommendations.

1.5 Studies of Privacy Controls

Another cause of privacy concerns may be the lack of adequate controls for the disclosure of real-time personal information. Other studies have examined rules and the users desired diversity in the expressiveness of permissions in these types of systems [4, 7, 24]. In some cases, it may be enough for some users to simply create groups of contacts to assign permissions [15, 24], but others may require more flexibility in their rules [4] . In other research, it was found that a greater degree of rule expressiveness (e.g. being able to create group, time, and location-based rules) may increase the efficiency of allowing users to share information without violating their own personal privacy preferences [7], and that relationship-based default rules and machine learning techniques may reduce user burden in creating expressive rules [18, 25].

Based on this existing work, we delve into the design of commercial location-sharing systems and survey participants on their perceptions of the benefits and risks of specific scenarios of use for location-sharing systems.

2 An Evaluation of Privacy Controls in Location-Sharing Applications

We evaluated 89 applications, social networks, and APIs to evaluate their privacy controls. See the Appendix for a list of the applications. Our privacy and location-based services data is available online for download.

2.1 Method

We used a user-contributed online list of location-based services[8] as our directory of sites. In general, the sites on this list are social in nature. We found its completeness to be unparalleled across the web. We removed from consideration any sites that were not location-based services, or

[8] A list of Location Based Social Networking sites. http://bdnooz.com/lbsn-location-based-social-networking-links/. Last visited August 10, 2009.

sites that were offline or defunct (n = 10). This leaves us with a final set of 89 applications.[9] We did not consider "surveillance technologies."

To create our dataset, we completed a number of steps. First, we first visited the website for each application. We read the "About" page, frequently asked questions (FAQ), "Help" pages, and any other documentation available to search for explanations of their privacy controls. Additionally, we evaluated web interfaces, Facebook applications, and screen shots and descriptions of the iPhone application in the iTunes App Store. We evaluated the following features of these applications:

- **Date of launch:** While many of the current location-based services have been relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public, or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.
- **Privacy Policy:** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service).
- **Privacy Controls:** We noted any ability that allowed users to control access to their location information.
- **Notice:** Some systems notify users when others request their location, or make an activity log available to allow users to see who has requested and received their locations.
- **Immediately accessible privacy settings:** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled "Privacy" would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.

2.2 Data Analysis

We constructed a datasetbased on our collection of the features listed above. In this section, we present the results of our analysis.

System Characteristics The primary purpose of the majority of these applications was for tracking friends or finding new ones. Other highlights included sites geared towards location-based dating, travel planning and sharing, and information seeking (e.g. finding local "hot spots"). One site even allows users to tag speed traps.

Of the 89 applications surveyed, 63 are available for use on mobile phones. Of those phone-based applications, the iPhone was the most popular development platform (40 applications). Application developers also created products for the Blackberry (32), phones that use the Android OS (21), or other phones (34). These numbers include services that developed a mobile formatted web version of their application and are not mutually exclusive. For example, a single service may have an iPhone application, a Blackberry application, and an Android application.

The architectures of the location-sharing applications fell into two categories:

- **Open:** Users can be found by friends and strangers.

[9] Note: One of the applications included on the list, Locaccino, was developed by the authors.

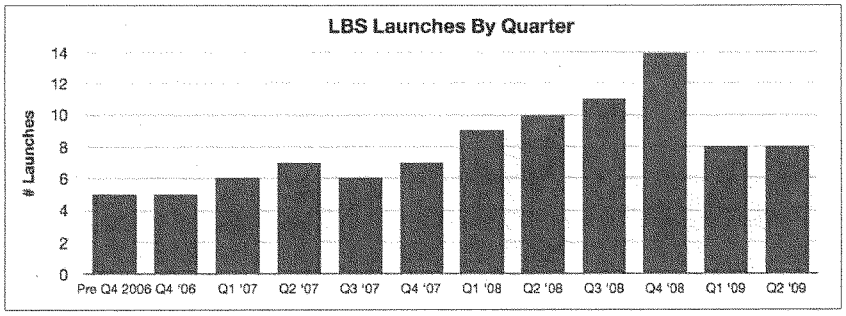


Fig. 3: The number of location-sharing applications launched each quarter (includes 89 applications evaluated in our study and 7 defunct applications).

- **Closed:** Users may only be requested by "friends" on the system. In this case, users much have already granted the requester access (e.g. by accepting a friend request).

Of the surveyed applications, five did not allow users to request other users' location information; but allowed users to seek information about places or landmarks; and two are location-sharing APIs. Of the remaining sites, 29 are closed systems, and 52 are open systems.

Rate of Creation The development of location-sharing applications has steadily increased over time as shown in Figure 3. Several new technologies may have spurred the development of location-sharing technologies. These include the launch of Yahoo's FireEagle platform (Q1 2008) and the iPhone SDK[10] with its Core-Location framework (Q3 2008).

The rate at which location-based services were introduced to the market increased from 5 per quarter at the end of 2006 to 14 per quarter at the end of 2008. After the economic downturn in 2008 the rate of introduction slowed, but new services continue to be introduced in 2009 at a rate of at least 8 per quarter. This overall growth leads us to believe two things. First, the development-side technologies are in place for location-based services and social networks to be created, and there are not unsolvable technical issues in the way of growth. Second, there do not seem to be strong market leaders who are prohibiting others from entering the market. Even with large players like Google, and established brands like Loopt, we have not seen any one of these technologies spread to a large section of the populace (however, finding active user data for any of these services has proven to be difficult).

Privacy Controls Due to the sensitive nature of real-time location information and the existence of guidelines recommending clear notice to users, one would expect all location-sharing applications to detail their policies for the collection and use of personal information. Instead, we found only

[10] iPhone Dev Center. http://developer.apple.com/iphone/

Category	Yes	No	Unknown	Not Applicable
Privacy Policy	66.3% (59)	33.7% (30)	-	-
Privacy Controls	76.4% (68)	16.9% (15)	1.12% (1)	5.62% (5)
Accessible Privacy Settings	16.9% (15)	75.3% (67)	2.25% (2)	5.62% (5)

Table 1: An overview of the proportion of applications that have privacy policies, privacy controls, and explicit privacy settings.

66% of the applications had privacy policies at all. For those services that did have privacy policies, the majority collect and save all data (e.g. locations, personal information entered into one's profile, and identifying web information such as one's IP address) for an indefinite amount of time. Only one, Mologogo[11] explicitly stated that it deletes GPS data after one month. Another interesting exception is Google Latitude which stores only the most recent location update.[12]

Our review of location-sharing applications reveals that the majority do have some form of privacy controls (76%). However, the majority of those privacy controls are not easily accessible from the main page or home page of the application itself. For the applications we reviewed, over 70% required users to visit or click multiple screens before they reached the privacy settings (see Table 1). This lack of immediately accessible privacy controls may be a result of the small amount of screen real estate available to application developers, especially in the case of mobile phones. For example, there was one case (Rummble[13]), included in the "Yes" category for accessible privacy settings in Table 1, where the web interface for the system had a link to the privacy controls, but the iPhone interface did not.

The types of privacy controls for the location-sharing applications are the following:

- **Blacklist:** Users are able to block specific individuals from viewing their location. (Found in 15.7% (14) of services.)
- **Friends Only:** This whitelist-based control restricts access to users denoted as a "Friend." By default, closed systems are considered friends only. (Found in 49.4% (44) of services.)
- **Granularity:** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. "Andrew is in Pittsburgh, Pennsylvania.") (Found in 12.4% (11) of services.)
- **Group:** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the "college friends" group to view my location.) (Found in 12.4% (11) of services.)
- **Invisible:** This feature may also be termed the "Private," "Only me," or "No one" setting. Users continue to send location data, but their locations are not divulged. (Found in 34.8% (31) of services.)
- **Location-based rules:** This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as "Work" or select an area on a map, and their location information is revealed to anyone who requests them when they are at that location. (Found in 1.12% (1) of services.)

[11] Mologogo. http://www.mologogo.com/
[12] Privacy (Google Latitude). https://sites.google.com/a/pressatgoogle.com/latitude/privacy
[13] Rummble. http://www.rummble.com/

- **Network:** This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location. (Found in 12.4% (11) of services.)
- **Per-request permissions:** Users must specifically review each location request, and decide whether or allow or deny the request prior to the location being revealed. (Found in 2.25% (2) of services.)
- **Time-based rules:** Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm). (Found in 1.12% (1) of services.)
- **Time-expiring approval:** Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is "live." During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible. (Found in 2.25% (2) of services.)
- **No restrictions:** Anyone is able to view the user's location. (Found in 16.9% (15) of services.)
- **Not Applicable:** Privacy controls do not apply. (Valid for 5.62% (5) of services.)
- **Unknown:** We were unable to find information about the privacy controls. (1.12% (1) service.)

In general, we see that the "Friends Only" and "Invisible" restrictions are the most prevalent. Of the 89 applications we reviewed, only four provided explicit notice to the user regarding who had requested their location. Aka-Aki,[14] Locaccino,[15] and Mobiluck[16] provide request logs to the user so they can view "Who's Viewed Me," Sniff[17] sends out a text message notification providing the name of the person making the request, and HeyWay[18] requires the user to explicitly approve or reject each location request (providing the name of the requester making the request). The native Loki browser plug-in explicitly asks the user if an application is making a request can access that information, but does not provider the name of the person making the request. Only one specific application Locaccino[19] had time-based and location-based rules.

3 Location-Sharing Risk/Benefit Analysis

We conducted an online survey to understand the magnitude of the risks and benefits associated with location-sharing services.

3.1 Method

For an individual user to accept a technology, an acceptable balance of personal risk and benefits must be established [12]. To understand these risks and benefits, we investigated the perceived-risk attitude or the expected value of location-sharing risks and benefits towards the use of location-sharing technologies. This evaluation takes into account the willingness or likelihood of engaging in the activity as a function of its expected benefit or harm [8]. We conducted an online survey to

[14] Aka-Aki. http://www.aka-aki.com/
[15] Locaccino. Note: the authors of this paper were also involved in the development of this application. http://www.locaccino.com
[16] Mobiluck. http://www.mobiluck.com
[17] Sniff. http://www.sniffu.com/
[18] HeyWay. http://niftybrick.com/heyway.html
[19] Locaccino. http://www.locaccino.org

capture users' perceptions of how likely certain scenarios would be if they used location-sharing scenarios and the magnitude of benefits or risks related to each scenario.

Recruitment In April 2009, we solicited participants to complete a survey to examine their personal perceptions about location-sharing technologies. Online announcements were posted on the "Volunteers" section of craigslist.com for major metropolitan areas of the United States and in online sweepstakes websites, recruiting individuals over the age of 18. The survey was available online for two weeks. We raffled a $75 Amazon.com gift certificate as the incentive for participation.

Demographics The final survey sample consisted of 587 respondents. Although 655 people completed the survey, respondents who completed the survey in under 4 minutes were eliminated from the final dataset. Due to the number of questions in the survey, we believed that anyone who answered in under 4 minutes was simply clicking through the survey, rather than reading and responding to the questions. Participants' ages ranged from 18 to 79 years of age (M = 35.7), and 61% were female. The respondents were fairly well educated, with 43.8% indicating that they had college degrees and 29.1% having graduate degrees. In general, most people (72.4%) had heard of technologies that allow people to share their locations with others.

3.2 Survey Data Analysis

Technology Use At the beginning of the survey, an example of an online-location sharing technology was presented to the study participants. A screen shot of of a map with a thumbnail of a person's picture pinpointed on the map was displayed, indicating that the person had been located with this technology (see Figure 4). Participants were asked to list some benefits and risks or dangers associated with this technology.

Some examples of benefits listed by our respondents are the following:

- Give out directions quickly to friends and family.
- Able to track loved ones and opportunity to surprise someone for a special event.
- People you know can find you, parents can track their kids, facilitates a rendezvous.
- Serendipitous encounters.
- Remote awareness of friends and relatives.

Some examples of dangers listed by our respondents are the following:

- Anyone could know exactly where you are - there is no privacy - anyone could find you at any given time.
- If someone intends to do you harm, they would find you easily.
- An unwanted person will find you and stalk you. It is not safe. You have no control.
- Location history could be harvested for stalking or marketing.
- People could find out if no one was home.

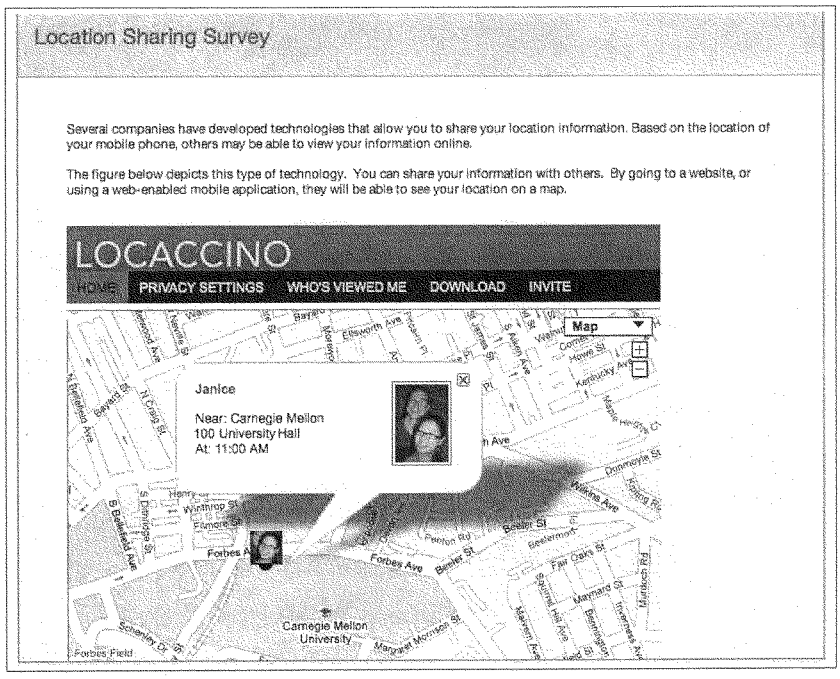


Fig. 4: A screen shot of the location-sharing interface presented to our survey participants

Respondents were asked a series of 7-point Likert scale questions asking them to rate the usefulness of location-sharing technologies (ranging from *not useful* (1) to *extremely useful* (7)), their privacy concerns surrounding their use of these technologies (ranging from *not concerned* (1) to *extremely concerned* (7)), and the risk of using these applications (ranging from *the risk far outweighs the benefit* to *the benefit far outweighs the risk*). These questions were asked both at the beginning and end of the survey to determine if participating in the survey altered users' opinions.

The results reveal that people's first impression of location-sharing technologies is that they are mostly not useful. After taking the survey, which included various usage scenarios, people's opinions changed slightly, and they found the technology slightly more useful. They also became more concerned about allowing others to view their locations at the end of the survey. Participants' attitudes about the risk of using location-sharing technologies slightly outweighing the benefits did not change: they felt that the risk still outweighed the benefits. See Table 2 for mean values and paired t-test p values.

Item	Before	After	t statistic	p value
Usefulness	3.72	3.94	-3.91	**<0.001**
Concern	5.15	5.42	-4.66	**<0.001**
Risk	3.27	3.33	-1.01	0.31

Table 2: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful*) (7), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), and the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the beginning and end of the survey. The degrees of freedom for the paired t-tests is 586.

Item	M	t statistic	p value
You	3.84	-1.84	0.07
Family	3.67	-3.78	**<0.001**
Friends	4.30	4.05	**<0.001**
Company/Employer	3.63	-4.52	**<0.001**

Table 3: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)). The responses are compared in a t-test to the midpoint (4). The degrees of freedom for the t-test are 567.

In the survey, we also asked participants about how concerned they were about controlling access to their location on a scale of *not concerned* (1) to *extremely concerned* (7). We found that participants were extremely concerned about having control (M = 6.17).

We also asked participants to rate the likelihood of the use of location-sharing technologies by him or herself, their family, their friends, or their company or employer. Based on a 7-point Likert scale ranging from *very unlikely* (1) to *very likely* (7), we find that people think it is unlikely that their families and employers will use location-sharing technologies. As for themselves, they are neither likely nor unlikely to use the technologies, but think that they friends are more likely to use these types of applications. The responses to this question and their comparison to the midpoint of the scale are summarized in Table 3.

Gender Differences Dividing participants by gender, we see that men find location-sharing technologies slightly more useful than women do, but men still find these technologies neither useful nor useful. Women are also much more concerned with allowing others to view their locations, tend to feel that the risk of using these technologies far outweighs the benefit, and do not find it likely that they will use these technologies. These responses are detailed in Table 4.

Scenarios We asked participants to rate the likelihood of the occurrence of the scenarios below on a 7-point Likert from very unlikely to very likely. Each scenario is also rated as a harm or a benefit. For each of the harms scenarios, participants were asked to rate each harm from a scale from *not*

Item	Female	Male	t statistic	p value
Usefulness	3.77	4.20	-2.78	**.006**
Concern	5.60	5.14	3.73	**<0.001**
Risk	3.07	3.72	-4.19	**<0.001**
Likeliness of Use	3.56	4.26	-3.8	**<0.001**

Table 4: Participants' responses to 7-point Likert scale questions regarding the usefulness (*not useful* (1) to *extremely useful*) (7), concerns associated with allowing others to view your location (*not concerned* (1) to *extremely concerned* (7)), the risk of using location-sharing technologies (*the risk far outweighs the benefit* (1) to *the benefit far outweighs the risk* (7)) at the end of the survey, and the likeliness of use by the respondent. The degrees of freedom for the two-sample t-tests is 585.

harmful at all (1) to *extremely harmful* (7). For each of the benefits scenarios, participants were asked to rate each benefit on a scale from *no benefits at all* (1) to *great benefit* (7).

The responses to the scenarios are detailed in Table 5 and Table 6.

There were several scenarios in which people would be extremely likely to benefit from such services: finding people in an emergency, finding information based on location, and finding (tracking) their children. Based on the survey results, people also seem to realize that using location-sharing technologies will likely open them to receiving advertisements based on their location, being intruded upon, as well as accidentally revealing the location of their homes.

Level of Privacy Concern We sought to determine the level of privacy concerns that people perceive when they are sharing their information online by asking several privacy scale questions. These privacy scale questions are based on an instrument developed by Malhotra et al. to measure Internet Users' Information Privacy Concerns (IUIPC) [22]. The IUIPC scale defines several groupings of concern, including control, awareness of privacy practices, collection of information, errors, unauthorized secondary use, improper access, and global information privacy concern; and consists of 27 questions. Based on a pilot test where we correlated the use of Facebook, an online social network, and the use of its privacy settings, we selected a sampling of 6 questions. Based on these questions, we calculated a "Privacy score" for each respondent. This score is an average of the ratings of the following six statements presented to the users, rated on a 7-point Likert scale, ranging from *strongly disagree* (1) to *strongly agree* (7). The higher the privacy score, the more concerned the person is about their privacy.

Participants were asked to rate the following statements:

- It is very important to me that I am aware and knowledgeable about how my personal information will be used. (IUIPC Awareness)
- I'm concerned that online companies are collecting too much personal information about me. (IUIPC Collection)
- Online companies should have better procedures to correct errors in personal information. (IUIPC Errors)

Scenario	Likelihood	Benefit
Finding people in an emergency	5.64	5.97
Finding information based on your location	5.29	4.99
Keeping track of the location of children in your family	5.17	5.18
Checking people's locations to make sure they are ok	4.98	5.05
Finding nearby friends for social activities	4.76	4.36
Using people's locations to coordinate a meeting	4.67	4.34
Keeping track of elderly relatives	4.66	5.11
Keeping track of where you've been	4.65	3.84
Coordinating family activities	4.59	4.39
Finding a coworker who is running late for a meeting	4.42	4.03
Coordinating ride sharing or carpooling	4.38	4.29
Having fun with locations	4.35	3.47
Recruiting people to participate in activities	4.01	3.83
Finding new people with similar interests	3.49	3.46

Table 5: Benefits-based location-sharing scenarios and their likelihood and magnitude of benefit ratings based on survey results, ordered by highest likelihood.

