GOING DARK: LAWFUL ELECTRONIC SURVEILLANCE IN THE FACE OF NEW TECHNOLOGIES

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

FEBRUARY 17, 2011

Serial No. 112–59

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://judiciary.house.gov

U.S. GOVERNMENT PRINTING OFFICE

64–581 PDF WASHINGTON : 2011

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

COMMITTEE ON THE JUDICIARY

LAMAR SMITH, Texas, *Chairman*

F. JAMES SENSENBRENNER, JR., Wisconsin
HOWARD COBLE, North Carolina
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
STEVE CHABOT, Ohio
DARRELL E. ISSA, California
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas
JIM JORDAN, Ohio
TED POE, Texas
JASON CHAFFETZ, Utah
TOM REED, New York
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
DENNIS ROSS, Florida
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
JERROLD NADLER, New York
ROBERT C. "BOBBY" SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
MIKE QUIGLEY, Illinois
JUDY CHU, California
TED DEUTCH, Florida
LINDA T. SÁNCHEZ, California
DEBBIE WASSERMAN SCHULTZ, Florida

SEAN MCLAUGHLIN, *Majority Chief of Staff and General Counsel*
PERRY APELBAUM, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*
LOUIE GOHMERT, Texas, *Vice-Chairman*

BOB GOODLATTE, Virginia
DANIEL E. LUNGREN, California
J. RANDY FORBES, Virginia
TED POE, Texas
JASON CHAFFETZ, Utah
TIM GRIFFIN, Arkansas
TOM MARINO, Pennsylvania
TREY GOWDY, South Carolina
SANDY ADAMS, Florida
BEN QUAYLE, Arizona

ROBERT C. "BOBBY" SCOTT, Virginia
STEVE COHEN, Tennessee
HENRY C. "HANK" JOHNSON, JR., Georgia
PEDRO PIERLUISI, Puerto Rico
JUDY CHU, California
TED DEUTCH, Florida
DEBBIE WASSERMAN SCHULTZ, Florida
SHEILA JACKSON LEE, Texas
MIKE QUIGLEY, Illinois

CAROLINE LYNCH, *Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

FEBRUARY 17, 2011

GOING DARK: LAWFUL ELECTRONIC SURVEILLANCE IN THE FACE OF NEW TECHNOLOGIES

THURSDAY, FEBRUARY 17, 2011

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 11:23 a.m., in room 2141, Rayburn House Office Building, the Honorable Tim Griffin (acting Chairman of the Subcommittee), presiding.

Present: Representatives Griffin, Forbes, Gowdy, Adams, Quayle, Conyers, Scott, Johnson, Chu, and Quigley.

Staff Present: (Majority) Richard Hertling, Deputy Chief of Staff; Caroline Lynch, Subcommittee Chief Counsel; Arthur Radford Baker, Counsel; Lindsay Hamilton, Clerk; (Minority) Bobby Vassar, Subcommittee Chief Counsel; Joe Graupensberger, Counsel; and Veronica Eligan, Professional Staff Member.

Mr. GRIFFIN. The Subcommittee will come to order.

Welcome to today's hearing on "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies." I would especially like to welcome our witnesses and thank you for joining us today.

I am joined today by my colleague from Virginia, distinguished Ranking Member of the Subcommittee, Bobby Scott. And I don't see the Chairman emeritus Conyers, but he may join us.

Today's hearing examines the issue of the growing gap between the legal authority and the technological capability to intercept electronic communications. This is known in law enforcement circles as "going dark."

Going dark is not about requiring new or expanded legal authorities. It is about law enforcement's inability to actually collect the information that a judge has authorized. Simply stated, the technical capabilities of law enforcement agencies have not kept pace with the dazzling array of new communication devices and other technologies that are now widely available in the marketplace.

Court-ordered electronic surveillance has long been a valuable tool for effective law enforcement. It is a technique that is used as a last resort, when other investigative techniques have failed or would be likely to fail or would even be too dangerous to try.

The judicial process that must be followed to seek a court order to authorize this type of surveillance is neither easily nor quickly

obtained. There are many layers of review, many facts that must be established, and ultimately, a judge decides if such a technique is warranted.

Once authorized, law enforcement must comply with reporting requirements to the court that issued the order, and there are procedures to protect the privacy rights of innocent parties that may use the communication device at issue. The loss of this investigative technique would be a huge risk to both our public safety and our national security.

Congress initially addressed the growing gap between what law enforcement was legally authorized to intercept and what they were technically capable of intercepting by passing the Communications Assistance for Law Enforcement Act. By clarifying the obligations of the telecommunications industry, this act attempted to close the gap and enable law enforcement to address the electronic surveillance challenges presented by new technologies.

But that was back in 1994. Since then, extraordinary developments in communication technology have yielded new communication devices, new services, and new modes of communication that did not exist or had not fully reached their maximum potential when we first addressed this problem.

CALEA, as it currently exists, does not address the contemporary challenge that law enforcement agencies face when attempting to legally intercept electronic communications.

This issue is not unique to Federal agencies. But many of our State and local agencies may be at an even greater risk of going dark because many of them do not have the financial resources or the expertise to resolve interception problems.

Interception solutions are not cheap, and one size does not necessarily fit all. The competition in the communication industry has yielded a shift from standardized to proprietary technology. This often requires law enforcement agencies to develop individual interception solutions that may or may not work in other instances.

The debate on how best to modernize the law and ensure that our law enforcement agencies do not lose this valuable investigative tool will not be easily resolved. Balancing privacy interests, ensuring continued innovation by the communications industry, and securing networks from unauthorized interceptions must all be a part of the debate, and they will all need to be factored into any solution.

I am particularly interested in hearing about collaboration and information sharing among the various Federal, State, and local law enforcement agencies as they attempt to efficiently find solutions to the interception challenges.

I welcome our witnesses and look forward to hearing their testimony.

I now recognize for his opening statement the Ranking Member of the Subcommittee, Congressman Bobby Scott of Virginia.