- Online companies should never share personal information with other companies unless it has been authorized by the individuals who provided the information. (IUIPC Unauthorized secondary use)
- Online companies should take more steps to make sure that unauthorized people cannot access personal information in their databases/servers. (IUIPC Access)
- I am concerned about threats to my personal privacy today. (IUIPC Global Concern)

To determine if this scale was internally reliable, we compute a Cronbach's α score for this set of questions. This statistic allows us to determine if the items, together, measure a consistent viewpoint. A set of items with a Cronbach's α score of above 0.70 is considered to be reliable. We found this 6-item scale for assessing users privacy concerns regarding online companies to be reliable, with a Chronbach's α of 0.85.

To determine if the privacy score had any relation to users' use and perceptions of location-sharing technologies, we examined their correlations. We see that the higher the privacy score, the more likely it is that users will feel that the risks of using location-sharing technologies outweigh the benefits (Risk After, $r(586) = -0.23$, $p < .0001$); that they would be less likely to use such technologies ($r(586) = -0.12$, $p = 0.004$); and feel that this technology is not useful (Usefulness After, $r(586) = -0.11$, $p = .007$). Additionally, users with higher privacy scores were older ($r(586) = 0.23$, $p < .0001$), more concerned about privacy (Concern After, $r(586) = 0.41$, $p < .0001$), and more concerned about controlling access to their location($r(586) = 0.39$, $p < .0001$).

Expected Values of Risks and Benefits To examine the ranking of the scenarios, we computed an expected value for the risk variable by multiplying the likelihood perceptions by the magnitude

Scenario	Likelihood	Harm
Being bothered by ads that use your location	5.27	4.68
Having people intrude on your private space	5.15	5.51
Revealing the location of your home	5.11	5.93
Being found by someone you don't want to see	5.10	5.56
Being found when you want to be alone	5.07	5.08
Revealing activities you are participating in	4.83	4.17
Being stalked	4.75	6.32
Having the government track you	4.62	5.38
Being judged based on your location	4.35	4.50
Having your boss spy on you	4.21	5.15

Table 6: Risk-based location-sharing scenarios and their likelihood and magnitude of harm ratings based on survey results, ordered by highest likelihood.

of the risk (harms) or benefit. This value allows us to compare within the sets of scenarios that are considered harms and those that are considered benefits.

Within each set of harms and benefits, the expected value for the risk (or benefit) of each was compared to the other harms or benefits with paired t-tests to determine which scenarios are significantly distinct from each other ($p < 0.05$). The relative rankings for the benefits and risks as determined by their expected value are summarized in Table 7 and Table 8.

Evaluating each expected benefit, one sees that, by far, the most significant benefit is being able to find people in an emergency. The next distinct benefit is being able to track one's children. Finding information based on one's location, checking to see if people are ok, and tracking relatives are the third set of distinct benefits. The least valued expected benefit of location-sharing technologies is finding new people based on one's location.

The greatest expected harms derived from the use of location-based technologies are revealing one's home and being stalked. People perceive that being found by people one wants to avoid and having others intrude on one's personal space are the next set of situations associated with these technologies. Being found when one wants to be alone, being tracked by the government, and receiving ads based on one's locations are the third set of distinct harms. It seems that people are the least bothered by the risks of being judged based on one's location and revealing activities that one is participating.

Analysis of participants with children One potentially useful scenario for location-sharing technologies is keeping track of children in one's family. We asked participants to list the number of children they had, and divided our participants into two categories: those who have children and those who do not. The group with children includes those with adult children. Demographics are summarized in Table 9. We see that having children does have an impact of one's perceptions of these technologies.

Participants with children rated location-sharing technologies significantly more useful at the beginning of the survey as compared to participants without children ($M_{WithChildren} = 3.93$ vs.

Ranking	Scenario
1.	Finding people in an emergency
2.	Keeping track of the location of children in your family
3.	Finding information based on your location
3.	Checking people's locations to make sure they are ok
3.	Keeping track of elderly relatives
4.	Finding nearby friends for social activities
4.	Using people's locations to coordinate a meeting
4.	Coordinating family activities
5.	Coordinating ride sharing or carpooling
5.	Discovering that a friend from out of town is visiting
6.	Keeping track of where you've been
6.	Finding a coworker who is running late for a meeting
7.	Recruiting people to participate in activities
7.	Having fun with locations (e.g. games, pranks)
8.	Finding new people with similar interests

Table 7: The relative rankings of benefits obtained from the use of location-sharing technologies.

$M_{WithoutChildren}$ = 3.59, $t(585)$ = -2.17, p = 0.03). After taking the survey, both groups felt the same about location-sharing technologies being neither useful nor not useful ($M_{WithChildren}$ = 4.08 vs. $M_{WithoutChildren}$ = 3.85, $t(585)$ = -1.5, p = 0.13).

When asked about the likelihood of use of these types of technologies, participants with children were significantly more likely to feel that they, their families, friends and employers would be likely to use these technologies as compared to people without children. See Table 10 for details of survey results and t-tests.

Examining the responses to the scenarios, we see that participants with children derived greater expected benefit, as compared to respondents without children from the following scenarios: checking people's locations to make sure they are ok, coordinating family activities, keeping track of the location of children in your family, keeping track of elderly relatives, and finding new people with similar interests. Those with children also had a greater amount of expected risk from being bothered by ads that use their location, being tracked by the government, and revealing activities they are participating in. These differences are detailed in Table 11.

For respondents with children, being able to track their kids becomes the top benefit, tied with being able to find people in an emergency. Even when we control for age and gender, we find this to be the case.

4 The Ability of LBS Applications to Address Users' Perceived Risks

As location-based services proliferate in numbers but not in users [11, 23], we examined the ability for these location-sharing applications to address users' privacy concerns. We see that the number of applications has been increasing and companies have developed platforms that make it easier for

Ranking	Scenario
1.	Revealing the location of your home to people you do not want to give your address to
1.	Being stalked
2.	Having people intrude on your private space
2.	Being found by someone you don't want to see
3.	Being found when you want to be alone
3.	Having the government track you
3.	Being bothered by ads that use your location
4.	Having your boss spy on you
5.	Revealing activities you are participating in
5.	Being judged based on your location

Table 8: The relative rankings of risks related to the use of location-sharing technologies.

Item	Without Children	With Children
Gender	Fem: 218, Male: 147	Fem: 140, Male: 82
Avg. Age	30.9	43.7

Table 9: Participants characterized by whether or not they have children or do not have children.

others to create applications that leverage location information. Based on the results of our survey, we see that people still do not find these location-sharing technologies all that useful, and they are still concerned about their privacy when sharing their locations online. In general, people still believe that the risks of sharing their locations online outweigh the benefits.

Based on our analysis of the risks associated with these technologies, we now examine the existing privacy controls of these technologies and investigate the ways in which these controls can address users' major concerns. We also suggest additional methods of addressing users' concerns.

4.1 Addressing risks with privacy controls

To determine if privacy controls are effective in location-sharing technologies, we first examine users' greatest expected risks.

As enumerated in Table 8, we see that the top ranked expected risks are the following:

- Revealing the location of your home to people you do not want to give your address to
- Being stalked
- Having people intrude on your private space
- Being found by someone you don't want to see
- Being found when you want to be alone.
- Having the government track you.
- Being bothered by ads that use your location .

Below, we examine how location-based applications' privacy controls address these concerns.

Item	Without Children	With Children	t statistic	p value
You	3.67	4.11	24.01	**<0.001**
Family	3.32	4.26	28.36	**<0.001**
Friends	4.27	4.36	26.52	**<0.001**
Company/Employer	3.48	3.87	26.21	**<0.001**

Table 10: Participants' responses to 7-point Likert scale question regarding the likelihood of the use of location-sharing technologies (very unlikely (1) to very likely (7)) for people without children and with children. The degrees of freedom for the t-test are 585.

Item	Without Children	With Children	t statistic	p value
Okayness Checking	25.0	29.9	-4.06	**<0.001**
Coordinating Family Activities	20.5	26.1	-4.65	**<0.001**
Tracking Children	26.1	34.6	-6.18	**<0.001**
Tracking Relatives	24.2	29.9	-4.12	**<0.001**
Finding New People	13.0	16.0	-2.8	**0.005**
Bothered by Ads	24.7	27.7	-2.35	**0.02**
Tracked by the Government	25.3	28.0	-1.98	**0.05**
Revealing One's Activities	20.1	22.4	-2.08	**0.04**

Table 11: Participants' expected benefits and risks based on if they have children or if they do not have children. The values were calculated by multiplying the likelihood ratings of each secenario with its rated risk and benefit. Degrees of freedom for the two-sample t-tests are 585.

Blacklist: With blacklists, users are able to block specific people with whom they do not wish to reveal this location. This restriction allows users to protect against revealing the location of their homes, block known stalkers and people they do not wish to see. If users are active in managing and updating their blacklists, they may also reduce the ability to having people intrude on their space, and avoid being found when they want to be alone. Unfortunately, in the last two cases, users must spend the effort and time to add people to a blacklist, and must remember to remove people from the blacklist once they want to be found again.

Friends Only: By solely allowing all friends to access users' locations, this protects users from being stalked (users may remove their stalkers from their friend lists). Unfortunately, this control does not protect from being found by friends when one wants to be alone or being found by someone who is a friend, but whom you may not wish to see. To deal with these concerns, users may manage their friend lists by adding and removing friends as they see fit.

Granularity: Allowing the location-sharing application to only provide general information (e.g. neighborhood, city, or state) about one's location mitigates the risks (except for being bothered by ads and and being tracked by the government). Unfortunately, by only providing a wide range of possible locations, this also negates the benefits provided by location-sharing applications.

Group-based rules: Allowing people access to your location by dividing them into groups mitigates several privacy concerns. These group-based rules allow users to protect the location of their homes, to hide themselves from stalkers, and to avoid people they do not want to see. Based on how large one's group is and how active they are in assigning people to groups may also reduce, but not eliminate the risks of having people intrude on their private space and being found when they want to be alone.

Invisible: By going invisible, the user reduces the risks listed above except for that of being bothered by location-based ads and government tracking. The user can significantly reduce the risk of being stalked or of being found by people they don't want to see, but they also reduce the benefits of these services. To most effectively deal with the risks, they must be very active in turning invisible mode on and off, which places a significant burden on the user.

Location-based rules: Defining access by location allows the user to effectively protect the location of his home or spaces in which one needs private space or alone time. These rules may also block known stalkers at locations they do not wish to reveal. By continuously updating these rules, users may effectively address most of the risks, but this requires users to regularly update their rules.

Network: A network is typically larger than a group (e.g. the Chicago network). This may make it easier for users to define rules, but may not be an effective means in protecting them from the risks listed above. By defining network based rules, one prevents the general public from locating them, but may not keep stalkers within their network from finding them, or it may not prevent others from finding the location of their home, or preserving their personal space and alone time.

Per request permission: Requiring users to approve of each location request reduces the risks listed above except for that of being tracked by the government and being bothered by ads. Unfortunately, this method requires that users be interrupted, and this may become too burdensome on the user.

Time-based rules: Basing restrictions on time allows users to create restrictions to protect the locations of their homes (assuming they are home at regular times). Time-based restrictions can also protect users from being intruded upon, being found, and allows them to be be alone at certain times of day or days of the week.

Time-expiring approval: Allowing users to specifically permit others to locate them mitigates most risks (excluding government tracking and being served with advertisements based on their location). Unfortunately, allowing users to be the only ones to "push" location information also negates most of the top benefits of location sharing (e.g. one would not be able to find someone in the case of an emergency when they need to wait for the user to make his location available for a small period of time).

No restrictions: Having no rules allows users to be located by anyone. This opens them up to all the benefits as well as the risks of using location-sharing technologies.

We see that the rules that allow users to mitigate the greatest risks are the following:

- Blacklist
- Granularity

- Group-based rules
- Location-based rules
- Time-based rules

Each of these rules alone, including the burden on the user, does not address the largest expected risks of using location-sharing technologies. We find that location-sharing technologies offer limited flexibility in their privacy controls. It is rare that systems give users the ability to specify expressive rules to control the sharing of their location information. Furthermore, there are no commercially available systems that offer anywhere near as powerful a control set as one could imagine: with the ability to specify rules based on specific users and groups of contacts, to control access based on time and location, to return locations at varying granularities, and to become invisible or obfuscate locations in extreme situations. There is one system, Locaccino, developed by the authors their university, that offers time, location, and group based rules, as well as invisibility. A combination of all of these rules would be the most effective in addressing users' privacy concerns.

Another factor that has been mentioned briefly is user burden. In some cases, it would be possible for the user to toggle being invisible on and off all day, based on that day's events. Unfortunately, in our experience, people easily forget to do this. Once the location-sharing software is up and running, it is easier to leave it running; otherwise, once people go offline or invisible, they are likely to leave the software in that setting. Similarly, in systems that do offer a myriad of privacy controls, methods must be developed to help users create rules based on their daily schedules, and regular and irregular interactions with others.

4.2 Discussion

By defining the relative value of users' expected risks and benefits regarding the use of location-sharing services, we develop an understanding users' privacy concerns. We see that, in general, industry guidelines do not address these concerns, and the privacy controls in existing applications do not comprehensively address these concerns. In this paper, we have provided recommendations for sets of privacy control that may assist developers in addressing users' privacy concerns.

Based on the current perceptions of benefits and harms of location-sharing technologies at this time (noting that perceptions of risks in this area may evolve or shift), the primary risks can be addressed or mitigated by the design of the location-sharing technology. Based on the current restrictions offered by location-sharing technologies, we find that these risks may not be addressed, in full, by the current palette of available privacy controls. Instead, location-sharing applications may want to consider making more expressive privacy controls available to their users. With more expressive controls, people may become more comfortable with sharing their location information and find more value in these services. Additionally, future work must be done to determine how to reduce user burden. A balance must be found between expressiveness and usability or with offering users complex and detailed privacy controls and making these controls easy to use.

Another matter to consider is that of users' evolving privacy concerns. Currently, we find that users' still do not find location-sharing services useful. This may be due to the lack of usage in general. Without a critical mass of users, current users are unable to reap the benefits of being

able to find their friends or to track family members. As more and more people adopt these types of technologies, and peer opinion about these technologies becomes more favorable, the level of concern that people feel may diminish. Additionally, we find that it is younger people or people with children who are more interested in location-sharing applications and are more likely to adopt these services.

Appen| Location-Sharing Applications

As of 2/20/10

Open Systems: Users can be requested by people with whom they do not have a connection (i.e. Strangers)

Closed Systems: Users must be "Friends" or connected to one another

* Application also has time and location-based access restrictions

Application	Creation Date	URL	Push / Pull	System	Accessible Privacy	Privacy Policy Aug 2009	Privacy Policy Feb 2010	Policy Mentions Location	Home Page Mention	Black-list	Explicit Request	Friends	Gran-ularity	Group	In-visible	Network	Time Expire	None	N/A	Un-known
Aka-Aki	03/01/07	http://www.aka-aki.com/	Push	Open	No	Yes	Yes	Yes	Yes			X			X					
Belysio	08/22/08	http://www.belysio.com/	Pull	Open	No	Yes	Yes	Yes	No			X			X	X				
Blim	10/17/06	http://www.blim.com/	Pull	Open	No	No	No	--	Yes			X			X					
Bluemapia	06/17/08	http://www.bluemapia.com/	Push	Open	No	No	No	--	No						X					
Blummi!	10/18/08	http://www.blummi.com/	Pull	Open	Unknown	No	No	--	No				X							
Brightkite	04/01/07	http://www.brightkite.com/	Push	Open	Yes	Yes	Yes	Yes	No			X	X	X	X	X				
Buddy Beacon	11/10/06	http://where.com/buddybeacon/	Pull	Open	No	Yes	Yes	Yes	Yes	X										
BuddyCloud	04/01/08	http://www.buddycloud.com/cms/	Push	Open	No	No	No	--	No				X							
BuddyMob	12/01/08	http://www.buddymob.com/	Push	Open	No	No	No	--	No									X		
Buddyway	08/11/08	http://www.buddyway.com/	Push	Open	No	No	No	--	No									X		
Buzzd	02/06/08	http://buzzd.com/	Pull	Open	No	Yes	Yes	No	No			X			X					
Carticipate	03/08/08	http://www.carticipate.com/	Push	Open	No	Yes	Yes	No	No									X		
Centrl	03/16/07	http://centrl.com/	Pull	Open	No	Yes	Yes	Yes	No			X				X				
CitySense	06/09/08	http://www.citysense.com/	Pull	N/A	NA	Yes	Yes	No	No										X	
ComeTogethr	10/01/08	http://www.cometogethr.com/	--	Open	Yes	Yes	Missing	--	No			X		X	X					
Doppir	07/01/07	http://www.doppir.com/	Push	Closed	No	No	No	--	No			X								
EagleTweet	04/04/09	http://eagletweet.com/	Push	Open	No	No	YES	Yes	No											
FindbyClick	12/21/06	http://www.findbyclick.com	KILLED NOVEMBER 2009			No													X	
FindMe	03/18/08	http://electricpocket.com/findme/	Pull	Open	No	No	No	--	No						X					
FireEagle	08/12/08	http://fireeagle.yahoo.net/	Pull	API	Yes	Yes	Yes	Yes	Yes				X		X	X				
Flaik	11/26/07	http://www.flaik.com/	Pull	Open	Unknown	No	No	--	No											X
Footprint History	02/01/09	http://www.footprinthistory.com/	Push	Closed	No	Yes	Yes	No	Yes			X								
FourSquare	03/13/09	http://foursquare.com	Push	Closed	No	Yes	Yes	Yes	No			X								
Foyage	12/01/08	http://i.foyage.com	Pull	Open	No	No	No	--	No						X					
Friends on Fire	03/13/09	http://apps.facebook.com/on-fire/	Pull	Closed	Yes	Yes	Yes	Yes	Yes			X	X							
GeoMe	10/01/08	http://www.geo-me.com	Push	Closed	No	Yes	Yes	Yes	No			X								
GeoSpot	03/12/08	http://www.geospot.com/gs/Home	Push	N/A	NA	Yes	Yes	No	No										X	
GeoUpdater	12/10/08	http://linuxinside.org/geoupdater/	Push	Closed	Yes	Yes	Yes	No				X	X			X				
Google Latitude	02/04/09	http://www.google.com/latitude	Pull	Closed	Yes	Yes	Yes	Yes	Yes	X		X								
Groovr	12/29/08	http://www.Groovr.com	KILLED JANUARY 2010			Yes						X		X						
Gympse	05/22/09	http://www.gympse.com/	Push	Closed	Yes	Yes	Yes	Yes	No			X					X			
GyPSii	03/06/08	http://www.GyPSii.com/	Pull	Open	No	Yes	Yes	Yes	No			X			X					
HeyWay	06/17/09	http://nifty brick.com/heyway.html	Push	Closed	No	No	No	--	Yes		X	X		X		X				
HiMyTribe	08/07/09	http://www.himytribe.com/	Push	Closed	No	No	No	--	No			X		X						
ICloseby	01/30/08	http://www.icloseby.com	Push	Open	No	No	No	--	No	X										
iPling	06/29/07	http://www.iPling.com	Push	Open	No	Yes	Yes	Yes	No				X							
Ipoki	12/18/07	http://www.ipoki.com/	Pull	Open	Yes	Yes	Yes	Yes	No			X			X					
IRL	04/19/09	http://corp.triconnect.com	Pull	Open	No	No	YES	Yes	No									X		
LightPole	01/01/07	http://www.lightpole.net	KILLED OCTOBER 2009			Yes													X	
Limbo	08/01/07	http://www.limbo.com	Push	Open	No	Yes	Yes	No	No	X				X						
Locaccino*	03/01/09	http://www.locaccino.org	Pull	Closed	Yes	Yes	Yes	Yes	Yes			X		X		X				
Locatik	05/22/08	http://www.locatik.com	Pull	Open	No	Yes	Yes	Yes	No									X		
Locatrix	04/08/09	http://www.locatrix.com	CUT FROM LIST - Parent			Yes				X		X	X		X					

Locle	10/01/08	http://www.locle.com	Pull	Closed	No	No	No	--	No	X		X								
Loki	04/09/07	http://www.loki.com	Pull	API	No	Yes	Yes	Yes	No		X									
Loopt	11/16/06	http://www.loopt.com	Pull	Closed	Yes	Yes	Yes	Yes	No	X		X				X				
Map My Tracks	12/23/07	http://www.mapmytracks.com	Push	Open	No	Yes	Yes	No	No									X		
MapMe	07/01/08	http://www.mapme.com	Push	Open	No	Yes	Yes	Yes	No			X			X	X				
Match2Blue	12/21/08	http://www.match2blue.com/cms/	Push	Open	No	Yes	Yes	Yes	No									X		
Meet Now Live	04/01/08	http://www.meetnowlive.com	Push	Open	No	Yes	Yes	Yes	No									X		
MeetMoi	11/25/08	http://www.meetmoi.com	Pull	Open	No	Yes	Yes	No	No				X							
Microsoft Vine	04/28/09	http://www.vine.net/default.aspx/	Push	Closed	Yes	Yes	Yes	Yes	No			X		X						
Mizoon	10/02/08	http://www.mizoon.com/	Push	Open	No	No	No	--	No									X		
Mobilaris	11/01/03	http://www.mobilaris.com	CUT FROM LIST - Parent			No									X					
Mobiluck	09/01/07	http://www.mobiluck.com	Pull	Open	Yes	Yes	NO	--	Yes	X		X			X					
Mologogo	10/01/07	http://www.mologogo.com	Pull	Open	No	Yes	Yes	Yes	No						X					
Moximity	09/26/08	http://www.moximity.com	KILLED NOVEMBER 2009			Yes						X								
MyGeoDiary	09/17/08	http://www.mygeodiary.com	Push	Open	No	Yes	Yes	Yes	Yes						X					
MyGeolog	12/10/08	http://www.mygeolog.com/	Push	Open	No	No	No	--	Yes						X	X				
Myrimis	09/04/07	http://www.Myrimis.com	Pull	Closed	No	Yes	Yes	No	Yes			X								
Now Here	03/22/08	http://www.nowhere.de/	Push	Closed	No	No	No	--	No			X								
Nulaz	04/10/08	http://www.nulaz.net/	Pull	Open	No	Yes	Yes	No	No			X			X					
Plazes	08/16/04	http://www.Plazes.com	Push	Open	No	Yes	Yes	Yes	Yes			X				X				
Pocket Life	12/16/08	http://www.pocketlife.com	Pull	Closed	No	Yes	Yes	Yes	Yes			X		X	X					
Quiro	09/01/06	http://www.myqiro.de	Pull	Closed	No	Yes	Yes	Yes	No			X			X					
Rumble	12/13/07	http://www.Rumble.com	Push	Open	Yes (Web), No (Phone)	Yes	Yes	Yes	No			X			X					
Shizzow	03/05/09	http://www.shizzow.com	Push	Open	Yes	Yes	Yes	Yes	No	X					X					
Skobbler	09/28/08	http://beta.skobbler.de/	Pull	Open	No	Yes	Yes	Yes	No					X						
Skout	01/16/09	http://www.us.skout.com	Push	Open	No	Yes	Yes	Yes	No	X					X					
Sniff	04/01/08	https://www.sniffu.com/us/	Pull	Closed	No	Yes	Yes	Yes	Yes	X		X			X					
Snikkr	05/21/09	http://www2.snikkr.net/	Pull	Open	No	No	YES	Yes	Yes						X		X			
Socialllight	10/19/05	http://socialight.com/	Pull	Open	No	Yes	Yes	Yes	No			X								
Sparrow	02/12/09	http://clickontyler.com/sparrow/	Push	Open	No	No	No	--	No									X		
Spot Adventures	05/21/09	http://www.spotadventures.com	Push	Open	No	Yes	Yes	No	No						X					
SpotJots	01/29/08	http://www.spotjots.com/	Push	Open	No	No	No	--	No									X		
The Grid	12/30/07	http://www.thegrid.co.za/	Push	Closed	No	Yes	Yes	Yes	No			X								
TownKing	07/04/07	http://www.townqueens.com/	Push	Open	No	No	No	--	No									X		
Trackut	10/08/08	http://www.trackut.com	Pull	Closed	No	Yes	Yes	No	No			X								
Trapster	04/01/08	http://www.trapster.com	Push	N/A	NA	Yes	Yes	No	No										X	
Triplt	06/27/07	http://www.triplt.com/	Push	Closed	No	Yes	Yes	No	No			X								
Troovy	06/10/07	http://troovy.com/bc/vancouver/	Push	Open	No	No	No	--	No									X		
Twibble	03/17/08	http://www.twibble.de/	Push	Open	No	No	No	--	No									X		
Twinkle	04/01/08	http://tapulous.com/twinkle/	Push	Open	No	Yes	Yes	Yes	No									X		
Twittelator	07/11/08	http://www.stone.com/Twittelator/	Push	Open	No	No	No	--	No	X										
WeNear	07/01/08	http://www.wenear.com/	Pull	Closed	No	No	No	--	No	X		X			X					
Whereis Everyone	07/03/08	http://everyone.whereis.com/	Pull	Closed	No	Yes	Yes	No	Yes	X		X	X		X					
WhereYou GonnaBe	04/18/08	http://www.wherevougonnabe.com	Pull	Closed	No	No	No	--	No			X								
Whrrl	10/23/07	http://whrrl.com/	Push	Open	No	Yes	Yes	Yes	No					X						
Zhiing	10/18/08	http://zhiing.com/	Push	Closed	No	Yes	Yes	Yes	No			X								

* Application also has time and location-based access restrictions

- **Creation Date** While many of the current location-based services have [illegible] relaunched, rebranded, or generally attempted to "reboot" their service, we have tried to find the most accurate date of a first public, or widespread beta launch for each of the services. Many of these dates are based on news articles, press releases, and blogs that announced the opening of the service.
- **Push/Pull** Most services use one of two approaches to location sharing, either users post their location at times they feel comfortable "checking in" to a specific place (push) or have their location stored, ideally near real-time, so that it can be requested by friends (pull). Most pull systems allow users to push their location, especially if their phone or settings prohibit automatic updating.
- **System** Most services also use one of two system models. Closed systems require users to be "friends" with each other, while an open model allows users to be requested by anyone in the system. This is separate, though not unrelated, to public sharing.
- **Accessible privacy settings** We noted whether or not the main interface allowed users to prominently see and access their privacy controls. For example, an application where one of the main tabs is labeled "Privacy" would fall under this category. An application that requires users to visit several pages or menus (e.g. Profile/Account/Settings/Privacy) does not.
- **Privacy Policy** We checked to see whether or not the website detailed their information practices (detailed in a privacy policy or included in a legal statement or terms of service). We checked this information both in August 2009, and February 2010.
- **Policy mentions location** We checked to see if the privacy policies explicitly mention location information, geographic data, etc.
- **Home page mention** We also check to see if the product/application homepages made any mention to privacy, security, user control, or something that would give users a sense of control over their information. Privacy policy links did not count.
- **Blacklist** Users are able to block specific individuals from viewing their location.
- **Per-request (explicit) permissions** Users must specifically review each location request, and decide whether or allow or deny the request prior to the location being revealed.
- **Friends Only** This whitelist-based control restricts acc[illegible] to users denoted as a "Friend." By default, closed systems are [illegible]sidered friends only.
- **Granularity** This advanced control allows users to instruct the system to provide a less detailed location to the person requesting information (e.g. "Andrew is in Pittsburgh, Pennsylvania.")
- **Group** This restriction allows users to define access based on groupings of users. (e.g. Allow everyone in the "college friends" group to view my location.)
- **Invisible** This feature may also be termed the "Private," "Only me," or "No one" setting. Users continue to send location data, but their locations are not divulged.
- **Network** This restriction allows the user to select existing communities to whom their location may be revealed. For example, user may join a geographical network or an interest-based community with whom they wish to share their location.
- **Time-expiring approval**: Several systems allow users to set a specific time frame (e.g. 1 hour) during which a link to the map of their location is "live." During this time frame, the recipient of the location message may view the map. After the expiration of this time, the link will no longer be accessible.
- **No restrictions**: Anyone is able to view the user's location.
- **Not Applicable** Privacy controls do not apply.
- **Unknown** We were unable to find information about the privacy controls.

- **Time-based rules** (not shown) Users may define durations of time and days of the week during which their location may be revealed (e.g. from 10 am to 3 pm).
- **Location-based rules** (not shown)This restriction allows users to define locations in which their location-information may be revealed. For example, users may tag a location as "Work" or select an area on a map, and their location information is revealed to anyone who requests them when they are at that location.

References

1. Best practices and guidelines for location-based services. *CTIA Wireless Association* (April 2 2008). http://www.ctia.org/business_resources/wic/index.cfm/AID/11300.
2. Mobile marketing revenue to hit $24 billion in 2013. *ABI Research* (January 14 2008). http://www.abiresearch.com/abiprdisplay.jsp?pressid=1037.
3. Wireless quick facts. *CTIA Wireless Association* (2008). http://www.ctia.org/media/industry_info/index.cfm/AID/10323.
4. ANTHONY, D., KOTZ, D., AND HENDERSON, T. Privacy in location-aware computing environments. *IEEE Pervasive Computing 6*, 4 (2007), 64–72.
5. BARKHUUS, L., BROWN, B., BELL, M., HALL, M., SHERWOOD, S., AND CHALMERS, M. From awareness to repartee: Sharing location within social groups. In *CHI '08* (April 2008), pp. 497–506.
6. BARKHUUS, L., AND DEY, A. Location-based services for mobile telephony: a study of users' privacy concerns. In *INTERACT'03* (2003), pp. 702–712.
7. BENISCH, M., KELLEY, P., SADEH, N., SANDHOLM, T., CRANOR, L., HANKES-DRIELSMA, P., AND TSAI, J. The impact of expressiveness on the effectiveness of privacy mechanisms for location sharing. Tech. Rep. CMU-ISR-08-141, Carnegie Mellon University, December 2008. http://reports-archive.adm.cs.cmu.edu/anon/isr2008/CMU-ISR-08-141.pdf.
8. BLAIS, A.-R., AND WEBER, E. A domain-specific risk-taking (dospert) scale for aduct populations. *Judgement and Decision Making 1* (2006), 44–37.
9. BROWN, B., TAYLOR, A., IZADI, S., SELLEN, A., KAYE, J., AND EARDLEY, R. Location family values: A field trial of the whereabouts clock. In *Ubiquitous Computing (Ubicomp '07)* (2007), Springer-Verlag, pp. 354–371.
10. CONSOLVO, S., SMITH, I., MATTHEWS, T., LAMARCA, A., TABERT, J., AND POWLEDGE, P. Location disclosure to social relations: Why, when, & what people want to share. In *CHI '05* (2005).
11. CORVIDA. What's plaguing your mobile social network? *ReadWriteWeb* (May 15 2008). http://www.readwriteweb.com/archives/whats_plaguing_your_mobile_soc.php.
12. FISCHHOFF, B. Acceptable risk: A conceptual proposal. *Risk: Health, Safety & Environment 1* (1994), 1–28.
13. FROMMER, D. Loopt location to update in the background on iPhone. *Business Insider* (September 4 2009). http://www.businessinsider.com/loopt-to-run-in-the-background-on-iphone-2009-6.
14. HOLSON, L. Privacy lost: These phones can find you. *New York Times* (October 23 2007). http://www.nytimes.com/2007/10/23/technology/23mobile.html.
15. HSIEH, G., TANG, K., LOW, W., AND HONG, J. Field deployment of IMbuddy : A study of privacy control and feedback mechanisms for contextual IM. In *Ubiquitous Computing (Ubicomp '07)* (2007), pp. 91–108.
16. IACHELLO, G., SMITH, I., CONSOLVO, S., ABOWD, G., HUGHES, J., HOWARD, J., POTTER, F., SCOTT, J., SOHN, T., HIGHTOWER, J., AND LAMARCA, A. Control, deception, and communication: Evaluating the deployment of a location-enhanced messaging service. In *UbiComp 2005* (2005), Springer-Verlag, pp. 213 – 231.
17. JUNGLAS, I., AND WATSON, R. Location-based services. *Communications of The ACM 51*, 3 (March 2008), 65–69.
18. KELLEY, P. G., HANKES DRIELSMA, P., SADEH, N., AND CRANOR, L. F. User-controllable learning of security and privacy policies. In *AISec '08: Proceedings of the 1st ACM workshop on Workshop on AISec* (2008), ACM, pp. 11–18.
19. KHALIL, A., AND CONNELLY, K. Context-aware telephony: Privacy preferences and sharing patterns. In *CSCW '06* (2006).
20. KIM, M., FIELDING, J. J., AND KOTZ, D. *Risks of Using AP Locations Discovered Through War Driving*. Springer Berlin / Heidelberg, 2006, pp. 67 – 82.
21. LEDERER, S., MANKOFF, J., AND DEY, A. K. Who wants to know what when? privacy preference determinants in ubiquitous computing. In *CHI '03* (2003), no. 724-725.
22. MALHORTA, N., KIM, S., AND AGARWAL, J. Internet users' information privacy concerns (iuipc): The construct, the scale, and a causal model. *Information Systems Research 15*, 4 (2004), 336–355.
23. MCCARTHY, C. The mobile social: Not ready for prime time? *News.com* (February 13 2008). http://www.news.com/8301-13577_3-9870611-36.html.
24. PATIL, S., AND LAI, J. Who gets to know what when: Configuring privacy permissions in an awareness application. In *CHI '05* (2005), pp. 101 – 110.
25. RAVICHANDRAN, R., BENISCH, M., KELLEY, P. G., AND SADEH, N. M. Capturing social networking privacy preferences: Can default policies help alleviate tradeoffs between expressiveness and user burden? In *Proceedings of 2009 Workshop on Privacy Enhancing Technologies* (August 2009).
26. ROBERTS, P., AND CHALLINOR, S. IP address management. *BT Technology Journal 18*, 3 (July 2000), 127–136.
27. SADEH, N. *M-Commerce: Technologies, Services, and Business Model*, 1st ed. Wiley, 2002.
28. SADEH, N., HONG, J., CRANOR, L., FETTE, I., KELLEY, P., PRABAKER, M., AND RAO, J. Understanding and capturing people's privacy policies in a mobile social networking application. *Personal and Ubiquitous Computing* (Forthcoming 2008).

29. SMITH, I., CONSOLVO, S., LAMARCA, A., HIGHTOWER, J., SCOTT, J., SOHN, T., HUGHES, J., IACHELLO, G., AND ABOWD, G. Social disclosure of place: From location technology to communication practices. In *Pervasive '05* (2005), Springer-Verlag, pp. 134 – 151.
30. TSAI, J. Y., KELLEY, P., DRIELSMA, P., CRANOR, L. F., HONG, J., AND SADEH, N. Who's viewed you?: the impact of feedback in a mobile location-sharing application. In *CHI '09: Proceedings of the 27th international conference on Human factors in computing systems* (New York, NY, USA, 2009), ACM, pp. 2003–2012.

Mr. RUSH. Thank you very much.

The Chair now recognizes Mr. King for 5 minutes for the purposes of an opening statement.

TESTIMONY OF JERRY KING

Mr. KING. Thank you, Mr. Chairman and members of the joint committee for inviting uLocate here today to discuss the use of location information in commercial software applications. What I hope to accomplish this morning is to provide you with an example of how such information can be used to benefit the consumer in the form of a mobile location search application within a privacy-sensitive business model.

To start, please allow me to tell you a little bit about uLocate's mobile application WHERE and how we use location. We launched WHERE in 2007 and have since become a top provider of mobile local search content that informs, entertains and helps consumers save time and money. WHERE's popularity is demonstrated by millions of downloads on top phones such as the Android and iPhone and BlackBerry and feature phones on most North American carriers including AT&T, Sprint and T–Mobile.

Local content available through WHERE includes everything from the weather, news, traffic, coffee shops with WiFi, you name it, plus we have integrated a variety of Yellow Pages search providers to further expand the information available at the consumer's fingertips. WHERE also helps people reach their destinations with easy-to-use maps and directions.

In addition to providing local content and search services, WHERE enables brands and advertisers to reach a local audience through contextually and demographically targeted ads. Interestingly, as we move from displaying non-location-based banner ads last year to more targeted advertising, we began to receive positive feedback from our users. As opposed to expressing frustration with generic or irrelevant banner ads, our users commented that our new style ads were positive additions to their experience. In other words, ads and offers for local businesses that make sense within the consumer's experience turn out to be viewed as value-added content.

We also noticed that such ads generated more revenue for uLocate. For example, by using location, time of day and other factors, we know that an ad for a local service station inside of a traffic widget has a higher click-through rate. Similarly, ads for local pizza shops at lunchtime perform very well.

Next, I will provide you some details about how WHERE collects location information. WHERE employs several location technologies such as GPS, WiFi and network-based location to determine the consumer's whereabouts. When a consumer starts WHERE for the first time, they are informed that WHERE will attempt to get their location. Consumers that are concerned about this can also choose not to allow WHERE to get location automatically. Consumers within WHERE always have the option to manually set their location either to their actual position on the planet or someplace else at any time for any reason.

WHERE users can also control location accuracy. For example, if the user chooses to update their location within WHERE, they are

presented with a list of options ranging from zip code to GPS fix. For many search activities, zip code is more than sufficient while a street address may provide a more optimized experience for other functions. Once the location of the consumer's handset is updated, we cache that new location on the consumer's handset. When location is sent from a handset to our backend service as part of a service request as in a search, the location data is encrypted.

Having processes and policies that address collection and storage of location information is important but is only part of our approach to protecting consumer privacy. I would also like to address the issue of sharing location information, unlike some location-based services in market where it does not allow anyone to pull or monitor or track the location of anyone else. We also do not allow the automatic posting of locations that allow others to track a WHERE user's location. Lastly, we do not share personally identifiable location information of WHERE users with any third parties. Having a well-defined and trusted application with respect to these three behaviors has been a cornerstone of our approach to protecting consumer privacy within WHERE.

WHERE does allow users to publish or push their location to others within certain user-controlled functions such as reviews or check-ins. This is done to provide the consumer with the ability to generate location-specific content such as a restaurant review and post that content on a variety of social networks such as Facebook.

I hope this statement has provided you with some insights into what we consider a well-behaved location-based application. In sum, we use location to deliver beneficial consumer experience and we put the consumer in control of both managing their location information and sharing it with others.

Thank you for the opportunity to speak with you today. I look forward to your questions.

[The prepared statement of Mr. King follows:]

STATEMENT OF JERRY KING
CHIEF OPERATING OFFICER, ULOCATE COMMUNICATIONS INC.

BEFORE THE
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY & THE INTERNET
COMMITTEE ON ENERGY & COMMERCE
UNITED STATES HOUSE OF REPRESENTATIVES

HEARING ON THE COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES

FEBRUARY 24, 2010

Thank you Mr. Chairman and Members of the Subcommittee for inviting uLocate Communications Inc. here to discuss the use of location information in commercial software applications. What I hope to accomplish this morning is to provide you with an example of how such information can benefit the consumer in the form of a mobile local search application within a privacy sensitive business model.