Mr. SCOTT. Well, thank you very much, and thank you for holding this hearing.

I am glad to have the hearing today because over the past few months, there have been news reports that new communications technologies are making it more difficult for law enforcement to engage in court-authorized wiretaps. The same reports indicate that

the Administration may be preparing legislation to deal with this issue.

All of this has led to conjecture and speculation about whether or not there is, in fact, a problem, what the scope of the problem may be, and what Congress may be asked to do about it. Today's hearing is constructive because we need information to see what is really going on.

Some communications companies cited in the news reports tell us that they have not been given any specific complaints about their cooperation with law enforcement, and they say they have yet to hear details of any reported problems. So I am pleased that we have two distinguished law enforcement witnesses here today to discuss these matters.

We also have a witness to testify with us today who is not a law enforcement representative, but an engineer with extensive experience in communications technology and who is an expert in the relationship between security and surveillance. I realize that this is the beginning of a discussion about a range of issues, which are likely to include implementation of the CALEA statute, as you have indicated, as well as what law enforcement is currently experiencing.

But I believe at the onset of this discussion, eyes need to be open to all of the considerations involved. There is no way around the fact that any calls for increased surveillance capabilities will have significant implications for technological and economic development, as well as basic privacy concerns. I am glad to hear that we will have a variety of perspectives on these issues from our witnesses today.

I want to make one last comment before concluding my statement, and that is that last week I attended a classified briefing given by the FBI including one of our witnesses today. And I appreciate the opportunity to hear the information that was presented.

But while I think that sometimes it is appropriate for Government officials to discuss classified material in closed sessions, particularly discussions of specific cases, it is critical that we discuss this issue in as public a manner as possible. I do not think that congressional consideration of these issues should rest on arguments made in secret. It would be ironic to tell the American people that their privacy rights may be jeopardized because of discussions held in secret.

So, Mr. Chairman, I look forward to our witnesses today, and thank you for Chairing the hearing.

Mr. GRIFFIN. Thank you.

I now recognize the most recent Chairman emeritus of the Committee, John Conyers of Michigan, for his opening remarks.

Mr. CONYERS. Thank you, Mr. Acting Chairman.

I am happy to be here today to welcome all of the witnesses. And to me, this is a question of building back doors into systems hearing, if we had to give it a nickname. And I believe that legislatively forcing telecommunications providers to build back doors into systems will actually make us less safe and less secure.

I believe further that requiring back doors in all communication systems by law runs counter to how the Internet works and may make it impossible for some companies to offer their services.

And finally, it is my belief that our communication companies must be allowed to innovate without technological constraints if they are to continue to develop products and services that successfully compete with foreign companies.

Now that I have given you my views, I would be eager to hear yours, and I thank you very much, Mr. Chairman.

Mr. GRIFFIN. Thank you.

Without objection, other Members' opening statements will be made a part of the record.

[The prepared statement of Mr. Johnson follows:]

Prepared Statement of the Honorable Henry C. "Hank" Johnson, Jr., a Representative in Congress from the State of Georgia, and Member, Subcommittee on Crime, Terrorism, and Homeland Security

Good morning. I would like to thank the witnesses for being here. I want to begin by applauding the Chairman's efforts in seeking to arm law enforcement with the tools they need.

This hearing will largely focus on the Communications Assistance for Law Enforcement Act, CALEA.

CALEA's purpose is to enhance the ability of law enforcement and intelligence agencies to conduct electronic surveillance by requiring that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment to ensure that they have built-in surveillance capabilities, allowing federal agencies to monitor communications.

In the wake of new technologies, law enforcement, particularly the FBI, has concerns about its inability to conduct court ordered surveillance and refers to this inability as "Going Dark."

Law enforcement would like to extend the CALEA requirement to more communications like Skype, encrypted BlackBerry devices, and social networking sites like Facebook and Twitter.

While it is important to arm law enforcement with the tools they need, we must be mindful of what such an expansion would cost the American people?

Not simply in terms of dollars and cents, but in privacy rights, civil liberties, our national security, innovation and global competitiveness?

In addition to sitting on the Judiciary Committee, I sit on the Armed Services Committee and am very concerned about how expanding CALEA could jeopardize national security, especially cyber security.

As Susan Landau states in her written testimony, we must be careful that the difficulties faced by law enforcement are not solved in a manner that puts U.S. communications at serious risk of being hacked by criminals, non-state actors, or other nations.

It is important that we move with caution when it comes to expanding CALEA. Legislatively forcing telecommunications providers to build back doors into their systems to allow for surveillance by law enforcement may also provide opportunities for hackers and foreign adversaries to gain access to these systems.

Legislatively expanding CALEA could create vulnerabilities in our communications systems that would allow cyber criminals and terrorists to attack us.

Expanding CALEA could also hurt America's competitiveness. Our economic growth depends in large part on the continued expansion of ways we use the Internet. Imposing technological constraints on communications companies may make it more difficult for American companies to develop products and services that successfully compete with other countries.

Expanding CALEA could certainly have some unintended consequences that would be detrimental to our country. We must keep this in mind as we examine this issue.

I look forward to hearing from our witnesses about how we can balance the rights of law enforcement without compromising our national security interests or trampling over the privacy rights of millions of Americans.

Thank you, Mr. Chairman, and I yield back the balance of my time.

Mr. FORBES. Mr. Chairman?

Mr. GRIFFIN. Yes, sir?

Mr. FORBES. Mr. Chairman, could I just take 2 minutes for the Committee?

I just want to recognize a good friend of mine who is here today. We are proud of Chief Marshall. He is the president of the International Association of Chiefs of Police. But near and dear to me, he is the chief of police in Smithfield, Virginia, in Congressman Scott and my home State.

And we are proud of all of our witnesses, but particularly glad to see him. And I just wanted him to know that I have got some amendments on the floor. So I will be slipping in and out, but we are so glad to have you here today.

Thank you, Mr. Chairman. I yield back.

Mr. GRIFFIN. Did he bring any hams with him? [Laughter.]