To start, please allow me to tell you about uLocate's mobile application – WHERE® - and how we use location. We launched WHERE in 2007 and have since become a top provider of mobile local search content that informs, entertains, and helps consumers save time and money. WHERE aggregates best-of breed content from multiple sources to create a top-tier local search experience that includes real-time user generated recommendations and targeted advertising and offers based on the consumer's preferences.

WHERE's popularity is demonstrated by millions of downloads and top ratings on 'smart phones' such as iPhone, Android, Blackberry, and Palm Pre, and on feature phones from wireless carriers such as AT&T, Sprint, and T-Mobile.

Local content available through WHERE includes everything from the weather, news, restaurant reviews, directions to the closest coffee shop with WiFi, cheap gas, traffic updates, movie show times, and more. Plus, we have integrated a variety of 'yellow pages' search providers to further expand the information available at the consumer's fingertips. WHERE also helps people reach their destinations with easy to use maps and directions.

In addition to providing local content and search services, WHERE enables brands and advertisers to reach a local audience. We currently serve advertisements on mobile devices across all of the major US wireless carriers. Once the consumer establishes their location within WHERE, we are able to deliver both contextually and demographically targeted campaigns.

Interestingly, as we moved from displaying non-location based banner ads to more targeted advertising last year, we began to receive positive feedback from our users. As opposed to expressing frustration with generic or irrelevant ads, our users commented that our new style of location or service related ads were positive additions to their experience. In other words, ads and offers for local businesses that make sense within the consumer's experience turn out to be viewed as value-added content.

We also noticed that such ads generated more revenue for uLocate. For example, by using location, time-of-day, application context, and other factors, we know that an ad for a local service station inside of the Traffic widget will have a higher clickthrough rate, as will ads for local pizza shops at lunchtime.

Next, I will provide you with some details about how WHERE collects location information.

The first thing that I would like to point out is that the CTIA *Best Practices and Guidelines for Location Based Services* are an excellent source of information for how location can be used in a responsible and consumer-focused way. Given our close relationship with the wireless carriers, adherence to these guidelines has always been central to the services we offer – and, we believe, to our success in the market.

In order to deliver location-based services, WHERE employs several location technologies such as GPS, WiFi, and network-based location to determine the consumer's whereabouts. When a consumer starts WHERE for the first time they are informed that WHERE is a location-based application and will attempt to get their location automatically. Consumers that are concerned about privacy can choose not to allow WHERE to get location in the background. Choosing this option requires users to explicitly approve location acquisition every time they launch WHERE.

Consumers can also manually set their location – either to their actual position on the planet or some other place – depending on their preference and at any point in time.

Furthermore, WHERE users can control location accuracy. For example, if the user chooses to update their location with WHERE, they are presented with a list of options ranging from zip code to actual GPS fix. For many search activities, zip code is often sufficient (e.g., Movie theaters), while a street address may provide a more optimized experience for other functions (e.g., restaurant reviews).

Once the location of the consumer's handset is updated (either automatically or manually), we cache the new location locally on the consumer's handset. When

location is sent from the handset to our back-end servers as part of a service request, the location data is encrypted.

We do log service requests (e.g., a search for nearby coffee shops) in our database under a randomly generated ID along with the encrypted location data. The data in these logs is then aggregated and only the aggregate data is used for downstream analytical functions. These logs are purged periodically and are never used to track or share personally identifiable information or behaviors.

Having processes and policies that address the collection and storage of location information is only part of our approach, however. I would like to also address the issue of sharing location information.

Unlike some location-based services in market, WHERE does not allow anyone to 'pull' or monitor the location of anyone else. We also do not allow automatic posting of locations that might allow others to track a WHERE user's location. Lastly, we do not share personally identifiable location information of WHERE users with any third parties. Having a well-defined and trusted application with respect to these three behaviors has been a cornerstone of our approach to protecting consumer privacy.

WHERE does allow users to publish or 'push' their location to others within certain user controlled functions such as reviews and 'check ins'. This is done to provide the consumer with the ability to generate location-specific content (e.g. restaurant reviews) and post that content on a variety of social networks (e.g., Facebook) and forums (e.g., WHERE Reviews).

I hope this statement has provided you with some insights into what we consider to be a 'well-behaved' mobile location-based application operating in today's market.

In sum, we use location to deliver a beneficial experience to the consumer and we put the consumer in control of both managing their location information and sharing it with others.

Thank you for the opportunity to speak with you today. I would be pleased to answer any questions you may have.

Mr. RUSH. The Chair now recognizes Mr. Bernard for 5 minutes.

TESTIMONY OF TONY BERNARD

Mr. BERNARD. Thank you. On behalf of Useful Networks and the location industry, thank you to your respective committees for their time and my fellow witnesses for their time in this important topic.

I am Tony Bernard, vice president and general manager of Useful Networks. Useful Networks is a Denver-based company that delivers innovative local location-based services to consumers, wireless carriers, application developers and mobile marketers. We were founded in July of 2006 and are focused on location aggregation and enablement, providing a location clearinghouse and related services with our PlaceWhere platform. Useful Networks is a wholly owned subsidiary of TruePosition, the global leader in location determination and intelligence solutions that help protect citizens, combat crime and save lives.

A location aggregator provides its third-party partners with location connectivity to a variety of sources including wireless carrier infrastructure. Aggregators may also offer privacy management like Useful Networks does to complement the location connectivity we provide. To the gentleman's points earlier, this platform is both forward looking and adaptable in that it offers a multi-tiered privacy framework to enable compliance with the current and future requirements for access to and use of an end-user's location information. PlaceWhere ensures compliance with privacy best practices as manifested by a variety of stakeholders including industry and government entities, wireless carriers and most importantly, consumers.

My focus today is to talk about location-based advertising. A few of the players in the location-based advertising value chain include publishers, which own and manage content portals via which audience is aggregated and into which mobile advertisements be published. An example of the type of application publisher would be uLocate and their WHERE application. We also work with ad networks who aggregate publisher inventory and sell ad campaigns. Examples of those would include Quatro and Millennial Media. We work with ad exchanges who aggregate ad networks for publishers, enabling them to serve the most profitable ads from the available networks.

Additionally, ad agencies play a role in location-based advertising. They buy advertising from ad networks, assign creative campaigns and sell their brands. Examples of these would include traditional ones such like Saatchi and Saatchi as well as emerging digital agencies like Razorfish. And finally, there are location enablers like Useful Networks who endeavor to establish rules by which others can engage in location-based advertising and ensure they are complied with.

So it is important to talk briefly about the state of location-based advertising in the United States. The CTIA published a set of best practices and guidelines for use of location services in 2008 fundamentally predicated on the two principles of user notice and informed consent. Specifically, the ability to use a consumer's location to provide a location-enhanced advertisement is fundamentally predicated upon an explicit opt-in where such consent is provided

by the consumer on an informed basis with respect to if, how, when and by whom their location information may be used. Consumers may subsequently opt out of their location being used for such purposes.

Whereas wireless carriers tend to rigidly enforce these principles, to the earlier points raised, the emerging devices carrier category, examples of which would include the iPhone and Nexus One devices, do not yet fall under the auspices of these guidelines, and what we see now is what could be perceived as a regulatory gap where consumers can have very different expectations and experiences with the same application if that application is on a carrier device versus a non-carrier-controlled device. I look forward to talking more about that topic.

Another significant evolution in location-based advertising is the emergence of the check-in model. The emerging check-in model is enabling the transition from passive to active location sharing. Where passive is typically location tracked by the network, active is the consumer making a choice to share that location information. Examples of these include applications like BrightKite, Foursquare, Gawala, and MyTown. It is anticipated that these check-in capabilities will become an even more ubiquitous feature across a wide variety of location-based applications and services in the near future and it will be important to understand implications to these.

Another component of the state of location-based advertising is how location context is enabling a transition by advertisers from paying for impression-based campaigns to performance-based campaigns. Mobile devices in general and location-aware devices specifically add significant context for advertisers. This context is unavailable via traditional advertising channels such as print and online advertising. Combining this context with mobility creates new opportunities for advertisers to improve the efficiency of their advertising spend by focusing on conversion.

A few examples of location-based advertising. Useful Networks, launched a trial in 2009 working with a tier one U.S. carrier and an advertising network which in turn worked with a major fast-food chain and a major automotive company to launch two location-based advertising trials which were centered around a store finder page and were designed to test and prove the added benefits that location enablement brings to mobile marketing campaigns. These trials resulted in a yield of three times as many store finder page views as compared to the number of page views when the end-user was asked to enter their zip code.

Another trial we are preparing to commence is with a company called Mobox. Mobox is a location-based mobile ad platform that serves ads into mobile content, reaching over 30 million unique U.S. mobile users. Useful Networks is providing location connectivity and privacy management to enable location targeting via Mobox's platform.

Again, I would like to thank their committees for their interest and attention to this important topic and look forward to talking about these issues in more earnest during the future testimony. Thank you.

[The prepared statement of Mr. Bernard follows:]

House of Representatives
Committee on Energy and Commerce

Joint Hearing, Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the Internet

"The Collection and Use of Location Information for Commercial Purposes"
Location-Based Advertising Testimony

Presented by:
Tony Bernard
Vice President and General Manager
Useful Networks, Inc.
February 24, 2010

Useful Networks Overview

1.1. Company Description

Useful Networks (www.useful-networks.com) is a Denver-based company that delivers innovative mobile location technology products to end-users, mobile operators, application developers and mobile marketers. Founded in July 2006, Useful Networks has consistently provided technologies that bring value to location. The company's three core goals are to create the most compelling location-aware applications for web and mobile; to offer brands and agencies a completely new way to connect with consumers; and to act as a location clearinghouse for content providers with our PlaceWhere™ Platform.

Useful Networks is a wholly owned subsidiary of TruePosition (www.trueposition.com). TruePosition is the global leader in location determination and intelligence solutions that help protect citizens, combat crime, and save lives. TruePosition location solutions meet the mission-critical requirements of enterprises and government agencies. These solutions include future-proof technologies, innovative applications, and comprehensive networking and systems services. TruePosition has more patents, technical expertise, and operational experience in wireless location than any other company in the world. Every day more than 100 million people depend on location services supported by TruePosition technology. TruePosition is a wholly owned subsidiary of Liberty Media Corporation attributed to the Liberty Capital group (Nasdaq: LCAPA), which owns a broad range of electronic retailing, media, communications and entertainment businesses. For more information, visit www.trueposition.com or www.libertymedia.com.

1.2. Location Aggregator Model

A location aggregator provides its third-party partners (e.g., application developers, mobile marketers) with location connectivity to a variety of location sources, including wireless carrier location infrastructure. Location sources include (but are not limited to) on-device GPS (with or without carrier assist data), carrier network-based location, on-device Bluetooth and WiFi-based positioning.

In order to derive an end-user's location from any source, the end-user must be presented with notice of how, when and by whom location will be used, such that an informed consent by the end-user may be provided (and may subsequently be revoked) at any time. Therefore, location aggregators may seek to additionally provide policy & privacy management capabilities to ensure the aggregator's third-party partners' compliance with privacy best practices as manifested by a variety of stakeholders. Key stakeholders include (but are not limited to) industry and/or government entities (e.g., CTIA, FTC, FCC, MMA), wireless carriers and end-users.

1.3. PlaceWhere

1.3.1. Location connectivity

The PlaceWhere platform enables third-party application developers to access a variety of location sources via a single API – in the near term, primarily wireless carrier-based sources. In addition to carrier-based location sources, the API also supports emerging sources such as WiFi- and Bluetooth-based location, providing 3rd party application developers with a range of options with respect to which location type(s) are best suited to their application.

The various location sources can provide a very different "yield," or precision of location fix, based on a variety of conditions. For example, on-device GPS can provide relatively high location granularity, whereas Cell ID tends to provide less-precise location. The yield of the respective sources in turn aligns with the performance requirements of various commercial applications. While less-precise Cell ID-based locations may suffice for a location-aware mobile marketing campaign, more-precise assisted GPS (where "assist" data is provided by the carrier network) is typically required by location-based social networking applications.

1.3.2. Multi-tiered privacy framework

The multi-tiered privacy framework in PlaceWhere is designed with the disparate yet complementary needs of the various stakeholders in mind. Specifically, the framework is based on the following successive stakeholder tiers.

1.3.2.1. Regulatory

The regulatory tier embodies the various laws, rules, regulations and best practices as they relate to access to and use of the end-user's location. Examples include the CTIA LBS Best Practices and Guidelines, and the Children's Online Privacy Protection Act (COPPA).

1.3.2.2. Wireless carrier/Device-as-carrier

Each wireless carrier can have its own unique requirements under which they will allow access to and use of its customers' location information. These requirements are similar in many regards, but may also differ in material ways, such that a cross-carrier policy framework is desirable to third-party application developers in order to simplify the development process while ensuring compliance with carrier-specific requirements.

Emerging "device-as-carrier" platforms (e.g., iPhone, Nexus One) are increasingly playing a role similar to that which has traditionally been the domain of wireless carriers, in that the device manufacturers are in some cases establishing and enforcing their own "rules of engagement" for accessing end-users' location information on their devices. For example, Apple recently began limiting the ability of iPhone application developers to access end-user location data for advertising purposes.

1.3.2.3. End-user

The controls provided to the end-user are tailored to the specific type of application and its associated "risk profile" with respect to usage of location information. Such end-user controls consistently manifest the key principals of informed consent, explicit (vs. default) opt-in and permission revocation, regardless of the application's underlying risk profile. Examples of risk profiles include (but are not limited to):

- Peer-to-peer locate (Enterprise/Account holder control)
- Peer-to-peer locate (End-user control)
- Self-locate (news/info, games)
- Self-locate (search/advertising/marketing)

1.3.3. Location-based advertising capabilities

1.3.3.1. Content localization

Tailor mobile web content (e.g., news & weather) based on the end-user's location. More relevant information improves the user experience.

1.3.3.2. Ad geo-targeting

Use the end-user's location to improve the relevance of an advertisement or offer. For example, a local business owner could purchase advertising inventory targeting only end-users in his geographic region, thereby enhancing the campaign's effectiveness by ensuring the local owner only pays for impressions/clicks from local, potential customers.

1.3.3.3. Store locator

Use the end-user's location to provide guidance to nearby store/franchise locations. For example, a national auto brand can use location to provide a list of the dealer locations closest to the end-user.

1.3.3.4. Proximity alert

Proximity-based marketing programs have traditionally been limited by the cost and utility of location technology. For example, a marketer may desire to continuously "poll" the locations of opted-in members of its loyalty program for the purpose of sending offers when an opted-in member is within 100 yards of a store location. This use case could be prohibitively expensive due to the "per-dip" nature of location expenses.

The emerging "check-in" model is enabling the transition from passive (i.e., the network tracks opted-in subscribers) to active (i.e., the end-user "checks in" when arriving at a location and is provided an incentive to do so). Examples of check-in applications via which proximity-based marketing is taking place include BrightKite, Foursquare, Gowalla and MyTown. It is anticipated that "check-in" capabilities will emerge as a ubiquitous feature set across a variety of location-based applications and services, given the aforementioned location cost & utility constraints.

2. LBA Value Chain
   2.1. Publishers

   Own and manage content portals via which audience is aggregated and into which mobile advertisements can be published. Work with various stakeholders to maximize revenue & profits by optimizing fill rates. Examples: CNN, Where (uLocate)

   2.2. Ad Networks

   Aggregate publisher inventory (available ad space and impressions) and sells ad campaigns. Examples: AdMob, Quattro Wireless, Millennial Media

   2.3. Ad Servers

   Software-based platform; enable campaign management, ad selection and ad serving capabilities. Examples: MADS, OpenX

   2.4. Ad Exchanges

   Aggregate Ad Networks for publishers, enabling them to serve the most profitable ads from the available networks. Example: AdWhirl

   2.5. Ad Agencies

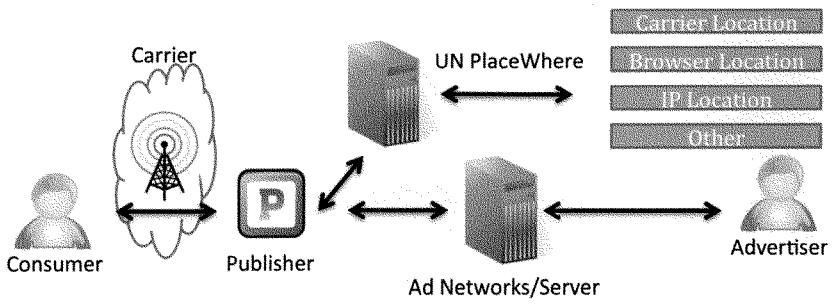
   Buy advertising from Ad Networks, designs creative campaigns and sells to brands. Example: Saatchi, Hyperfactory

   2.6. Location Enablers

   Provide location data from a variety of sources, making it available to publisher content targeting and ad selection processes. Example: Useful Networks

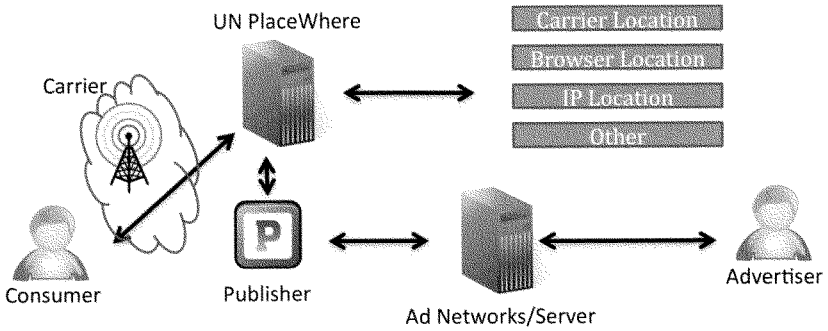
   2.7. Ecosystem Examples
      2.7.1. Publisher initiates location request

      Publishers request location from PlaceWhere prior to receiving a request for content from the Consumer. Publishers could also use this location to request and serve targeted ads.



2.7.2. Consumer request proxied through PlaceWhere

Consumer requests are proxied thru PlaceWhere, and the request is location-enabled before it gets to the Publisher. The Publisher may then use location to make an ad request.



3. State of LBA

3.1. Opting In, Opting Out

The ability to use the end-user's location for the purpose of providing a location-enhanced advertisement is fundamentally predicated upon an explicit opt-in, where such consent is provided by the end-user on an informed basis with respect to if, how and when and by whom their location may be used. Correspondingly, end-users may subsequently opt-out of their location being used for such purposes. It is worth noting that current online-based advertisements leverage coarse, IP-based location to localize display ads without requiring an opt-in from the end-user.

3.2. Passive vs. Active Location & Impact of Check-In Model

The emerging "check-in" model is enabling the transition from passive (i.e., the network tracks opted-in subscribers) to active (i.e., the end-user "checks in" when arriving at a location and is provided an incentive to do so). Examples of check-in applications via which proximity-based marketing is taking place include BrightKite, Foursquare, Gowalla and MyTown. It is anticipated that "check-in" capabilities will emerge as a ubiquitous feature set across a variety of location-based applications and services, given the aforementioned location cost & utility constraints.

3.3. Location Context: Enabling the Transition from Impressions to Performance

Mobile devices in general – and location-aware devices specifically – add significant context for advertisers. Such precise context has been largely unavailable via traditional advertising channels such as print and online. Combining context with mobility creates new opportunities for advertisers to improve the efficiency of their advertising spend by focusing on conversion.

3.4. "The Last Mile": Conversion Beyond the Click

The addition of context via location – coupled with the dynamic nature of mobile advertising technologies – creates an environment in which advertisers are increasingly willing to pay premiums for performance-based campaigns (e.g., cost-per-click, click-to-call, offer redemption) with proven ROIs, and are less willing to pay for traditional impression-based campaigns (e.g., cost-per-thousand impressions, or CPM) with uncertain ROI with respect to conversion. As consumers engage with campaigns via their mobile devices, the opportunity to further "prove" ROI via offer redemption (e.g., the consumer clicks on a banner ad, receives a coupon code and redeems the offer by entering the coupon code at the merchant's point-of-sale terminal) will in turn improve, thereby solving "the last mile" issue of proving an advertisement led to the desired action by the consumer. An example of a performance-based campaign is a national auto franchise which uses location to optimize an ad, leading to (a) a click by the end-user (advertiser pays based on CPC) and (b) redemption of an offer (e.g., $10 iTunes gift card for scheduling a test drive).

4. Case Studies & Examples
   4.1. Storefinder Trial – Quick Serve Burger franchise & National Auto Dealer
      4.1.1. Executive Summary

UN worked with a major U.S. Carrier (which will be referred to as "the carrier") and a major advertising network (which will be referred to as "the ad network"), who in turn worked with a major fast food restaurant chain (Trial #1) and a major automotive company (Trial #2), to launch two location-based advertising trials in the United States. The LBA Trials were centered around a Store Finder page and were designed to test and prove the added benefits that location-enablement brings to mobile marketing campaigns.

4.1.2. Trial Setup

Both trials created very similar end user experiences. The end user experience involved two call-to-action banner ads displayed on the carrier's mobile portal enticing the customer to find the two brands' store locations. Although both banner ads were virtually identical (except for the opt-in language featured on the location-enabled banner ad), each banner ad resulted in a different after-the-click experience.

- Control Group: 50% of the banner ad clicks directed the user to a manual zip code entry page.
- Trial Group: 50% of users saw a location-enabled banner ad that used the user's location to generate a Store Finder page without requiring the user to enter in their zip code.
- Trial Purpose: to test whether a location-enabled marketing campaign will result in a higher percentage of Store Finder page views (i.e., higher conversion rates).

4.1.3. Trial Results

- Brand #1 – Quick Service Restaurant Vertical: ~100% of those users who clicked on the location-enabled banner ad saw the fast food restaurant's Store Finder page. In contrast, only 28% of those users who were directed to the manual zip code entry page actually submitted their zip code and viewed the brand's Store Finder page. Stated differently, the non-location enabled banner ad resulted in a 72% abandonment rate.
- Brand #2 – Automotive Vertical: ~10% of those users who were directed to the manual zip code entry page actually submitted their zip code and viewed the automotive company's Store Finder page (compared to ~100% of those users who clicked on the location-enabled banner ad).

4.1.4. Trial Findings

The quick serve restaurant trial showed that a location-enabled solution yields 3 times as many Store Finder page views than does one requiring a manual zip code entry. The automotive company trial showed that the

location-enabled solution yields 10 times as many Store Finder page views. Therefore, it is reasonable to conclude that a location-enabled marketing campaign is, at a minimum, 3 times as valuable as a non-location enabled marketing campaign.

4.2. Upcoming LBA Trial – MoVoxx

4.2.1. Trial Overview

MoVoxx is a location-based mobile ad platform that intelligently serves ads into mobile content reaching over 30 million unique US mobile users. GeoSense™ platform combines real-time user location data within the ad serving process to enable national brands and local merchants the ability to launch location-based mobile advertising campaigns – at scale.

Useful Networks is providing location connectivity (to enhance Movoxx's existing data set) and privacy management (to ensure compliance with best practices). This new geo-targeting capability is expected to improve relevance of the mobile channel for small business and local merchant advertisers. To reach them, MoVoxx will aggregate local merchants' mobile campaigns, through partners such as Citysearch, Marchex and iPromote, as well as by working directly with larger brands interested in geo-targeting such as Sears.

Mr. RUSH. Thank you.

The gentleman, Mr. Altschul, is recognized for 5 minutes.

TESTIMONY OF MICHAEL ALTSCHUL

Mr. ALTSCHUL. On behalf of CTIA, I want to thank Chairman Rush and Chairman Boucher, all the members of the two subcommittees for the opportunity to testify here.

My name is Mike Altschul and I have served as CTIA's general counsel since 1990. In that role, on behalf of CTIA, I have been involved in the development of a number of voluntary industry best practices including CTIA's best practices and guidelines for location-based services that you have heard the other witnesses on the panel describe. I am very proud that CTIA and the wireless industry have long been at the forefront of efforts to promote location privacy. In the late 1990s, we supported the Wireless Communications and Public Safety Act, which amended section 222 of the Communications Act to require the express prior authorization of the customer for the disclosure of the wireless customer's location information for location-based services. That really has provided the foundation for everything that has followed since.

In fact, in 2000, following the enactment of the Wireless Communications and Public Safety Act, CTIA petitioned the FCC to adopt a set of fair location information practices for wireless location-based services modeled upon the familiar fair information practice principles of notice and consent. More recently, as location-based services began to be deployed for applications other than E911, CTIA developed the current set of best practices to promote and protect the privacy of wireless customers' location information. You have heard what they have done and you have also heard from the other witnesses that in the 2 years since we adopted and developed these best practices, as so often happens in the wireless industry, technology has overtaken our static assumption and the location-based services now being offered turn out to be quite different from what had been envisioned just 2 years ago. You have heard how the move towards opening platforms including the iPhone and the Google Android platform, the introduction and overwhelming consumer adoption of smartphones, which include their own GPS capabilities, and the increased prevalence of GPS-enabled service applications that can be downloaded to a handset and enabled without any involvement or knowledge by a wireless carrier have combined to make a carrier-centric approach to location-based services no longer sufficient for guidelines.

So these factors and the rapid developments of the past 2 years have led us to reevaluate our guidelines, and as we have completed work on the new guidelines, it is our goal to ensure there will always be one clearly identified location-based service provider with the obligation to inform the user as to how location information will be used and disclosed in addition to obtaining customers' consent before initiating the service.

While the scope of the new CTIA guidelines is different, the focus is not. The new guidelines will build on the foundation we laid 10 years ago by continuing to put a premium on user notice and user consent. We believe the guidelines offer a meaningful framework for the protection of user privacy and we urge policymakers to rec-

ognize that the industry's willingness to develop best practices and to revise these guidelines as circumstances warrant represents the best way to balance the needs to promote and protect user privacy while also facilitating the deployment of new and innovative products and services.

A call for legislative restraint does not mean there is no role for Congress while the industry and technology evolve. Congress also has made clear that the express prior authorization of the customer is the prerequisite for the disclosure of a wireless customer's location information. While section 222 on its terms applies only to telecommunications carriers, its requirements have been observed by all providers of wireless location-based services across all the different application levels. As these services continue to evolve and develop in both predictable and unpredictable ways, Congress has an important oversight role in ensuring that all providers of location-based services deliver effective notice and obtain consent regardless of the device or technology used so that wireless users can continue to exercise informed consent to control the use or disclosure of their location information.

As Mr. Morris mentioned, one area in which we believe legislative guidance may be appropriate is a clarification of the terms under which location information may be released to law enforcement. As you know, just this month in the 3rd Circuit, there was oral argument on the issue of what standards should apply when law enforcement seeks to gain access to a wireless user's location information. Most courts have allowed access to stored location records based on a court order and demonstrated need, but in the 3rd Circuit, the U.S. Department of Justice and privacy advocates argued whether access to these historical location records should meet a probable-cause standard. Service providers need clarity so as to not be caught in the middle of these disputes.

Finally, we urge Congress to recognize the interstate nature of location-based services, the mobile nature of wireless users and to take care in whatever framework may be adopted to preempt state regulation of these services. A uniform national approach presents the best way of protecting user privacy and educating and informing wireless customers while fostering the innovation, investment and introduction of new location-based services by wireless carriers, device manufacturers, operating system developers and application creators.

Thank you again for the opportunity to share our views with the subcommittees. We look forward to working with you as you continue your efforts on this issue.

[The prepared statement of Mr. Altschul follows:]

Testimony of Michael Altschul, Senior Vice President and General Counsel,
CTIA – The Wireless Association®
before the
House Energy and Commerce
Subcommittee on Communications, Technology, and the Internet, and
Subcommittee on Commerce, Trade, and Consumer Protection

February 24, 2010

On behalf of CTIA – The Wireless Association® ("CTIA"), I want to thank Chairman Boucher and Chairman Rush, ranking members Stearns and Radanovich, and members of the two subcommittees for the opportunity to appear at today's hearing to share the wireless industry's views on the proper regulatory framework for location-based services.

My name is Mike Altschul, and I have served as CTIA's General Counsel since 1990. In my capacity at CTIA, I have been involved in the development of CTIA's Best Practices and Guidelines for Location-Based Services ("Guidelines"). I have represented CTIA before the Federal Trade Commission and the FTC's activities related to privacy and location-based services, the most recent of which was the January 28, 2010 "Exploring Privacy" roundtable held at the University of California, Berkeley, School of Law. Additionally, I have been involved with CTIA's advocacy on these issues before the Federal Communications Commission.

CTIA has been at the forefront of location privacy while balancing the need for legitimate access to a customer's location information in emergencies and for law enforcement purposes from the inception -- beginning fifteen years ago when CTIA and Public Safety proposed a "Consensus Solution" to the Federal Communications Commission's wireless E-911 rulemaking proceeding. I am proud that CTIA has been a leader in regard to location privacy ever since. In the late 1990s, we supported *The Wireless Communications and Public Safety Act of 1999* (Public Law 106-81, 113 Stat. 1286-1290), which addressed some of the issues that arose from the FCC's E-911 rulemaking, including a provision that specifically authorized carriers to provide call location information concerning a user of a commercial mobile service to: (1) emergency dispatchers and emergency service personnel in order to respond to the user's call; (2) the

user's legal guardian or family member in an emergency situation that involves the risk of death or serious physical harm; or (3) providers of information or data base management services solely for assisting in the delivery of emergency services. Significantly, *The Wireless Communications and Public Safety Act* also amended Section 222 of the Communications Act to require "the express prior authorization of the customer" for the disclosure of the wireless customer's location information for any other purpose.

In 2000, CTIA petitioned the FCC to adopt a set of Fair Location Information Practices for wireless location-based services. CTIA's proposal was modeled on the familiar Fair Information Practice Principles. Although the FCC declined to adopt CTIA's proposal, the fundamental principles of customer "notice" and "consent" have been widely adopted and continue to provide the basis for the wireless industry's approach to location-based services.

Two years ago, as location-based services began to be developed and deployed for applications other than E-911, CTIA worked with its members and other interested parties to develop a set of industry "Best Practices and Guidelines" to promote and protect the privacy of wireless customers' location information. The 2008 Guidelines directed the entities that provide location based services to inform users about how their location information will be used, disclosed, or protected so that a user can make an informed decision about whether or not to use a particular location-based service or authorize disclosure of his or her location. Additionally, once a user has opted to use a location-based service, or authorized disclosure of his or her location, the 2008 Guidelines contemplate that the user should have choices as to when or whether location information would be disclosed to third parties, as well as providing that the user should have the ability to revoke such authorization at any time.

In crafting the 2008 Guidelines, we recognized, consistent with Section 222 of the Communications Act, and the FCC's rules governing Customer Proprietary Network Information ("CPNI"), that user privacy must be balanced with legitimate law

enforcement and emergency or other needs. Accordingly, the guidelines did 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 operation of any network or LBS; or
- in the form of aggregate or anonymous data.

Today, we are in the process of revising the 2008 Guidelines. Why are we revising the Guidelines so soon? Up until recently, there was a widely held assumption that location-based services would involve a wireless carrier having access to a user's location information and then using or sharing that information to provide a location-based service. That is what Congress contemplated when it enacted amendments to Section 222 of the Communications Act as part of the *Wireless Communications and Public Safety Enhancement Act of 1999*, and that is what we envisioned just two years ago as we worked with our members to craft what became the 2008 Guidelines.

As is often the case, things turned out a bit differently than had been envisioned, as the last two years have brought profound change to the wireless industry. The rapid evolution toward open platforms, the overwhelming consumer adoption of smart-phones, and the increased prevalence of GPS-enabled location-based service applications that can be downloaded to a handset and enabled without any involvement or knowledge by a wireless carrier[1] combined in a way that suggested that a carrier-centric approach to location-based service guidelines is no longer sufficient or even desirable. These factors led us to reevaluate the 2008 Guidelines, and as we complete work on the 2010 Guidelines, we envision that they will ensure that there is always one clearly identified location-based services provider with the obligation to inform the user as to how location information will be used and disclosed and to obtain the user's consent before initiating the service. Under the revised Guidelines, the user will always know who is responsible

[1] An overview of non-carrier provided location based services can be found at http://www.ftc.gov/os/comments/privacyroundtable/544506-00088.pdf.

for the careful handling of his or her location information. We will be working with our members and other interested parties to push for broad acceptance of the Guidelines. While the scope of the new Guidelines is different, the focus is not. The new Guidelines will build on the foundation we laid ten years ago by continuing to put a premium on user notice and consent.

With respect to notice, we envision that location-based service providers ought to 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 a particular service, giving the user ultimate control over their location information.

The Guidelines envision that location-based service providers will use written, electronic or oral notice that will ensure that users have an opportunity to be fully informed of the providers' information practices. Notice must be provided in plain, easily understood language, it must not be misleading, and if combined with other terms or conditions, the portion pertaining to the location-based service must be conspicuous.

If, after having obtained consent, a provider of location-based services wants to use location information for a new or materially different purpose not disclosed in the original notice, the provider must inform the user with further notice and obtain the user's consent to the new or other use.

The Guidelines also dictate that location-based service providers must inform users how long any location information will be retained, if at all. As a general matter, providers should retain user location information only as long as business needs require, after which such information should be destroyed or rendered unreadable.

Additionally, the Guidelines also direct location-based service providers to periodically remind users when their location information may be shared with others and of the users' location privacy options. The specific terminology, timing and frequency of such notice depends on the nature of the particular service. 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 a one-time, user-initiated concierge service call (e.g., a call requesting a nearby service).

Another significant change from the 2008 Guidelines is the clear requirement that every user be informed whenever a location-based service is installed and used on their device. In some circumstances, account holders (as opposed to users) may control the installation and operation of location-based services (e.g., business account holder utilizing a location service for fleet management or a parental account holder providing phones for use by a child or member of a "family plan"). In addition to providing notice to the account holder, location-based service providers must ensure that notice is provided to each user that location information is being used by or disclosed to the account holder or others. This now clearly stated requirement will reduce the risk of surreptitious or unauthorized tracking. While we do not believe this is required by Section 222 – which addresses the rights of the "customer" and not the rights of the "user," we believe it is the right approach to promoting and protecting user privacy.

In addition to providing significant guidance regarding the type of notice that users should expect, the Guidelines will continue to speak to the issue of consent.

CTIA's Guidelines contemplate that location-based service providers will obtain user consent to the use or disclosure of location information ***before*** initiating a location-based service. The form of consent may vary with the type of service or other circumstances, but location-based service providers bear the burden of establishing that consent to the use or disclosure of location information has been obtained before initiating service.

The Guidelines require that consent be informed and based on a notice consistent with the notice requirements set forth by the Guidelines. 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 a location-based service 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. The Guidelines expressly reject pre-checked boxes that cause a user to be automatically opted-in to location information disclosure or choice mechanisms that are buried within a lengthy privacy policy or a uniform licensing agreement. Such an approach would be insufficient to express user consent under the CTIA Guidelines.

Users should have confidence when obtaining a location-based service from those location-based service providers that have adopted the Guidelines that their location information will be protected and used or disclosed only as described in provider notices. By receiving notice and providing consent consistent with these practices, users will maintain control over their location information.

The Guidelines encourage providers of location-based services 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. CTIA supports the ongoing and continuous education of users so they may make informed choices.

We believe the Guidelines offer a meaningful framework for the protection of user privacy. Further, we urge policymakers to recognize that the industry's willingness to develop best practices, and to revise those guidelines as circumstances warrant, represents the best way to balance the need to promote and protect user privacy while also facilitating the deployment of new and innovative products and services.

A call for legislative restraint does not mean that there is no role for Congress while the industry evolves. Congress already has made clear that "the express prior authorization of the customer" is the prerequisite for the disclosure of a wireless customer's location information. While Section 222 on its terms applies only to "telecommunications carriers," its requirements have been observed by all providers of wireless location-based services. As these services continue to evolve and develop in both predictable and

unpredictable ways, Congress has an important oversight role in insuring that all providers of location-based services continue to deliver effective notice and obtain consent regardless of the device or technology used, and regardless of the provider's business model, so that wireless users can continue to exercise control over the use or disclosure of their location information.

One area in which specific guidance from Congress may be appropriate is the clarification of the terms under which location information may be released to law enforcement. Just this month, the U.S. Court of Appeals for the Third Circuit heard oral argument on the issue of what legal standard should apply when law enforcement seeks to gain access to a wireless user's location information records, or seeks to track individuals prospectively. Many federal magistrates have determined that law enforcement must obtain a warrant based on probable cause to prospectively track a device. Other magistrates have authorized tracking on a lower standard. Most courts have allowed access to stored location records based on a court order and demonstrated need, but in the Third Circuit, the Department of Justice and privacy advocates argued whether access to these historical location records should meet a probable cause standard. Service providers need clarity so as to not be caught in the middle of these disputes regarding the appropriate legal standard.

Finally, we urge Congress to recognize the interstate nature of location-based services, and the mobile nature of wireless users, and to take care in whatever framework may be adopted to preempt state regulation of these service offerings. A uniform, national approach to these issues presents the best way of protecting user privacy and educating and informing wireless customers while fostering innovation, investment, and the introduction of new location based services by wireless carriers, device manufacturers, operating systems developers, and applications creators.

On behalf of CTIA, thank you again for the opportunity to share our views with the subcommittees. We look forward to working with you as you continue your efforts.

Mr. RUSH. The Chair now recognizes Mrs. Collier for 5 minutes for the purposes of an opening statement, and she will conclude our witnesses' opening statements. Mrs. Collier, you are recognized for 5 minutes.

TESTIMONY OF ANNE COLLIER

Ms. COLLIER. Thank you, Chairman Rush and Chairman Boucher and members for me here today. My name is Anne Collier and I am co-director of ConnectSafely.org and serving as co-chair of the Online Safety and Technology Working Group.

We have been following location-based services for several years now and we don't feel they represent a unique safety risk to young social-media users for several reasons that I will go into. We do, however, feel particular consideration needs to be given to children's privacy as geolocation products and services increasingly connect to children's other social tools and networks.

First, some context. U.S. teens now send or receive more than 3,100 text messages a month. For them, a text isn't like a phone call, it is part of a conversation, part of the ongoing flow of their social life, and texting is only one of their tools for hanging out online and offline. They also use their phones to update their social network profiles, play games, snap and upload photos and videos to profiles, and even talk. There is as yet no data on teens' LBS use but we know that more than 65 million, or about a third, of Facebook users of all ages currently access Facebook through their mobile devices, and who is all this communication with? Research shows that the vast majority of teen social networks, 91 percent, use all these tools to socialize with friends they see regularly, usually at school.

We adults think and talk about standalone products and services in terms of use but with kids, it is more useful to view LBS in terms of child and adolescent development. For example, location-based services depend a lot on users' mobility and autonomy and involve a certain amount of spontaneity. The main objectives are spontaneous in-person get-togethers and finding good places to eat or drink when you are on your own in a city. A user really needs the independence enjoyed by an older teen or adult to enjoy LBSs. The mobility of a driver's license helps too. Urban youth may have more physical mobility without a driver's license but there is no reason to believe they have proportionately more freedom from adult supervision.