Mr. FORBES. Mr. Chairman, if he did, they would be the best hams in the world, I will tell you. [Laughter.]

Mr. MARSHALL. If it would help you with your deliberations. [Laughter.]

Mr. GRIFFIN. It might make me go to sleep. Thank you for that.

It is now my pleasure to introduce today's witnesses. Valerie Caproni—is that correct?

Ms. CAPRONI. That is correct.

Mr. GRIFFIN. Oh, great. Ms. Caproni has been a general counsel in the FBI's Office of the General Counsel since 2003. Prior to her work with the FBI, she was regional director of the Pacific Regional Office of the Securities and Exchange Commission. She then became a counsel at the law firm of Simpson, Thacher, and Bartlett, specializing in white-collar criminal defense and SEC enforcement actions.

Ms. Caproni has also previously worked in the U.S. Attorney's Office as an assistant U.S. attorney, chief of special prosecutions, and chief of the Organized Crime and Racketeering Section, and as chief of the Criminal Division.

Ms. Caproni received her bachelor of arts in psychology from Newcomb College of Tulane University—I am a Tulane grad as well—in 1976 and her law degree from the University of Georgia in 1979.

Chief Marshall is president of the International Association for Chiefs of Police. He has held the position of chief of police in Smithfield for over 18 years and has been in State and local law enforcement for 25 years. Chief Marshall serves as Chairman for the Law Enforcement Date Exchange and sits on the Advisory Policy Board for the FBI's CJIS Division.

Chief Marshall is the past president of the Hampton Roads Chiefs Association and is on the executive board of the Virginia Association of Chiefs of Police.

Chief Marshall received his bachelor of arts in criminology from St. Leo University and his master's in public administration from Old Dominion University. He is a graduate of the FBI National Academy and the Police Executive Leadership Program through the University of Virginia and the Virginia Police Chiefs Foundation.

Susan Landau, Dr. Landau, studies the interplay between privacy, cybersecurity, and public policy for Radcliffe Institute at Harvard University. Prior to her work at the Radcliffe Institute, Dr.

Landau was a distinguished engineer at Sun Microsystems for 12 years.

Before her work at Sun Microsystems, she taught computer science at the University of Massachusetts and Wesleyan University. Dr. Landau is the co-author with Whitfield Diffie of "Privacy on the Line: The Politics of Wiretapping and Encryption." And her book "Surveillance or Security: The Risks Posed by New Wiretapping Technologies" will be published this spring.

Dr. Landau received her bachelor of arts from Princeton University, her master's of science from Cornell University, and her Ph.D. from MIT.

Without objection, the witnesses' statements will appear in the record, put in their entirety. Each witness will be recognized for 5 minutes to summarize their written statement.

The Chair now recognizes Ms. Caproni.

TESTIMONY OF VALERIE CAPRONI, GENERAL COUNSEL, FEDERAL BUREAU OF INVESTIGATION

Ms. CAPRONI. Thank you.

Good morning, Chairman Griffin, Ranking Member Scott, and Members of the Subcommittee. Thank you for the opportunity to testify before you today regarding the problem that we refer to as "going dark."

Most of us are old enough to remember when the world of communications involved a home telephone and an office telephone. In that world, when a court authorized law enforcement to conduct a wiretap, we knew exactly where and how to conduct it.

We placed a device called a "loop extender" on the target's telephone line. That device intercepted the target's telephone conversations, which were then routed to our monitoring plant so we could hear everything said on the telephone and learn the telephone numbers of all incoming and outgoing calls.

Then the world of communications got a little more complicated. The telephone companies started to shift their technology from analog to digital signals, and cell phones became ubiquitous. The phone companies were adding services like call forwarding, call waiting, and three-way calling.

All of that had a negative impact on our ability to conduct authorized wiretaps, and Congress stepped into the breach. In 1994, it passed the Communications Assistance for Law Enforcement, or CALEA.

To ensure that advances in technology would not outstrip law enforcement's ability to conduct court-approved wiretaps, CALEA required telecommunication carriers to develop and deploy intercept solutions in their networks so that when the Government gets a wiretap order, it can actually conduct the authorized surveillance.

Since then, the number of ways in which we communicate has exploded. We still have home office and cell telephones that can be forwarded, put on hold, and make three-way calls. But we also now have home and office email accounts, Twitter accounts, Facebook and MySpace pages, BlackBerrys and Androids, iPhones and iPads.

We can chat, text, and send instant messages. We can video chat. We can upload videos with comments, and we can communicate using an avatar in Second Life.

If all of that is not complicated enough, we can access our accounts from our home desktop computer via cable connection to the Internet or from a laptop that has a wireless connection. We can access our accounts from our office computer, from a computer in the business center of a hotel, and even from an iPad via a Wi-Fi hotspot while drinking no-fat latte at the closest Starbucks.

The advances in our ability to communicate have many advantages, but they also have made it exponentially more difficult for law enforcement to execute court-authorized wiretaps. Over the past several years, the FBI and other law enforcement agencies have increasingly found themselves serving wiretap orders on providers that are not covered by CALEA and, therefore, under no preexisting legal obligation to design into their systems a wiretap capability.

Such providers may or may not have intercept capabilities in place for all of their services. If they have no capability or only limited capability, it takes time to engineer a solution—sometimes days, sometimes months, and sometimes longer.

Potentially critical evidence in intelligence can be lost while the provider designs a solution so that it can isolate to the exclusion of all others the communications of the particular person whose account we are authorized to wiretap and then deliver those communications and only those communications to law enforcement with the relevant metadata.

Our inability to immediately and completely execute court wiretap orders is not limited to new and exotic ways of communicating. Providers that are covered by CALEA and, therefore, required to maintain a solution in their systems are sometimes unable to immediately execute wiretaps.

Sometimes that happens because the company has made changes to its network but did not adjust its intercept solution so that it would still work. Sometimes the problem is that the approved industry standard does not provide the Government all the information it is lawfully authorized to collect.