Meanwhile, LBSs are, to young people, just another twist on status updates. The 75 percent of teens owning cell phones now, they have for some time had other ways to let each other know their plans and whereabouts and they are constantly in touch, text messages, updates to social network profiles, Gmail chat and instant messages, to name a few. They are always in touch with each other. And remember, the operative phrase is "each other." Virtually all of this communication is with known peers.

Still, understandably, the most visceral and concerning risk associated with location-based and all Net services is predation. So let us go into that a little bit. Research about LBS use is needed in this area too but we do already know a lot about youth risk online. First, not all youth are equally at risk. The young people most at

risk online, on phones are those most at risk already offline, and a child's psychosocial makeup and home and school environments are better predictors of risk than any technology a child uses.

Second, the risk of Net-related predation is extremely low relative to real-life risk, according to David Finkelhor, director of the Crimes Against Children Research Center. In a report just last spring, Dr. Finkelhor and his co-authors wrote, "There is no evidence that online predators are stalking or abducting unsuspecting victims based on information they posted at social networking sites." A recent study of how teens deal with strangers in a social site found that 92 percent of those who had received sexual solicitations had responded appropriately, ignoring, blocking or reporting the sender.

Finally, a quick snapshot of an emerging privacy challenge. Because Google Buzz is brand new and a hybrid of LBSs, Gmail, microblogging and social networking, we are all at the early stages of figuring out its implications for kids, a lot of whom use Gmail. Charlene Lee, a mom and well-known industry analyst in San Francisco, blogged just this past Sunday that she discovered her 9-year-old daughter was using Buzz with her friends. They had only had one conversation so far but they had no idea their conversation was public. She thought about just disabling Buzz on her daughter's computer but the kids were enjoying it so much that Lee decided she would let her daughter keep going if all the kids kept the conversation private. And there is the rub. Ensuring that all the girls keep it private will be a project for her, probably involving communication with all the other parents.

Privacy is now a collective effort on the part of users every bit as much as providers in this user-generated medial environment. It is a negotiation among users in a peer group sharing thoughts, tagging photos, et cetera. Privacy protection is user generated too, not just a matter of privacy features. This is going to take a lot of consumer education by us NGOs and the industry and government.

This issue also points to the impact on children's, everybody's privacy of combining social media products within companies across devices and platforms and then across users' networks like Facebook Connect. A lot of consumer education is needed with support from industry best practices. Thank you.

[The prepared statement of Ms. Collier follows:]

February 22, 2010

Rep. Bobby L. Rush
Chairman
Subcommittee on Commerce,
Trade, and Consumer Protection

Rep. Rick Boucher
Chairman
Subcommittee on Communications,
Technology, and the Internet

Congress of the United States
House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington, DC 20515-6115

RE: February 24, 2010, testimony at a joint hearing entitled "The Collection and Use of Location Information for Commercial Purposes" before the Subcommittee on Commerce, Trade, and Consumer Protection and the Subcommittee on Communications, Technology, and the Internet

Dear Chairmen Rush and Boucher and Members:

By way of introduction, I am co-director of ConnectSafely.org, founder and executive director of its parent organization, Net Family News, Inc., and currently serving as co-chair of the Online Safety & Technology Working Group, created under the Protecting Children in the 21st Century Act of 2008. ConnectSafely.org is the leading interactive resource on the Web for parents, teens, educators, and everyone engaged and interested in young people's safe, enriching use of the fixed and mobile social Web. Founded in 1999, Net Family News, Inc., is a 501c3 nonprofit organization based in Salt Lake City, Utah, with offices in Salt Lake and Palo Alto, Calif.

Young people's tech-enabled social lives

US teens now send or receive an average of 3,146 text messages a month and 9-to-12-year-olds 1,146, according to the latest figures from Nielsen (http://bit.ly/d5iiHC). For them, a text isn't like a phone call, it's part of a conversation as well as of the ongoing flow (or seemingly 24/7 drama) of school life. But texting is only one of young people's social tools. They also use their phones to update their profiles in social network sites,

play games, snap and upload photos to their social network profiles, do the same with videos – and even talk. There is as yet no data on teens' mobile social-mapping or LBS use, but we know that more than 65 million, or about a third, of Facebook users of all ages currently access the social site through their mobile devices ("Online as soon as it happens," February 2010, EU's European Network and Information Security Agency <http://enisa.europa.eu>).

In today's fixed and mobile, user-driven media environment, young people's tech-enabled, real-world social lives are highly fluid experiences. They make little distinction between online and offline and fly fast among devices and services. The online and on-phone part are just that – part of and blending into the full picture. Research shows that the vast majority of them – those who aren't already so-called at-risk youth in real life – use technology and devices to socialize with their friends at school and in other important activities and places in their lives. According to the Pew/Internet Project, 91% of teen users of social network sites use them to stay in touch with friends they already see regularly (http://bit.ly/9cWGZ7). Technology and Net use simply can't be separated out from their everyday lives (see p. 31, see *Hanging Out, Messing Around & Geeking Out: Kids Living and Learning with New Media*, by Mimi Ito, et al, MIT Press, 2009).

We adults think and talk about stand-alone products and services, such as location-based services (LBSs), each with its terms of use and privacy policy, but it's helpful to keep in mind that young people's tech use is difficult to break down in that way. It's more useful to view the way they use technology in terms of child and adolescent development.

Take today's subject – social mapping or LBS – for example: The use of location-based social networking and games depends on users' mobility and autonomy and has an element of spontaneity. Spontaneous in-person get-togethers are a key purpose of these services – as well as finding good places to eat or drink when you're on your own and new to a city (see New York Times <http://nyti.ms/3h1gX>).

A user really needs the independence of an older teen or adult to enjoy BrightKite, Foursquare, or Loopt, for example. The mobility of a driver's license helps

too. What social currency or enjoyment would a 12-year-old get out of posting to his school friends, "I'm at Starbucks with my mom"? He might leave the "mom" part out of it, but his friends, aka social network, probably wouldn't freely be able to act on that announcement because the need for permission or a ride would intervene. Urban youth may have more physical mobility without a driver's license, but there's no reason to believe they have proportionately more freedom from adult supervision.

Meanwhile, location-based services are, to young people, just a new twist on status updates. With 75% of teens owning cellphones (see Pew/Internet, February 2010 <http://bit.ly/bXjTH3>), they've for some time had other ways to let each other know their plans and whereabouts: text messages, updates to social-networking profiles, Gmail chat, and instant messages, to name a few. And remember what I said above about who they're using these social tools to send messages to: "each other." "Most teens are not interested in being truly public," social-media researcher Danah Boyd told the Washington Post this month (http://bit.ly/9MrVKj). To the extent that LBSs are designed to connect with strangers, most teens are unlikely to use them.

As for youth who don't have engaged caregivers and are reaching out beyond their school-related social circles, there may be a greater degree of risk from LBSs, but this is the demographic that has long represented at-risk youth online, the minority of online youth who need the help of social workers, mental healthcare experts, and risk-prevention practitioners....

Youth risk on the social Web

The most visceral and concerning risk people seem to associate with the collection and use of location data, where minors are concerned, is predation. Research specifically looking at LBSs and predation is needed – and government support of such research would be most welcome – but we already know a lot about youth risk on the Internet in general.

From the significant body of youth-risk research reviewed and presented by the Internet Safety Technical Task Force of 2008 at Harvard's Berkman Center

(http://bit.ly/by0GRZ) as well as from subsequent such research, we know that, as far as predation is concerned...

1) Not all youth are equally at risk – the youth most at risk online are those most at risk offline, and a child's psychosocial makeup and home and school environments are better predictors of that risk level than any technology he or she uses.

2) Predation is not the most salient risk online youth face. Mean behavior and bullying by peers are much more common – in fact, two separate national studies have found that about one-third of online youth experience cyberbullying, which is closely associated with what's going at school.

3) The actual risk of Internet-related predation is extremely low, according to Dr. David Finklelhor, director of the Crimes Against Children Research Center at the University of New Hampshire – too low to be estimated in the CACRC's 2000 and 2005 studies of online sexual solicitations of youth. And in a major update last spring ("Trends in Arrests of 'Online Predators'" <http://www.unh.edu/ccrc/pdf/CV194.pdf>), he and his co-authors wrote: "There was no evidence that online predators were stalking or abducting unsuspecting victims based on information they posted at social networking sites." [Note that much of the geolocation information under discussion, here, as being posted via location-based apps, games, and services is being posted to social networking sites.]

For context: We have also long known that the vast majority of sexual exploitation cases against children are perpetrated by people they know in everyday life *off*line; a less-well-known fact is that between 1990 and 2005, when the World Wide Web got its start and grew exponentially, there was a 51% decline in overall child sexual exploitation, and the latest FBI figures show a continuing drop in violent crimes ("2008 Crime in the United States" <http://bit.ly/dBVIPy>). The number of rape cases is down 9.6% since 2004, "considerably more of a decline than the overall crime drop during this period," Dr. Finkelhor reported last September. He explained how that spells a decline in child sexual abuse: "While there is no specific child victimization category, bear in mind that well over half of the rapes known to law enforcement are against persons under 18,

so *this rape decline is very much a drop in child victimization"* (Finkelhor in an email to a group of youth-risk practitioners, researchers, and NGOs).

Apart from the unlikelihood of minors using LBSs when they don't have the means independently to meet up with friends in real time (as mentioned above), the research also shows they are psychosocially disinclined to interact with people who aren't friends and known peers and who aren't part of the flow of their social experience at any given moment. A recent study of how youth deal with strangers in a social network site – which, like texting, is part of their social flow – found that 92% of youth at the receiving end of sexual solicitations in a social site either had an appropriate reaction or ignored the solicitation ("The Association of Parenting Style and Child Age with Parental Limit Setting and Adolescent MySpace Behavior," by Dr. Larry Rosen, in Journal of Applied Juvenile Psychology, November-December 2008 <http://bit.ly/bfs3vP>). ["Appropriate reaction" was defined as telling the person to stop, blocking the person from their page, removing themselves from the situation by logging off, or reporting the incident to an adult or to the site.]

As for LBSs themselves, it is my understanding that most of the new social-mapping services do not involve automatic, software-produced disclosure of the cellphone owner's movements, but rather disclosure by the user himself of his whereabouts, in the form of a social-networking-style update. If there are concerns about what minors post about their location via LBSs, the concerns would necessarily also apply to other social-media services, including instant messaging, Skype, Facebook, Twitter, and texting on mobile phones. LBSs by themselves do not represent a unique safety threat. [PleaseRobMe.com, an awareness-raising site, points out that sharing one's location widely when not at home potentially lets burglars know one's house is up for grabs, but this is a risk to adults' property not to youth safety.] We are concerned about children who do download LBSs being bombarded with advertising and marketing based on their location and hope proliferating geolocation-enabled apps are informed about and operate in compliance with the Children's Online Privacy Protection Act.

The question has been asked whether the way LBSs function is too complex for young people to grasp. My answer is that they are no more complicated to use than

and 4) young people keep growing and maturing (an obvious fact that often somehow gets left out of the equation). Change – in technology, media, households, consumer behavior, unfolding research, and individual kids – truly is the only constant in this scene.

Consumer education + best practices + parental-control tools

Regulation is a blunt instrument in the face of this level of fluidity and change, micro and macro. Only the caring adults closest to a child can possibly know how to calibrate family rules and parental-control tools to fit a growing child's needs.

The ultimate protection for all children is the filtering "software" in their heads. It has numerous benefits: Every child is born with this latent filter, which improves with use, works with all devices, and is with her wherever she goes. Its downside is that children need help in developing their cognitive filter, and not all "developers" – parents, caregivers, educators, etc., teaching them media and life literacy – understand the ever increasing importance of this filter and the responsibility its owner and they have in developing it.

In other words, consumer education – for youth, parents, and schools – is not only essential but becoming increasingly more so. Its most basic and vital forms are the new media literacy and citizenship that help children's cognitive filter think critically about what's going out (behavioral and informational) as much as what's coming in as they use two-way social, or behavioral and collegial, media. This kind of literacy gets developed largely at home and school from the earliest ages, when children first use technology. But consumer education takes many other forms as they grow, forms that are just as important: from notice & consent in LBSs to tutorials for features in products and services to professional development for educators about teaching with new media. Children's education needs to be provided by parents, industry, government, and schools; *parent and educator* consumer education needs to be provided by NGOs, industry, and government.

Children can't learn how to use social technology and media properly without having access to these new media and technologies – just as swimming can't be taught without pools – so government and other entities need to join industry in promoting their

Facebook or MySpace and much less complex than a console videogame or multiplayer online game like World of Warcraft. We also know from a December 2008 study by Computer Associates that social sites' privacy features are not too difficult for teens to use, and teens do use them; the study showed that 79% of teen social networkers restrict access to their profiles in some way (http://bit.ly/7bRb). That is not to say that all users, including the relatively few teens likely to be using LBSs, will not need plenty of consumer education and sound notice-and-consent practices on the part of location-based providers concerning the wider dissemination of their posts through networks these services are connected to such as Facebook and Twitter. In other words, it's more important than ever that LBSs follow CTIA's guidelines for customer notice and consent and that all parties, from app developers to service providers, are committed to clear notice to and consent by consumers as to how their location information is being used.

Protecting a moving target

How to protect young people in a user-driven media environment in which youth define active use (see "Generation M2" from the Kaiser Family Foundation <http://bit.ly/7XukS3>) has been a puzzle since the advent of interactive media. First we thought we should figure out how to protect them from technology, since technology was "obviously" the main problem. Then we learned from the growing bodies of both youth-risk and social-media research that the main "problem" is actually child and adolescent development and behavior. Adults not up to speed on the research keep thinking that regulation must be a solution, and as a society we have struggled to enact legislation that could somehow protect both children and free speech, when it increasingly seems impossible to define, separate out, and control inappropriate adolescent behavior while somehow leaving alone what is appropriate, developmentally normative, and constructive.

Meanwhile, 1) social media and technologies continue to proliferate, 2) the Internet becomes increasingly accessible, 3) young people's social lives are increasingly a mashup of online and offline experiences and of new media, technologies, and devices,

wise use in US education and ending efforts to block them. This is becoming widely recognized overseas – see British education watchdog Ofsted's February 2010 report <http://bit.ly/aPR298> showing that schools rated "outstanding" for online-safety conditions and instruction used "managed" rather than "locked down" filtering, thereby requiring pupils to learn how to "take responsibility themselves for using new technologies safely."

Supporting that all-important education is a key industry best practice, which needs the support of government. For example, the wireless industry association is currently revising its best-practice guidelines, appropriately broadening the definition of location-based services. It is also working on a consumer-education campaign to increase public awareness of parental controls and other options parents have to support children's safe, constructive use. We recommend that the industry also mount an education program aimed at both parents and youth which is focused specifically on location-based services, games, and apps – so they understand how to use privacy features and who might see the location information they're disclosing.

Another important support to parents as they protect and educate their children are a broad variety of parental-control tools to choose from as their children mature. The mobile carriers provide a robust array of such tools, from time limits on devices to caller blocking to restricting app downloads. That last control is an excellent protection against minors using LBSs not appropriate for their use. The main current provider of cellphone apps, Apple, rates apps by age and provides parental controls for its iPhone and iPod Touch (though without much transparency to consumers and NGOs) in addition to the Smart Limits parental controls provided by iPhone service provider AT&T. NGOs, industry, and government need to work together to raise consumer awareness of these protective tools and features. An excellent recent example of government-NGO partnership is the Federal Trade Commission's NetCetera booklet and campaign. We'd like to see more coordination within the US government and between government, industry, and NGOs along the lines of the UK's Council for Child Internet Safety (http://www.dcsf.gov.uk/ukccis).

Conclusion

There is risk to using LBSs for youth, just as there is to their using any means to interact with the world – but mostly in the area of peer-to-peer interaction, where tech-based socializing is concerned. Teens use text messaging, talking, instant messaging, social networking, and other social tools to notify friends of their thoughts, plans, and whereabouts. We do not see LBSs as representing greater risk than other social media, particularly to youth under 16, because independence and mobility are basic criteria for enjoying the services. At the same time, the research shows that teens who are not taking extraordinary risks in the real world are savvy about ignoring or appropriately reacting to overtures from strangers, and that the risk of "online predators victimizing unsuspecting teens because of information they're posting in social sites" is not evident to the Crimes Against Children Research Center.

It's useful, especially since there is no research specific to minors' use of LBSs, to view their use in the context of young people's use of all social media and technologies, as well as in the context of the everyday, tech-enabled social lives of today's teens. Technology and Net use simply can't be viewed as separate from the flow of their online/offline social lives. With these social technologies, the research shows, the vast majority of youth are socializing with friends and peers at school.

To remove the risks associated with their social lives, online and offline, is not only impossible but harmful to their development, as risk assessment is a primary task of adolescent development, pediatricians and child-development specialists tell us. Legislating against youth risk is not the answer. A combination of parental-control technologies, industry best practices, more consumer education, and better coordination of efforts to protect youth both within the federal government and in cooperation with industry and NGOs is the best way to go.

ADDENDUM A

Right after I filed the above written testimony, a colleague "tweeted" about a new blog post by a parent about Google Buzz. Because Buzz is brand-new and a hybrid of LBSs, Gmail, micro-blogging, and social networking, we're all at the early stages of figuring out its implications for kids, a lot of whom are known to use Gmail (I haven't been able to find numbers).

The parent is social-media industry analyst Charlene Li. She blogged on Sunday (http://bit.ly/aARahl) that her 9-year-old daughter quickly figured out how to use Buzz (from her computer), enjoyed it, and had had one conversation on it with her friends. The problem was that her daughter and friends didn't know that the conversation wasn't visible only to them. It was a public conversation.

Li writes that "the easiest thing to do as a parent is to simply disable Buzz, meaning that the Google profile and all followers are deleted – permanently." But because her daughter enjoyed Buzz so much, she seems open to "managing groups, privacy settings, etc." so her child can continue using the service. "We'll give it a try," she writes, "but unless her friends also keep the conversation private, it will all be for naught." Ensuring that with the other kids in the group and their parents will be a project.

Google last summer agreed, in response to a complaint by the Children's Advertising Review Unit of the Better Business Bureau, a COPPA Safe Harbor, to require a birth date at registration to Gmail and, if a user indicates he or she is under 13, a session cookie to block the user from re-registering with an earlier birthdate.

That's a start, but what this issue points to is the impact on children's privacy of *combining* social-media products within companies and connecting them across networks such as Facebook Connect. Perhaps the FTC's forthcoming review of COPPA rules and enforcement will address this emerging issue. But we feel the brilliant software engineers and project managers who develop these products need to wear their parent hats more, companies need to be thinking through children's privacy from the earliest development stages, and industry best practices need special sections or clauses addressing child privacy and safety. *–Anne Collier, ConnectSafely*

ADDENDUM B

ConnnectSafely.org's Cellphone Safety Tips (http://bit.ly/9W4jBf)

Cellphones are increasingly full-blown handheld computers, and everything that can be done on the Web via computer – photo-sharing, Web browsing, game playing, tune-swapping, real-time text chat, and (oh yeah) talking *– can be done on a phone. Here are some basic ideas for keeping mobile phone use safe and constructive:*

Smart socializing. Use the same good sense about what you post from your phone as from a computer. Once they're posted, text, photos, and video are tough to take back, can be copied and pasted elsewhere, and are up there pretty much forever. Think about the people in them (including you!). Reputations are at stake – even more so if nudity or sex is involved.

Phones are personal. Letting other people use your phone when you're not around is like letting them have the password to your social network profile. They can impersonate you. Which means they can play tricks on you that could really become a problem. It's a good idea to lock your phone when you're not using it. It's not a good idea to let friends text for you while you're driving. Don't text while driving; just be safe and turn the phone off!