Whatever the reason, this is a problem that creates national security and public safety risks. The challenge facing us and our State and local counterparts is exacerbated by the fact that there is currently no systematic way to make electronic intercept solutions widely available across the law enforcement community.

Federal, State, and local law enforcement agencies have varying degrees of technical expertise regarding electronic surveillance and lack an effective mechanism for sharing information about existing intercept capabilities. This leads to the inefficient use of scarce technical resources and missed opportunities to leverage existing solutions.

The absence of institutionalized ways to coordinate and share information in this area impedes the deployment of timely, cost-effective intercept capabilities that are broadly available to the law enforcement community. Today's technical advances inure to the great benefit of society, but they create significant challenges to the Government's ability to conduct lawful wiretaps.

We see going dark as a problem with many facets, but they all boil down to this. The combination of carrots and sticks that the

Government has are not working to incentivize industries to develop and maintain adequate intercept solutions for their services.

As a consequence, when a court issues an order authorizing a wiretap, we are not consistently able to execute that order and promptly begin to collect evidence and intelligence. If we continue to be unable to accomplish that which even the most ardent privacy advocates will agree we ought to be able to accomplish—namely, to execute a wiretap order when authorized to do so by a court—then we will be significantly hobbled in achieving our mission of protecting the public safety and national security.

Thank you for the opportunity to address this Subcommittee, and I look forward to answering your questions.

[The prepared statement of Ms. Caproni follows:]

Department of Justice

STATEMENT OF

VALERIE CAPRONI
GENERAL COUNSEL
FEDERAL BUREAU OF INVESTIGATION

BEFORE THE

COMMITTEE ON JUDICIARY
SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

ENTITLED

"GOING DARK: LAWFUL ELECTRONIC SURVEILLANCE IN THE FACE OF NEW TECHNOLOGIES"

PRESENTED

FEBRUARY 17, 2011

Valerie Caproni
General Counsel
Federal Bureau of Investigation
Statement before the House Judiciary Committee
Subcommittee on Crime, Terrorism and Homeland Security
Washington, D.C.
February 17, 2011

GOING DARK: LAWFUL ELECTRONIC SURVEILLANCE IN THE FACE OF NEW TECHNOLOGIES

Good morning, Chairman Sensenbrenner, Ranking Member Scott, and members of the subcommittee. Thank you for the opportunity to testify before you today about how new technology and a rapidly changing communications landscape are eroding the ability of the government to conduct court ordered intercepts of wire and electronic communications.

Introduction

In order to enforce the law and protect our citizens from threats to public safety, it is critically important that we have the ability to intercept electronic communications with court approval. In the ever-changing world of modern communications technologies, however, the FBI and other government agencies are facing a potentially widening gap between our legal authority to intercept electronic communications pursuant to court order and our practical ability to actually intercept those communications. We confront, with increasing frequency, service providers who do not fully comply with court orders in a timely and efficient manner. Some providers cannot comply with court orders right away but are able to do so after considerable effort and expense by the provider and the government. Other providers are never able to comply with the orders fully.

The problem has multiple layers. As discussed below, some providers are currently obligated by law to have technical solutions in place prior to receiving a court order to intercept electronic communications but do not maintain those solutions in a manner consistent with their legal mandate. Other providers have no such existing mandate and simply develop capabilities upon receipt of a court order. In our experience, some providers actively work with the government to develop intercept solutions while others do not have the technical expertise or resources to do so. As a result, on a regular basis, the government is unable to obtain communications and related data, even when authorized by a court to do so.

We call this capabilities gap the "Going Dark" problem. As the gap between authority and capability widens, the government is increasingly unable to collect valuable evidence in cases ranging from child exploitation and pornography to organized crime and drug trafficking to terrorism and espionage – evidence that a court has authorized the government to collect. This gap poses a growing threat to public safety.

Two examples illustrate the Going Dark problem.

Over a two year period ending in late 2009, the Drug Enforcement Administration (DEA) investigated the leader of a major international criminal organization that was smuggling multi-ton shipments of cocaine between South America, the United States, Canada and Europe, and was trafficking arms to criminal organizations in Africa. A confidential source informed the DEA that the leader of the organization was a former law enforcement officer who went to great lengths to utilize communications services that lacked intercept solutions. Through the hard work of the agents and with the assistance of a confidential human source, DEA managed to dismantle the drug trafficking portion of the organization. Unfortunately, it was unable to prosecute the arms trafficking portion of the organization, which operated beyond the reach of law enforcement's investigative tools. In that case, the communications provider lacked intercept capabilities for the target's electronic communications, and the government's other investigative techniques were ineffective in gathering the necessary evidence. As a result, elements of this organization continue to traffic weapons today.

In another example, in 2009, the FBI investigated a child prostitution case involving a pimp who was trafficking in underage girls and producing child pornography. The target used a social networking site to identify victims and entice them into prostitution. The provider of the social networking site did not have a technical intercept solution. Although the agents had sufficient evidence to seek court authorization to conduct electronic surveillance, they did not do so because the service provider did not have the necessary technological capability to intercept the electronic communications. In this case, the FBI was able to build a case against the target and secure his conviction using other investigative techniques, but our inability to intercept certain electronic communications resulted in a weaker case and a lighter sentence than might otherwise have occurred. It also impeded the agents' ability to identify additional potential victims and co-conspirators.

While these examples illustrate the nature of the Going Dark problem, it is important to emphasize a few relevant points.

- The Going Dark problem is not about the government having inadequate legal authority – the legal authorities we have for intercepting electronic communications are adequate. Rather, the Going Dark problem is about the government's practical difficulties in intercepting the communications and related data that courts have authorized it to collect.
- Going Dark has been used to refer to law enforcement's ability to different types of investigative data. As we discuss the Going Dark problem today, we are not focusing on access to stored data. Rather, we are focusing on the interception of electronic communications and related data in real or near-real time. Without the ability to collect these communications in real or near-real time, investigators will remain several steps behind, and leave us unable to act quickly to disrupt threats to public safety or gather key evidence that will allow us to dismantle criminal networks.