Bullying by phone. Because people socialize on cellphones as much as online, cyberbullying can be mobile too. Treat people on phones and the Web the way you would in person, and the risk of being bullied goes down. Be aware, too, of people randomly taking pictures at parties – you may not want to be tagged in their social-network photo albums.

Sexting: It's the same on phones as on the Web - do not take, send, post or even store on your phone nude photos of anyone under 18. You could be charged with production, distribution, or possession of child pornography, a serious crime. You could also be subjected to jokes, bullying, blackmail, expulsion from school, loss of a job, etc. and the images can circulate forever.

The value of "presence." If you do a lot of texting, consider the impact that being "elsewhere" might be having on the people around you. Your presence during meals, at parties, in the car, etc. is not only polite, it's a sign of respect and appreciated.

Down time is good. Constant texting and talking can affect sleep, concentration, school, and other things that deserve your thought and focus. You need your sleep and *real* friends understand there are times you just need to turn off the phone - harassment can happen between midnight and morning too.

Social mapping. Most cellphones now have GPS technology and there are a growing number of services that allow friends to pinpoint each other's physical location. If you use such a service, do so only with friends you know in person, and get to know the service's privacy features!

ConnectSafely.org's Social Web Safety Tips for Teens (http://bit.ly/aGQG8z)

These tips, based on the latest research, will help teens' socializing stay fun and safe on both the fixed and mobile social Web. **Be your own person**. Don't let friends or strangers pressure you to be someone you aren't. And know your limits. You may be Net-savvy, but people and relationships change, and unexpected stuff can happen on the Internet.

Be nice online. Or at least treat people the way you'd want to be treated. People who are nasty and aggressive online are at greater risk of being bullied or harassed themselves. If someone's mean to you, try to ignore them - often that makes them stop. Use privacy tools to block them from viewing your full profile and contacting you.

Think about what you post. Sharing provocative photos or intimate details online, even in private emails, can cause you problems later on. Even people you consider friends can use this info against you, especially if they become ex-friends.

Passwords are private. Don't share your password even with friends. It's hard to imagine, but friendships change and you don't want to be impersonated by anyone. Pick a password you can remember but no one else can guess. One trick: Create a sentence like "I graduated from King School in 05" for the password "IgfKSi05."

Read between the "lines." It may be fun to check out new people for friendship or romance, but be aware that, while some people are nice, others act nice because they're trying to get something. Flattering or supportive messages may be more about manipulation than friendship or romance.

Don't talk about sex with strangers. Be cautious when communicating with people you don't know in person, especially if the conversation starts to be about sex or physical details. Don't lead them on - you don't want to be the target of a predator's grooming. If they persist, call your local police or contact CyberTipline.com.

Avoid in-person meetings. The only way someone can physically harm you is if you're both in the same location, so – to be 100% safe – don't meet them in person. If you really have to get together with someone you "met" online, don't go alone. Have the meeting in a public place, tell a parent or some other solid backup, and bring some friends along.

Be smart when using a cell phone. All the same tips apply with phones as with computers. Except phones are with you wherever you are, often away from home and your usual support systems. Be careful who you give your number to and how you use GPS and other technologies that can pinpoint your physical location.

ConnectSafely.org's Social Web Safety Tips for Parents (http://bit.ly/4zUOR3)

These tips for parents about safety on the social Web are based on the latest research from the Crimes Against Children Research Center at the University of New Hampshire (with input from our colleagues there).

Be reasonable and try to set reasonable expectations. Pulling the plug on your child's favorite social site is like pulling the plug on his or her social *life*. Instead of being protective, it can shut down communication and send kids "underground" where they're more at risk. It's too easy for them to set up free blogs and profiles from anywhere, including friends' houses or even a cell phone.

Talk with your kids about how they use the services. They, not news reports or even experts, are the ones to consult about their social-Web experience. Help them understand basic safety guidelines, such as protecting their privacy (including passwords), not harassing peers, never talking about sex with people they don't know, avoiding in-person meetings with people they "meet" online, and taking care in what they post - because anything people put online can be grabbed, reworked, and used against them.

Support critical thinking and civil behavior because no laws or parental-control software can protect better than a child's developing good sense about safety and relationships. Research shows that kids who are aggressive and mean online toward peers or strangers are at greater risk of becoming victims themselves. So teach them to be good citizens and friends online as much as offline.

Consider requiring Internet use in a high-traffic place in your home - not in kids' rooms - to help you stay aware of their online time. This way, you can encourage a balance between online time and their offline academic, sports, and social times. Know that there are also many ways kids can access the Internet away from home, including on many mobile phones and game players.

Try to get your kids to share their profiles and blogs with you, but be aware that they can have multiple accounts on multiple services. Use search engines and the search tools on social-networking sites to search for your kids' full names, phone numbers and other identifying information. You're not invading their privacy if they're putting personal info in public "places" online. If their pages are private, that's a good thing, but it's even better if they share it with you.

Mr. RUSH. The Chair now yields to the chairman of the Telecommunications Subcommittee, my friend, Mr. Boucher.

Mr. BOUCHER [presiding]. Well, let me thank our witnesses for their statements this morning and for your participating in our hearing and informing us on your well-studied views with regard to location-based services and privacy as associated with them. I have a series of questions I will propound to the witnesses but I want to say a word of welcome first to Mr. Whitfield from Kentucky, a friend of long standing, who is the new ranking Republican member of the Subcommittee on Consumer Protection and just say to him how much I look forward to working with him on privacy matters.

The Communications Act requires opt-in consent before telecommunications carriers can disclose geolocation information but there is no federal statute or regulation that governs privacy rights associated with non-carriers who come into possession of that information whether they collect it themselves or whether they receive it from someone who does, and I am wondering what our witnesses would say to this question. Has the time arrived for Congress to adopt a statute that applies a consent requirement with respect to geolocation services information, not only to telecommunications carriers but to others who come into contact with that information? Let us begin with Mr. Morris.

Mr. MORRIS. My answer to that question is a very short yes but with a qualification to say that we would certainly urge Congress to do just what you said and focus careful attention on location but we would hope it would be in the context of a larger privacy bill as opposed to a sectorially focused bill just on location itself. I mean, we have an anomalous situation in this country where my video rental records are more protected than my e-mail on Gmail and that to us doesn't make sense, so we hope that the work you do on location privacy is in the context of a broader baseline privacy bill.

Mr. BOUCHER. I couldn't have provided a better answer myself. Thank you. I think you can expect to see this measure emerge as part of a larger legislative item.

Mr. Altschul, I want to commend CTIA for the adoption of your series of best practices, guidelines and recommendations. I have a couple of questions for you. First of all, can you tell me the percentage of your carriers that are part of CTIA who are complying with your guidelines and recommendations at the moment?

Mr. ALTSCHUL. We believe that all of the carriers are complying with the guidelines, which were intended to build on the principles in section 222(f) and they provide guidance and examples for how to convert——

Mr. BOUCHER. So you think you have 100 percent compliance?

Mr. ALTSCHUL. We do, for the carriers that are supporting these services.

Mr. BOUCHER. I want to give you an opportunity to respond to some of the statements that Professor Cranor in her testimony made. I missed her oral testimony but her written testimony, which I have reviewed, suggests that your voluntary guidelines could be sharpened a bit, and I want you to respond to this. She says that they do not specify the form, placement or content of no-

tices, there is no mechanism for enforcement within our guidelines, there are no assurances that the location-based service providers follow the practices—that is kind of a subset of the previous comment—and your guidelines as they specify the disclosures that the carriers should make are somewhat confusing and might lead to different kinds of disclosures being made with regard to the same kind of information among the various different carriers. Would you like to respond to those comments?

Mr. ALTSCHUL. Yes. Thank you. First, by design, our guidelines do not provide a one-size-fits-all set of guidance or statements because the applications that fall within both the guidelines and, more importantly, the category of location-based services, do not fit one category. Certainly there is a very different set of privacy and customer expectations associated with a one-time query for a concierge-type service, where is the nearest gas station, to a continuing social networking application that links users by consent to one another's location. So rather than specifying one kind of notice, which we don't think would be appropriate across the broad spectrum of services, our guidelines address the fact that the notices should be tailored to the type of location service. I view that as a strength rather than a weakness in the guidelines.

As for not all of the applications that were in her survey following even rudimentary privacy practices and notices, we recently did a survey that didn't purport to be scientific. We actually went to the Web sites of some of the application service providers, created a snapshot of what is being provided, and there is a range of notice and consent and privacy statements. We submitted this paper to the Federal Trade Commission last month for their privacy workshop.

But through guidelines—and this will get to your question about the lack of enforcement—the industry and all of the participants in the industry, carriers and application providers alike, play a very important role in educating themselves and their customers as to what they should expect and should insist upon in using any kind of application location-based service, and that is the primary role of industry guidelines. We are not being codified in Title 18 of the U.S. Code. We are trying to understand the issues——

Mr. BOUCHER. Well, in the interests of time, Mr. Altschul—I am intrigued by your answers, I would like to hear more, but my time is expiring. Let me just suggest this. It might be helpful if you review Professor Cranor's comments and consider modifying your guidelines to the extent that you can sharpen them so that they provide greater clarity to the carriers, particularly on what kinds of disclosures the carriers should make with regard to services, to the information they come into contact with. I think it might be helpful. Would you be willing to consider doing that?

Mr. ALTSCHUL. Absolutely.

Mr. BOUCHER. I have one further question. My time has expired. I intend to be generous with the other members in terms of their time for questions as well.

Mr. King, Mr. Bernard, let me just pose this question to you. Do you think that your customers are aware of the secondary uses that your services are making of the geolocation information about them, and do they have a reasonable expectation based on informa-

tion that is made available to them that their geolocation information is going to be used by advertisers in order to target advertising to them. Mr. Bernard, Mr. King.

Mr. KING. Thank you, Mr. Chairman. One way to answer that is that the location information goes out to an advertising network and requests an ad so the location is just—it is not personally identifiable so that there is no information about that consumer going to the advertiser. We are selecting from an inventory of ads and then bringing them in and showing what we think are the most appropriate ad, given that context.

Mr. BOUCHER. Well, that is understood, but the question is, does that person have a reasonable expectation that those events are going to happen, that the advertisers are going to be marketing to them based in part on their location?

Mr. KING. Yes. We have a location-based application that is both free and ad driven where you can pay a subscription fee so they are free applications we believe that consumers expect to be ad driven, so the short answer would be yes to that.

Mr. BOUCHER. Mr. Bernard.

Mr. BERNARD. Thank you. Useful Networks does not support secondary uses to now, as I think about them, where secondary use is using that location subsequently beyond that for which you have already provided notice. So specifically in our mind, we provide primary use, and an example of that is our location-based advertising trial. End-users were presented with a banner ad on the mobile Web site enticing them to click on it to see a viewer location or a quick serve burger location near them. The next page they saw explicitly said please allow us to use your location to provide a list of stores near you, and only if they clicked were they provided——

Mr. BOUCHER. All right. That is very clear. Thank you. Mr. King and Mr. Bernard, I just want to pose one further question to you, and it is the same question I asked Mr. Morris at the outset. Is it time that we had a federal statute in order to provide a uniform set of standards across applications, not just for the telecom carriers but for those who are providing applications, selling applications, using applications as well?

Mr. KING. I would say in general, yes.

Mr. BOUCHER. Thank you. That is a great answer. That is what I am looking for.

Mr. Bernard?

Mr. BERNARD. It should be a uniform set of practices, not necessarily legislation.

Mr. BOUCHER. Well, OK. That is half a loaf. Thank you all very much.

The gentleman from Kentucky, Mr. Whitfield, is recognized for his questions.

Mr. WHITFIELD. Thank you, Mr. Chairman.

And Mr. Bernard, I didn't hear the last part of your answer. Would you repeat that for me?

Mr. BERNARD. The last part of that more specifically spoke to self-regulation. We believe there are certainly business incentives both on the part of the distribution centers, whether they are carriers or device manufacturers, as well as on consumers in that they

won't use services where they feel like their privacy is not respected.

Mr. WHITFIELD. Well, everyone——

Mr. BERNARD. We do agree with a level playing field.

Mr. WHITFIELD. Everyone on the panel has had the opportunity to answer that question except a few. Professor Cranor, what is your position on Chairman Boucher's question?

Ms. CRANOR. Yes, I think that it is probably time to have some legislation to have some privacy rules, but like Mr. Morris, I think that we shouldn't have a very narrow view on just location if we are going to set privacy rules, that there is a need for more general privacy legislation.

Mr. WHITFIELD. And Ms. Collier, what is your position?

Ms. COLLIER. I agree with that. I think it is time to update privacy law but, you know, it needs to coordinate with COPPA, the Children's Online Privacy Protection Act, but it shouldn't refer to just a single technology.

Mr. WHITFIELD. And Mr. Altschul?

Mr. ALTSCHUL. Well, we certainly endorse the idea of a level playing field and the consumers don't have to guess as to what their privacy rights are. We are always concerned that despite the best of intentions, when these principles are codified, either technology or unintended consequences will get in the way.

Mr. WHITFIELD. Professor Cranor, in your testimony you talked about a system that was developed at Carnegie Mellon, and I am not sure the pronunciation but is it Locaccino? Locaccino. Now, how widespread is that type of technology being used?

Ms. CRANOR. So our particular system is a research system that is being used by a thousand people. It is similar technology to what is being used by commercial providers. The main difference is that we have gone out of our way to provide privacy controls at a very fine-grained level for people who use it.

Mr. WHITFIELD. I see. And, you know, this is deviating a little bit from the technical aspect of this but also I found it interesting in your testimony, you said in your survey, we found that most of our participants did not expect that location-sharing technologies would be all that beneficial to them, and then that they did have significant concerns about their privacy when sharing their locations online. So what is your overall conclusion of that? It sounds like to me this is a service that is really not all that beneficial but——

Ms. CRANOR. Well, so what we found is that the general public for the most part doesn't understand why they would want location-based services. Now, there are plenty of people who have adopted them who do get it and they say yes, this is useful to me and I want to use them. But they are right now the minority of the population.

Mr. WHITFIELD. So you found most people just simply were not aware of the benefits of it?

Ms. CRANOR. Right. They don't find it beneficial, and when we talk about this with people, you know, the notion that there is a map and there is a pinpoint and that is me on it, that really scares people.

Mr. WHITFIELD. Right. I would just ask you, Mr. Morris, let us assume for the moment that we are going to regulate Internet privacy. Should the FCC do the regulating or should the FTC do the regulating or should different regulators govern different parties?

Mr. MORRIS. Well, we would suggest that the FTC is probably the better place to go for two independent reasons. One, the FTC has a very long track record and experience in looking at consumer privacy issues, and they have already through a number of workshops over the years have been looking specifically at location privacy. And secondly, the FCC is frankly really not the federal Internet commission. It really doesn't have a broad mandate to regulate the Internet. It doesn't frankly have regulatory experience at the application layer. It is obviously critically important at the lower layers of the communications stack and so, you know, its regulation of telecommunications carriers and underlying broadband services is clear and appropriate but it doesn't really have as extensive experience in the privacy area at the applications layer as the FTC does.

Mr. WHITFIELD. Thank you all, and I see my time is expired.

Mr. BOUCHER. Thank you, Mr. Whitfield.

The gentlelady from Florida, Ms. Castor, is recognized for 5 minutes.

Ms. CASTOR. Thank you, Chairman Boucher.

Mr. Altschul, I thought it was interesting, you said that even though all of your members are adherent to best practices that technology has overtaken best practices. So I guess in effect you are conceding that given how valuable the location data could be to marketers and it is to advertisers, that industry self-regulation is not realistic.

Mr. ALTSCHUL. No, what I meant to convey by saying the technology has overtaken our guidelines, our guidelines just 2 years ago were carrier centric. Carriers were clearly covered by section 222 of the Communications Act. That was before the introduction of iPhones and introduction of smartphones that have their own GPS receivers and before the broad adoption of WiFi public access points. What surprised the experts in the industry was how quickly the landscape changed in using this technology so that as you heard from everyone on the panel and many of the opening remarks today, increasingly location-based services and applications do not touch a wireless carrier's network. They have no knowledge of the application being used. What we have done is, we have gone back and in effect broadened our guidelines so that they are no longer going to be carrier centric but provide the same touchstones of consumer notice and consent regardless of whether the application runs with a carrier's knowledge or not.

Ms. CASTOR. So I think you stated clearly, you see your responsibility and your membership educating the consumer. Does that need to be something that is promoted in a specific sort of way as we develop new consumer consent provisions?

Mr. ALTSCHUL. I think that is the responsibility for all of the stakeholders, the industry, public policymakers, educators and the like, yes.

Ms. CASTOR. Ms. Collier, could you touch on what are some of the innovations in the arena of emergency services? Are we doing

enough there as the law? Do we need to focus on any specific provisions in updating that?

Ms. COLLIER. Emergency services and helping children be found?

Ms. CASTOR. The children's angle is really your area of expertise.

Ms. COLLIER. Yes.

Ms. CASTOR. Who best on the panel can address whether or not we need updates when it comes to emergency services in relation to LBS? Mr. Morris, go ahead.

Mr. MORRIS. I am always game to try to answer a question. You know, the emergency—and I have actually worked in technical standard-setting bodies on the transition in the emergency system from the old analog system to kind of a new IP-enabled Internet protocol-enabled, system, and the emergency community is very aggressively trying to make that transition but it is a very costly transition, and so I believe, my perception is that the FCC and the emergency community is actually proceeding at a fairly healthy pace to make the transition to IP-enabled emergency services and ultimately, you know, I think that some years from now, a couple of years from now, we really will have the ability to both dial 911 on this device and then take a picture of the auto accident that happened so that the emergency response facility can actually see the situation even before they send their responders. So my perception is that we are in fact making that transition, it is going to be a costly transition because there are lot of public service answering points, PSAPs, that are not currently technically and physically set up to do IP-enabled services like that. But the transition is underway.

Ms. CASTOR. Any other comments on that?

Thank you. I yield back.

Mr. BOUCHER. Thank you, Ms. Castor.

The gentleman from Florida, Mr. Stearns, ranking member on our Telecom Subcommittee, is recognized.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. Morris, I was watching the television back in my office and I saw that the gentleman from Kentucky asked you about jurisdiction and about whether the FCC or the Federal Trade Commission should be involved, and I think your statement was that the jurisdiction for the Internet should be the Federal Trade Commission. Is that what I am to understand you said?

Mr. MORRIS. Well, really, my position would be more that the jurisdiction of a privacy should be at the Federal Trade Commission. Frankly, I would urge that the Internet generally speaking doesn't need to have a designated agency that has broad jurisdiction over it. It really is a success story of non-regulation, and Congress in 1996 in section 230 of the Communications Code really set out its policy of having the Internet grow and develop without regulation.

Mr. STEARNS. All right. Let us assume what you are saying is that the privacy on the Internet—as you know, the FCC now has taken steps to address what they perceive as a problem and they have called it Net neutrality. I call it Net regulation. Based upon what you said dealing with privacy, would you agree with me that perhaps the FCC does not have the jurisdiction to regulate with its promulgating a Net Neutrality under the same assumptions that you made from the gentleman from Kentucky that privacy should

be under the Federal Trade Commission and the FCC has no jurisdiction over it?

Mr. MORRIS. Well, let me——

Mr. STEARNS. Would that be a fair statement?

Mr. MORRIS. No, it wouldn't, Your Honor, if I could—Your Honor——

Mr. STEARNS. I was hoping you would say yes.

Mr. MORRIS. If I could explain, let me answer it by saying that the Internet first grew up in a dial-up world where it rode on top——

Mr. STEARNS. I need you to be concise, so you say no. But let me ask you——

Mr. MORRIS. I think I can offer a one-sentence answer.