- Addressing the Going Dark problem does not require a broadly applicable solution to every impediment that exists to the government's ability to execute a court order for electronic surveillance. There will always be very sophisticated criminals who use communications modalities that are virtually impossible to intercept through traditional means. The government understands that it must develop individually tailored solutions for those sorts of targets. However, individually tailored solutions have to be the exception and not the rule.
- Addressing the Going Dark problem does not require fundamental changes in encryption technology. We understand that there are situations in which encryption will require law enforcement to develop individualized solutions.
- Finally, addressing the Going Dark problem does not require the Internet to be re-designed or re-architected for the benefit of the government. Within the current architecture of the Internet, most of our interception challenges could be solved using existing technologies that can be deployed without re-designing the internet and without exposing the provider's system to outside malicious activity.

Any solution to the Going Dark problem should ensure that when the government has satisfied a court that it has met the legal requirements to obtain an order to intercept the communications of a criminal, terrorist or spy, the government is technologically able to execute that court order in a timely fashion that is isolated to the individual subject to the order. At the same time, efforts to address this problem must do so in a way that strikes a fair balance between the needs of law enforcement and other important interests and values, such as cybersecurity, civil liberties, innovation, and U.S. global competitiveness

Legal Framework

The government conducts court-ordered electronic surveillance of the content of communications pursuant to Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended, and the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended. Title III authorizes the government to obtain a court order to conduct surveillance of wire, oral or electronic communications when it is investigating certain serious, enumerated crimes. FISA similarly relies upon judicial authorization, through the Foreign Intelligence Surveillance Court, to approve similar surveillance directed at foreign intelligence and international terrorism threats. The government obtains court authorization to install and use pen registers and trap and trace devices pursuant to chapter 206 of Title 18, United States Code, and FISA. Such devices reveal dialing, routing, addressing, and signaling information but not the substance, purport, or meaning of communications.

These authorities address privacy and civil liberties interests, commercial interests, and the government's interest in intercepting communications necessary to protect public safety. Indeed, Title III and FISA orders are among the most difficult investigative authorities to obtain and use. Focusing on intercepting phone calls in a criminal case, the investigator must establish, to the satisfaction of a federal district court judge, that there is probable cause to believe the person

whose communications are targeted for interception is committing, has committed or is about to commit one of the specific enumerated felonies, that alternative investigative procedures have failed, are unlikely to succeed or are too dangerous, and that there is probable cause to believe that evidence of the specified felony will be obtained through the surveillance. The application can only be submitted to the court with the approval of a high ranking official of the Department of Justice. After obtaining an intercept order, the investigator is required to minimize the interception of non-pertinent and privileged communications, and to provide the Court with regular progress updates. The court order expires after 30 days. If the government wishes to extend the period of surveillance, it must submit a new application with a fresh showing of probable cause. In short, Title III imposes a rigorous set of requirements designed to ensure that this investigative tool is used only against the most serious criminals and only when other, less intrusive techniques will not be effective to protect the public safety.

From the outset, the government has required some assistance from communications service providers to implement court orders for electronic surveillance. Both Title III and FISA include provisions mandating technical assistance so that the government will be able to carry out activities authorized by the court. For example, Title III specifies that a "service provider, landlord ... or other person shall furnish [the government]... forthwith all ... technical assistance necessary to accomplish the interception . . ." As the communications environment has grown in volume and complexity, technical assistance has proven to be essential for interception to occur. These provisions alone, however, have not been sufficient to enable the government to conduct surveillance in a timely and effective manner.

In the early 1990s, the telecommunications industry was undergoing a major transformation and the government faced an earlier version of this problem. At that time, law enforcement agencies were experiencing a reduced ability to conduct intercepts of mobile voice communications as digital, switch-based telecommunications services grew in popularity. In response, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994. CALEA requires "telecommunications carriers" to develop and deploy intercept solutions in their networks to ensure that the government is able to intercept electronic communications when lawfully authorized. Specifically, it requires carriers to be able to isolate and deliver particular communications, to the exclusion of other communications, and to be able to deliver information regarding the origination and termination of the communication (also referred to as "pen register information" or "dialing and signaling information"). CALEA regulates the capabilities that covered entities must have and does not affect the process or the legal standards that the government must meet in order to obtain a court order to collect communications or related data.

While CALEA was intended to keep pace with technological changes, its focus was on telecommunications carriers that provided traditional telephony and mobile telephone services; not Internet-based communications services. Over the years, through interpretation of the statute by the Federal Communications Commission, the reach of CALEA has been expanded to include facilities-based broadband internet access and Voice over Internet Protocol (VoIP) services that are fully inter-connected with the public switched telephone network. Although that expansion of coverage has been extremely helpful, CALEA does not cover popular Internet-based communications modalities such as webmail, social networking sites or peer-to-peer services.

At the time CALEA was enacted, the focus on traditional telecommunications services made sense because Internet-based and wireless communications were in a fairly nascent stage of development and digital telephony represented the greatest challenge to law enforcement. However, as discussed below, due to the revolutionary expansion of communications technology in recent years, the government finds that it is rapidly losing ground in its ability to execute court orders with respect to Internet-based communications that are not covered by CALEA. Also, experience with CALEA has shown that certain aspects of that law sometimes make it difficult for the government to execute orders even for providers that are covered by CALEA.

Challenges Associated with New Technologies

From a time when there were a handful of large companies that serviced the vast majority of telephone users in the country using fairly standard technology (the situation that existed when CALEA was enacted in 1994), the environment in which court-authorized surveillance now occurs is exponentially more complex and difficult. Since 1994, there has been a dramatic increase in the volume of communications, the types of services that are offered, and the number of service providers. It is no longer the case that the technology involved in communications services is largely standard. Now, communications occur through a wide variety of means, including cable, wireline, and wireless broadband, peer-to-peer and VoIP services, and third party applications and providers – all of which have their own technology challenges. Today's providers offer more sophisticated communications services than ever before, and an increasing number of the most popular communications modalities are not covered by CALEA.

Methods of accessing communications networks have similarly grown in variety and complexity. Recent innovations in hand-held devices have changed the ways in which consumers access networks and network-based services. One result of this change is a transformation of communications services from a straight-forward relationship between a customer and a single CALEA-covered provider (*e.g.* customer to telephone company) to a complex environment in which a customer may use several access methods to maintain simultaneous interactions with multiple providers, some of whom may be based overseas or are otherwise outside the scope of CALEA.

As a result, although the government may obtain a court order authorizing the collection of certain communications, it often serves that order on a provider who does not have an obligation under CALEA to be prepared to execute it. Such providers may not have intercept capabilities in place at the time that they receive the order. Even if they begin actively attempting to engineer a solution immediately upon receipt of the order and work diligently with government engineers, months and sometimes years can pass before they are able to develop a solution that complies with the applicable court order. Some providers never manage to comply with the orders fully.

Even providers that are covered by CALEA do not always maintain the required capabilities and can be slow at providing assistance. Indeed, as with non-CALEA providers, for some CALEA-covered entities, months can elapse between the time the government obtains a court order and surveillance begins. In the interim period, potentially critical information is lost even though a court has explicitly authorized the surveillance.

This failure of some CALEA-covered providers to be able to comply fully with court orders is due in part to the process in CALEA for establishing standards for intercept capabilities that law enforcement agencies have found to be ineffective in practice. CALEA accords industry "safe harbor" from a CALEA enforcement action when they build their solution consistent with published industry standards, regardless of whether or not the standards satisfy CALEA's technical capability requirements or meet the needs of law enforcement. That reality can result in providers developing and maintaining intercept capabilities that do not achieve the goal of actually providing the government the information it is lawfully authorized to collect.

To compound matters, CALEA's enforcement requirements make it very difficult for the government to bring an enforcement action in court against a covered provider. CALEA's enforcement provisions are written in a manner that leaves the government with the choice of pursuing a CALEA enforcement action against a provider or developing the solution that provides us the ability to collect the evidence we need to further our investigation. Placing the mission first, we invariably develop the intercept capability ourselves. Once a solution is developed, we cannot satisfy CALEA's standards for enforcement.

The enforcement mechanisms in Title III and FISA are also difficult to use as an effective lever to encourage providers to develop and maintain lawful intercept solutions. With respect to both providers that are covered by CALEA and providers that are not, the judicial remedy for non-compliance with the technical assistance requirements in Title III and FISA is contempt. A contempt action is practically and legally difficult to pursue and is unlikely to succeed absent a total refusal of cooperation.

Challenges Facing State and Local Law Enforcement

State and local law enforcement agencies also face a serious intercept capabilities gap. For the most part, our state and local counterparts do not enjoy the resources, facilities, experience, technical expertise, and relationships with industry that federal agencies utilize to effectuate electronic surveillance. With a few exceptions, they are largely unable to conduct electronic surveillance of any internet-based communications services.

The challenge facing our state and local counterparts is exacerbated by the fact that there is currently no systematic way to make existing federally developed electronic intercept solutions widely available across the law enforcement community. Federal, state and local law enforcement agencies have varying degrees of technical expertise regarding electronic surveillance and lack an effective mechanism for sharing information about existing intercept

capabilities. This leads to the inefficient use of scarce technical resources and missed opportunities to capitalize on existing solutions. In addition, there are significant communication gaps between law enforcement and the communications industry: law enforcement often lacks information about new communications services offered by providers while providers often lack understanding of the needs of law enforcement. The absence of effective coordination and information sharing impedes the development of timely, cost-effective intercept capabilities that are broadly available to law enforcement across the country.

To help address these issues, the President's fiscal year 2012 Budget requests $15 million to establish a Data Communications Assistance Center (DCAC). The DCAC will leverage the research and development efforts of Federal, State, and local law enforcement with respect to electronic surveillance capabilities, facilitate the sharing of technology between law enforcement agencies, advance initiatives to implement solutions complying with CALEA, and seek to build more effective relations with the communications industry. Due to the immediacy of these issues, DOJ is identifying space and building out the facility now.

Conclusion

The government's consideration of its electronic surveillance challenges must account for the complexity and variety of today's emerging communications services and technologies. This complexity and variety creates a range of opportunities and challenges for law enforcement. On the one hand, increased communications affords law enforcement potential access to more information relevant to preventing and solving crime. On the other hand, the pace of technological change means that law enforcement must update or develop new electronic surveillance techniques on a far more frequent basis, as existing tools will become obsolete quicker than ever before. In this setting, federal law enforcement faces new challenges on an ongoing basis. At the same time, state and local law enforcement agencies, who traditionally have fewer technical resources necessary to perform lawful electronic surveillance, increasingly need to rely upon the federal government to serve as a central source of expertise.

At this time, the Administration does not have a formal position at this time on whether any legislative changes are necessary. However, it is examining a variety of potential solutions that would address various aspects of the Going Dark problem. We look forward to working with Congress to find a solution that restores and maintains the ability of law enforcement agencies to intercept communications and collect related data pursuant to court orders in a manner that protects public safety, promotes innovation, and safeguards civil liberties. Chairman Sensenbrenner, Ranking Member Scott, and members of the Subcommittee, thank you for the opportunity to address this Subcommittee. I look forward to answering your questions.

Mr. GOWDY [presiding]. Thank you, Ms. Caproni.
Chief Marshall?

TESTIMONY OF CHIEF MARK MARSHALL, PRESIDENT, INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

Mr. MARSHALL. Good morning, Mr. Chairman and Members of the Subcommittee.

My name is Mark Marshall, and I serve as the chief of police in Smithfield, Virginia. I also serve as the president of the International Association of Chiefs of Police.

I am here today representing over 20,000 of IACP's members who are law enforcement executives in over 100 countries throughout the world. The majority of our membership, however, is here in the United States.