Mr. STEARNS. So I am just trying to sort of pigeonhole you here.

Mr. MORRIS. I appreciate that.

Mr. STEARNS. OK. So your argument was, the Internet grew up without regulation, you talked about in 1996, and how the idea was not to have regulation and let it expand without interference. That is what you said. And then you indicated that privacy should be under the Federal Trade Commission rather than the FCC. So would it be fair to say that any type of regulation of the Internet should not come through the FCC?

Mr. MORRIS. I think it is appropriate for the FCC to regulate the underlying telecommunications platform on which the Internet runs.

Mr. STEARNS. Phones, cable, broadcasting but not the Internet itself?

Mr. MORRIS. Not the applications and services that ride on top of——

Mr. STEARNS. OK. That is good enough for us. We appreciate your opinion. Let me follow up. You described a potential risk of location data being stored and used well into the future. Is there harm if the information is not tied to an individual? How often is the identity of the user known to the application provider and what information can an application provider gather about a consumer's identity and his or her habits?

Mr. MORRIS. Well, certainly if information is truly deidentified and anonymized, it presents less concern. But as Professor Cranor noted, there is a unique individual in this world who lives where I live and works where I work and so tracking my location over time could easily be tracked back to me through that. So I do think there are very serious concerns about retaining location over a longer period of time beyond the use that it is first obtained for.

Mr. STEARNS. Professor Cranor, location-based services are still I think in their infancy with their development and we just don't know where it is going to go from here. Would you believe that the federal government should address with regulation some of the new technology concerns that could possibly even hinder the development of future benefits? In other words, if we step in right now, is it a concern of yours that we could actually hinder this infancy type of industry and you might even say in your best mind where this industry will be 10 years from now, 5 years from now.

Ms. CRANOR. So I agree that the industry is in its infancy, and it is somewhat hard to predict where it will be but I would imagine

it will be very different 10 years from now than it is today and probably location-based services will be in much more widespread use. I think there is always a risk of stifling innovation with legislation. On the other hand, I think we do have some serious concerns, and rather than waiting 10 years and discovering that we are all in trouble, it would be good to kind of set things straight from the beginning and really have systems built with privacy designed in from the beginning. So I would urge you to consider legislating on privacy from the beginning and making that part of a more general privacy framework.

Mr. STEARNS. If you were me and you were doing a privacy bill, what would you suggest as being part of location-based privacy? You are writing the bill now yourself.

Ms. CRANOR. Right. Fortunately, that is not my job but——

Mr. STEARNS. Well, just hypothetically.

Ms. CRANOR. But hypothetically, so I think there probably should be some limits to the use of location data but also I think it is very important to make sure that individuals are fully aware and informed of use of their location data and that there are robust consent experiences available to them.

Mr. STEARNS. So a person could opt out or opt in? What would you prefer?

Ms. CRANOR. I think generally opt in, although I think it depends on what you mean by opt out and opt in in this situation.

Mr. STEARNS. Thank you, Mr. Chairman.

Mr. BOUCHER. Thank you very much, Mr. Stearns.

The gentleman from Maryland, Mr. Sarbanes, is recognized for 5 minutes.

Mr. SARBANES. Thank you very much, Mr. Chairman.

Ms. Collier, I am going to direct these questions to you. I guess you can answer them generally when it comes to privacy and so forth and particularly with respect to location-based services if you want. Would you say that there should be a higher standard of privacy at work when you are dealing with children as opposed to adults just generally speaking?

Ms. COLLIER. Yes, I would, and I think there is a higher standard applied right now with the Children's Online Privacy Protection Act that is being administered by the FTC.

Mr. SARBANES. One of the things that intrigues me is that children are the leading edge of the use of technology these days.

Ms. COLLIER. Some technologies, yes.

Mr. SARBANES. Well, they are the leading edge of use of many technologies that have significant privacy implications. Wouldn't you agree, or not?

Ms. COLLIER. Yes, some technologies that would have privacy implications. You know, they are not big on Twitter, they are not blogging as much anymore. It is a moving target. But, yes, absolutely, privacy is a tremendous consideration where children are concerned.

Mr. SARBANES. I mean, it strikes me that adolescence plus technology is a privacy nightmare in some ways.

Ms. COLLIER. Yes, and that is what I was basically saying in my testimony is that location-based technologies and services are not, you know, a unique problem in this area. Children are constantly

in touch with each other, constantly updating their status, their location with each other regardless of the technology.

Mr. SARBANES. And notification and notice and consent provisions or regimes that are established are also ones that sort of become like quicksand when you are dealing with kids. I mean, for example, Facebook I think has a rule that you have to be 13.

Ms. COLLIER. Right. Facebook complies with COPPA.

Mr. SARBANES. Right. Well——

Ms. COLLIER. There are a lot of kids under 13 who use Facebook.

Mr. SARBANES. Who we kidding?

Ms. COLLIER. Right.

Mr. SARBANES. Yes. So the kids are going on and representing—I guess they have to, I mean, I haven't gone through the process—but representing that they are meeting the standard when everybody knows that they are not. The teachers know. I mean, two-thirds of these classes of 12-year-olds and 11-year-olds, they are all on Facebook. So I guess what I am asking you is, how do we address that issue, which is that to me a lot of the privacy standards and expectations we have is either wishful thinking or it is a kind of wink-and-nod exercise when you lay it against just how compelling and seductive and powerful these technologies are, particularly for young people, and it makes me feel that it is almost futile, not quite perhaps, but to try to establish these things when it comes to protection of kids and privacy standards and other things, and I just ask you to reflect on that for the remainder of my time.

Ms. COLLIER. Well, I completely agree that what we are dealing here largely with is adolescent and child development and behavior, not technology, and that is very, very difficult to regulate. I do think that COPPA is a very important sort of baseline standard and the FTC is currently reviewing, you know, the rules and the enforcement of COPPA, rightfully so, but it does effectively protect children's protection under 13. But regulation is not the solution here. I really believe that consumer education is the solution, and I would love to see more thought given to consumer education and product development teams, that product development teams and the industry would be putting on their parent hats more and that consumer education happens right with product launch or when a product is in beta. There is no substitute for parental care and so consumer education involves both parents and children and it has to come through schools, it has to come—you know, we can't keep these products and services out of children's experience in school either. They are part of 21st century education. And therefore to encourage schools to block social media from school is absurd because you can't teach swimming without a pool and we can't hold back the competitiveness of American education. We have got to get technology into schools and stop giving teachers an excuse not to teach with social and interactive and new media, whatever you want to call it.

Mr. SARBANES. That is a great answer. Thank you.

Mr. BOUCHER. Thank you very much, Mr. Sarbanes.

The gentleman from Indiana, Mr. Buyer, is recognized for 7 minutes.

Mr. BUYER. Ms. Collier, I want to pick up where you just left off. The level of cyber bullying and sexting that is going on right now,

so for you to make a blanket statement that says that, you know, don't take these devices away from kids, I am almost to the point as a parent—my children went through public school. It has gotten so bad, I would probably find a private school that says my children are going to wear a uniform and they are not going to have access to technology like cell phones during school hours, and that is almost to the point where it has gotten.

Ms. COLLIER. That would be the easy way. I have kids in public school too, 12 and 18, and it would be easy just to ban all technology from their lives. But what would that do to them? What would that do their social lives?

Mr. BUYER. I don't believe it is banning it from their lives but it is definitely——

Ms. COLLIER. Within reason?

Mr. BUYER. The cyber bullying is really extraordinary that is going on right now, or how—I won't get into the sexting part of it. Let us just do the cyber bullying for a moment, how they can marginalize, isolate and then destroy someone that is 13 whereby that reputation is everything to them. Also, reputation is everything to us. I mean, if you want to talk about cyber bullying, be a member of Congress and deal with the yahoos that we get to deal with, and I don't mean the Web site either. I mean, we experience cyber bullying all the time.

I am going to pick up on something else Mr. Sarbanes had just said. He is absolutely correct, I believe, about the nightmares that this creates when you put technology in the hands of our children. At the same time, when it comes to privacy, as a parent, my children had limited privacy, and guess what? I have the right as a parent to spy on my children.

Ms. COLLIER. Yes.

Mr. BUYER. I have that right in my oversight to ensure that they are where they said they are going to be.

Ms. COLLIER. Absolutely.

Mr. BUYER. And I will tell you what, I would love to have as a parent the actual location ability on a GPS to know where my children are.

Ms. COLLIER. You can have that.

Mr. BUYER. I know. That is why I am saying. So with regard to this "privacy" so how we have to balance this, Mr. Sarbanes, with regard to how we protect our children from the outside in. At the same time, as a parent, how do we gain access to know what they are doing at all times. And there is a balance. And so when you made this comment about how do we get parents to take an active role and interest in the lives of their children, government isn't going to be able to do that. But you are right when you say about education. You are right, I also believe in corporate responsibility when the products come out. I also believe that our schools, since they are also the guardian of our children while they are gone, also have a social responsibility.

Ms. COLLIER. We have also got to stop scaring the bejeebers out of parents. We have done a very bad job of that. We have had a predator panic in this country for several years, and what that fear does is cause parents to overreact and shut things down rather than communicate with their kids.

Mr. BUYER. But how do we—we can do all the things I just said. This issue on cyber bullying, how do we——

Ms. COLLIER. Cyber bullying is just an electronic extension of bullying so what you are asking me is what do we do about bullying, and that is probably beyond the purview of this hearing but we should all be thinking about that. Bullying is——

Mr. BUYER. But bullying used to be a little more isolated. If they find themselves out at recess, if they find themselves at the gym, if they find themselves at the cafeteria, but now you can be in the classroom, you can be anywhere and you can be cyber bullied at any moment at any time because they make some statement or they make up a scenario and this kid then is tortured, you know, constantly. So it is more aggravated.

Ms. COLLIER. We need to get the schools up to speed on this, so we are working hard at that.

Mr. BUYER. As a parent, my children are now grown but I can tell you, I think the cyber bullying is really getting out of hand. I mean, you can turn on the news and you find that someone has now committed suicide and you discover that they were cyber bullied or some 16-year-old thought it would be cute to send a naked picture to her boyfriend, he then sent that to someone else and she commits suicide. I mean, this technology is also being used in a manner which we never anticipated by individuals who don't completely understand the realm of responsibility. Anyway, I appreciate you having this conversation with me. I yield back.

And thank you, Mr. Sarbanes. You brought up a really good issue.

Mr. BOUCHER. Thank you very much, Mr. Buyer.

We have recorded votes pending on the floor, and I think we probably have time for one more member to propound questions. Mr. Space is next. And then following that, we will need to have a recess. Mr. Doyle, I am sorry——

Mr. SPACE. Well, actually, Mr. Chairman, I am going to pass.

Mr. BOUCHER. Oh, you are going to pass? Well, thank you, Mr. Space. That does help us.

Mr. Doyle, the gentleman from Pennsylvania.

Mr. DOYLE. Thank you, Mr. Chairman, and my apologies for being late. We had several hearings at the same time.

Professor Cranor, welcome to this panel. It is always good to see someone from CMU here and not just because they are in my district, Mr. Chairman, but it is one of the great universities in America, and your work has been very helpful to this committee.

Professor Cranor, tell me, in your testimony you mentioned that Internet users legitimately care about their location privacy but that the current system isn't set up in such a way to give users a good sense of how location-based service providers will use that information nor do most location-based service providers supply users with comprehensive privacy controls and protective default settings, and you add that further additional protections might be necessary. I wonder if you could just elaborate a little bit on what additional protections may be necessary to ensure that we have proper control over location information, and do you think it requires Congress to take any action?

Ms. CRANOR. So I think that we need to start with at least having some guidelines which give more specific guidance about what is acceptable notice to users. You know, the fact that providing notice, you know, buried in the legalese of a privacy policy is not providing adequate notice, and guidance that, you know, saying well, you have privacy but there are exceptions and you have to go read the fine print, those sorts of things are not providing people with adequate notice. You know, as Ms. Collier raised, you know, with Google Buzz, you know, people started using it and had no idea that everything was public and that is a very common thing that we have seen in our research is that people use these services, they think only their friends are seeing their information, only their friends are seeing their location and yet it is being made public. So I think we need at the very least guidelines for the service providers and perhaps actually regulation along those lines as well.

Mr. DOYLE. I mean, what options do consumers really have today for choosing or negotiating their own privacy preferences? I mean, are there technologies available that would let consumers express their own privacy preferences up front where they could say up front this is how I want my information to be used and this is who I want to be able to see it?

Ms. CRANOR. Well, I think in the commercial services today, you can do that to a limited extent so there are some that you can certainly turn off the location sharing. There are some that let you choose between sharing with the public or sharing with a group of designated friends. So there are some controls but they tend to be fairly course grained, and you can't really have your cake and eat it too with most of them. With some of the more experimental systems like our research on Locaccino at CMU, you can actually have much finer-grained controls and so I think it would certainly be possible to give consumers a lot more options and a lot more control but we are not actually seeing that being deployed in commercial services.

Mr. DOYLE. Now, Mr. Morris, I saw you either laughing or smiling so I want to give you a chance to grab the microphone and chime in if you would like.

Mr. MORRIS. I started working in 2001 with the Internet engineering task force on a protocol called GeoPriv, geographic privacy, that attempts to do exactly what you are proposing, attempts to allow users to set the rules to say you can keep my information only for 24 hours and you can't pass it on to anybody else, and there's been some uptake with that technology but unfortunately at the applications layer, the Worldwide Web layer, that technology has not been accepted. We have been working to try to get it implemented at the applications there. So certainly the technology is out there. I frankly think it will take an act of Congress to really get the industry to really try to give users the level of control that you are talking about.

Mr. DOYLE. Mr. Chairman, I know we have votes pending. Thank you for your patience. And to all the panelists, thank you for being here today.

Mr. BOUCHER. Thank you very much, Mr. Doyle, and I want to express appreciation also to each of you. Your testimony has been informative and helpful to us.

The record for this hearing will remain open for a period of time, and there may be questions that members want to submit to you. If you receive those, please reply to them promptly. And we do appreciate your help. This has been very beneficial for us.

This hearing stands adjourned.

[Whereupon, at 12:04 p.m., the Subcommittees were adjourned.]

[Material submitted for inclusion in the record follows:]

STATEMENT
OF
RICK BOUCHER
SUBCOMMITTEE ON COMMUNICATIONS, TECHNOLOGY, AND THE INTERNET
"THE COLLECTION AND USE OF LOCATION INFORMATION FOR COMMERCIAL PURPOSES"

FEBRUARY 24, 2010

Today the Subcommittees on Communications, Technology, and the Internet and Commerce, Trade, and Consumer Protection convene an additional hearing to examine matters of consumer privacy. This hearing will examine the important matter of the privacy of location-based information in an increasingly mobile world. I appreciate the excellent cooperation among Chairman Rush and me, Chairman Waxman, Mr. Barton, Mr. Stearns, Mr. Radanovich and our staffs as the plans for today's hearing progressed.

With the development of cheaper and more efficient location-based technologies, increased use of smart phones, the launch of geolocation-enabled Web browsers,

and the proliferation of location-based applications, consumers everywhere are using thousands of different location-based services and applications that collect and use location data to communicate, socialize, travel, play and shop.

Location-based services may be used to locate family and friends in real time, for navigation and mapping, and to enhance social networking and gaming. Each location-based service or application requires some disclosure of an individual's location information to the service provider, but the degree of that disclosure, as well as the uses, retention, and sharing of an individual's location information, varies.

With no existing comprehensive laws or regulations that address the collection, use, disclosure or retention of location-based information, concerns have been raised about the privacy of location-based information and whether consumers understand what they are sharing, who will use it, and how the information will be used.

Location-based information may be collected and used in different ways. Sometimes wireless carriers provide location-based services, while in other instances they are offered by third-party application providers. These third parties can use a device's GPS capabilities to obtain location information directly, obviating the need to obtain location data from the wireless carrier.

One thing is clear, and that is that the number of devices and services that collect and use real-time location information about individuals will continue to proliferate. I therefore look forward to hearing from our witnesses about how we can best balance the deployment of location-based services with adequate protection of consumers' privacy. For example:

- Should the use of location-based information always require opt-in consent, or is opt-out consent sometimes appropriate?

- Are there services that consumers consider essential to the functioning of wireless devices or applications that require the collection and use of location-based information?

- What, if any, safeguards are in place to ensure that consumers give meaningful consent to the tracking of their location in real time?

I also look forward to hearing about the implications, if any, of current privacy statutes on the collection, use and disclosure of location-based information.

I am also interested to hear what the future of location-based technologies may hold – what new services they may enable and how to accommodate privacy concerns. I look forward to hearing from our distinguished panel about these and other matters. Thank you again to our witnesses for being here today, and I yield back the balance of my time.

Statement of the Honorable Joe Barton
Ranking Member, Committee on Energy and Commerce
"The Collection and Use of Location Information
for Commercial Purposes"
February 24, 2010

Thank you, Mr. Chairman, and thank you for holding this hearing.

I want to commend Chairman Boucher and Chairman Rush, on their efforts on privacy issues, and as co-chair of the Privacy Caucus, I have a particular interest in this topic. Our committee has a long history in this area, and I'm glad we're continuing that. Many companies are now competing by distinguishing themselves on the privacy issue. I think our work on these things have forced the industry to take a good hard look at itself, and they have made some positive changes.

I'm hopeful that we can continue that bipartisanship work. Privacy and data security are important to us all, and there is no

reason we all shouldn't sit down at the same table to draft legislation if we decide that is what is needed. I'm hopeful that when some of us go down Pennsylvania Avenue to the White House tomorrow, that the President, Speaker Pelosi, and Leader Reid have a similar approach to healthcare reform, but I'm not holding my breath.

But today we're focusing on privacy, and specifically the collection of use of information related to where someone is or has been. Many in Silicon Valley and in the technology community see this type of marketing and advertising as the "next big thing." No one is quite sure what business models will develop around this type of data, and how people might make money on it. That is both an exciting and a frightening fact for some.

Almost everyone in this room has a mobile device—if not two—in his or her pocket, purse, or briefcase. And those devices relay information that can pinpoint your exact location. Some

people aren't even aware that it's happening. Others actively participate in it by updating their Facebook page or using Twitter many times a day. In fact, I send out "tweets" about where I'm headed and who I'm meeting with in order to keep my constituents informed.

But what are the "rules of the road" about this information that is being collected, compiled, and used? What best practices is the industry developing? Do these companies have robust privacy policies? Are they giving consumers adequate notice about the use of location information? Are they selling this data?

Additionally, we need to closely examine what current laws there are, and perhaps more importantly, how the current framework may treat 2 companies differently despite the fact that they gather the exact same information in the exact same way. Section 222 of the Communications Act restricts how wireless carriers treat at least some location data, but what if an application

on your cell phone gathers that same data? We shouldn't be creating competitive advantages or disadvantages in the law based simply on different technologies.

If there is a lack of robust consumer education, or a lack of meaningful consumer choice, and if the industry doesn't solve those problems, we may need to step in. Our responsibility is to find the consumer harm here, and through this series of hearing and analysis of the marketplace, we may decide that regulation is needed. But I'll note that this analysis needs to be done. The FCC is talking about regulating the Internet in the form of net neutrality rules, and as far as I can tell they've not shown any evidence of a problem. If the case can be made about regulating the Internet, it is in the area of privacy long before net neutrality.

That said, Mr. Chairman, I look forward to the ongoing debate and discussion, and ideally, it will continue to drive the industry to regulate itself before we have to get involved.

I thank the great panel of witnesses for travelling to be here and for their help in this discussion. I look forward to their testimony.

Thank you, Mr. Chairman, and I yield back.

○