As my good friend Congressman Forbes indicated, I am from Hampton Roads, Virginia, a smaller jurisdiction there. I have the big-city problems without the big-city resources. And I have got 2 million people sitting on my doorstep.

I am pleased to be here to represent and to discuss the challenges currently confronting the U.S. law enforcement community on electronic surveillance issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our State highways and the streets of our communities each and every day. Very simply, in this day and age with budgets, we are tasked to do more with less.

A great number of those officers also use electronic surveillance as they investigate crimes. Each day, local, State, tribal, and Federal law enforcement agencies use lawful electronic surveillance as a critical tool for enforcing the Nation's laws and protecting the citizens we have the honor to serve. Moreover, electronic evidence is now a routine issue in all crimes and at most crime scenes.

The IACP believes that the lawful interception of voice and data communications is one of the most valuable techniques available to law enforcement in identifying and crippling criminal and terrorist organizations. Understandably, there is an increased volume and complexity of today's communication services and technologies. And the evolution and development of communication devices has had a significant impact on law enforcement's ability to be able to conduct that surveillance, as well as to recover valuable evidence from communication devices.

Additionally, legal mandates and authorities have not kept pace with the changing technology. CALEA or, the Communications Assistance for Law Enforcement Act, for example, does not cover many types of services that are, unfortunately, used routinely by criminals.

The advanced features of today's phones can process more information about where people have been, who they know, who they are calling, what they are texting, pictures they have sent and/or are sending, as well as larger amounts of data than ever before. Information recovered can also produce connections to other media like Facebook and Twitter, contact lists, call histories, calendars, waypoints, and email.

If properly recovered, this sort of stored data on communication devices has great investigative and intelligence value to assist law enforcement with investigations. The proposed center, however, does not attempt to thwart or inhibit social discourse, which is a fundamental piece to democratic societies, not attempting to water down Title III or judicial orders for these electronic intercepts.

Unfortunately, many of the agencies that need to be able to conduct electronic surveillance of real-time communications are on the

verge of going dark because they are increasingly unable to access, intercept, collect, and process wire or electronic communications information when they are lawfully authorized to do so.

This serious intercept capability gap often undercuts State, local, and tribal law enforcement agencies' efforts to investigate criminal activity such as organized crime, drug-related offenses, child abduction, child exploitation, prison escape, and other threats to public safety. This must change.

Law enforcement must be able to effectively use lawful electronic surveillance to combat terrorism and fight crime. Law enforcement needs the Federal Government to generate a uniform set of standards and guidelines to assist in this exploration.

In order for law enforcement to maintain its ability to conduct electronic surveillance, laws must be updated to require companies that provide individuals with the ability to communicate.

In September, the Law Enforcement Executive Forum, comprised of law enforcement executives, including the IACP, released a plan to address the spectrum of issues related to electronic surveillance. This plan was the National Domestic Communications Assistance Center, otherwise known as NDCAC. In the Federal Government, we have to have lots of acronyms.

The proposal calls for a strategy to be created to address issues related to maintaining law enforcement's ability to conduct court-authorized electronic surveillance. The proposal calls on Congress and the Administration to make funding available to establish the center.

The center would leverage the research and development efforts of the law enforcement community with respect to lawful electronic surveillance capabilities. The center would also facilitate the sharing of technology between law enforcement agencies.

I see that my time is up. So let me just wrap this up.

State, local, tribal, and Federal law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism, both in our streets and in the many communications devices available today. But we cannot do it alone. We need the full support, we need the assistance of the Federal Government.

We need clear guidance and regulations on our use of lawful interception of voice and data communications to aid us in successfully investigating and prosecuting the most dangerous of criminals. It is important for the safety of our hometowns, and that will equate to the safety of our homeland.

Thank you.

[The prepared statement of Mr. Marshall follows:]

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

TESTIMONY

Statement of

Chief Mark Marshall

President
International Association of Chiefs of Police

Before the

Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

United States House of Representatives

February 17, 2011

515 N. WASHINGTON STREET
ALEXANDRIA, VA 22314
703-836-6767
WWW.THEIACP.ORG

Good Morning Mr. Chairman and Members of the Subcommittee,

My name is Mark Marshall and I serve as the Chief of Police in Smithfield, Virginia and I also serve as the president of the International Association of Chiefs of Police. I am here today representing over 20,000 of IACP's members who are law enforcement executives in over 100 countries throughout the world. I am pleased to be here this morning to discuss the challenges currently confronting the U.S. law enforcement community on electronic surveillance issues.

In the United States, there are more than 18,000 law enforcement agencies and well over 800,000 officers who patrol our state highways and the streets of our communities each and every day. A great number of those officers also use electronic surveillance as they investigate crimes. Each day, state, local, tribal and federal law enforcement agencies use lawful electronic surveillance as a critical tool for enforcing the nation's laws and protecting the citizens they serve. Moreover, electronic evidence is now a routine issue in all crimes and at most crime scenes.

The IACP believes that lawful interception of voice and data communications is one of the most valuable investigative tools available to law enforcement in identifying and crippling criminal and terrorist organizations. Understandably, there is an increased volume and complexity of today's communication services and technologies. And, the evolution and development of communication devices has had a significant impact on law enforcement's ability to conduct electronic surveillance, as well as to recover valuable evidence from communication devices. Additionally, legal authorities and mandates have not kept pace with changing technology. CALEA or, the Communications Assistance for Law Enforcement Act, for example, does not cover many types of services that are routinely used by criminals.

The advanced features of today's phones can process more information about where people have been, who they know and are calling, what they are texting, pictures they have and are sending, as well as larger amounts of data than ever before. Information

recovered can also produce connections to other media like Facebook and Twitter, contact lists, call history, calendars, GPS waypoints and email. If properly recovered, this sort of stored data on communication devices has great investigative and intelligence value to assist law enforcement with investigations.

Many agencies that need to be able to conduct electronic surveillance of real time communications are on the verge of "Going Dark" because they are increasingly unable to access, intercept, collect and process wire or electronic communications information when they are lawfully authorized to do so. This serious intercept capability gap often undercuts state, local, and tribal law enforcement agencies' efforts to investigate criminal activity such as organized crime, drug-related offenses, child abduction, child exploitation, prison escape, and other threats to public safety.

This must change—law enforcement must be able to effectively use lawful electronic surveillance to combat terrorism and fight crime. Law enforcement needs the federal government to generate a uniform set of standards and guidelines to assist in this exploration. In order for law enforcement to maintain its ability to conduct electronic surveillance, laws must be updated to require companies that provide individuals with the ability to communicate too also provide law enforcement with the ability to lawfully intercept those communications in a timely and cost effective manner.

In September of 2010, the Law Enforcement Executive Forum (LEEF), comprised of law enforcement executives, including many from the IACP, released a plan to address the spectrum of issues related to electronic surveillance and to law enforcement's ability to recover and process data stored on communication devices. This plan, National Domestic Communications Assistance Center (NDCAC) Proposal, calls for a strategy to be created to address issues related to maintaining law enforcement's ability to conduct court authorized electronic surveillance. For instance, to determine if a solution within the law enforcement community exists and promote knowledge-sharing among law enforcement agencies and groups regarding technical, legal, policy, and other issues.

The Proposal also calls on Congress and the Administration to make funding available to establish the National Domestic Communications Assistance Center. The Center would leverage the research and development efforts of the law enforcement community with respect to lawful electronic surveillance capabilities and the ability to obtain communications device information. The Center would also facilitate the sharing of technology between law enforcement agencies. Finally, the Center would partner with industry to develop CALEA-related technical standards for services beyond those already being addressed by the FBI. The IACP fully supports The Proposal.

The IACP believes that carriers must be required to install, deploy and make available to law enforcement a solution to assist with lawfully authorized electronic surveillance of telecommunication services prior to or concurrent with the release of communications products to the public. The IACP also strongly urges that telecommunications carriers provide law enforcement agencies service for cost and not retail value.

The IACP calls on Congress to take into account the National Domestic Communications Assistance Center (NDCAC) Proposal and use the Proposal's recommendations to create a national strategy to assist state, local and tribal law enforcement in addressing the technical developments and issues related to electronic surveillance.

State, local, tribal and federal law enforcement are doing all that we can to protect our communities from increasing crime rates and the specter of terrorism—both in our streets and in the many communications devices available today, but we cannot do it alone. We need the full support and assistance of the federal government and clear guidance and regulations on our use of lawful interception of voice and data communications to aid us in successfully investigating and prosecuting the most dangerous of criminals.

Thank you.

Mr. GOWDY. Thank you, Chief.
Dr. Landau?

TESTIMONY OF SUSAN LANDAU, Ph.D., RADCLIFFE INSTITUTE FOR ADVANCED STUDY, HARVARD UNIVERSITY

Dr. LANDAU. Mr. Griffin and Members of the Committee, thank you very much for inviting me to testify.

I am Susan Landau, a fellow at the Radcliffe Institute for Advanced Study at Harvard University. I am here representing my own opinions and not that of Harvard or any of the other institutions with which I am affiliated.

I have spent, for the last half dozen years and more, time looking at the risks involved when you build wiretapping capabilities into communications infrastructures. And while there are issues in CALEA about security versus privacy and security versus innovation, I am here to talk about security risks in building the surveillance technology in.

A major national security problem facing the United States is cyber exploitation. We have nation states and criminals penetrating systems, finding the files of interest, and downloading them quickly and shipping them out of the country.

This began happening in the early 2000's and has occurred at U.S. military sites, at Government labs, and private industry. Google, Lockheed Martin, NASA, Northrop Grumman, Oak Ridge National Labs, the list goes on.

How serious is the threat? According to Deputy Secretary William Lynn, it may be the most significant cyber threat that the U.S. will face over the long term. In 2003, the FBI reported that industrial espionage cost the U.S. $200 billion. It is many times higher now.

Can wiretapping capabilities built into communications infrastructures be exploited? The answer is, unfortunately, "yes" because wiretapping is an architected security breach.

Let me tell you a story about Vodafone Greece. A CALEA-type switch was built into Vodafone Greece's network, built in by Ericsson. Vodafone Greece didn't want this switch. So it had been turned off. Because they didn't pay for that piece of the switch, they also didn't have auditing capabilities.

The result? A hundred senior members of the Greek government—including the prime minister, the head of the ministry of defense, the ministry of interior—were wiretapped for a period of 10 months until a text message went awry and they discovered the problem with the system.

At Telecom Italia over a period of 10 years, presumably from an insider attack, people using the system—celebrities, politicians, judges, sports figures—were wiretapped for a period of 10 years. Six thousand Italians. That is 1 in 10,000 Italians was wiretapped. Presumably, no large business deal or political arrangement was ever really private.

A Cisco switch made to comply with law enforcement wiretapping standards in Europe was discovered to have mechanisms in it that were designed in such a way that it was easy to spoof the system and evade auditing. When you think about a wiretapping system that can evade auditing, I want to remind you of people like Robert Hanssen, who evaded the auditing systems of the FBI for many years.

If you think about it, when a Lockheed Martin or a Northrop Grumman fails to adequately secure its networks, the cost can be thousands of proprietary files stolen. But if a communications provider, an applications provider, or a switch provider fails to have an adequately secured communications system, that cost occurs over the millions of communications that utilize that switch or application.

It is unlikely that surveillance can be built in securely. In the U.S., there are hundreds of communications providers, many of them very small, with fewer than 100 employees.

Many startups producing new communications applications are similarly small. Putting wiretapping into the mix risks the communications of all their customers.

I want to step back for a moment and talk about cryptography, a fight we had in the 1990's in which the NSA and the FBI opposed the deployment of cryptography through the communications infrastructure. In 1999, the U.S. Government changed its policy.

The NSA has been firmly behind the change of policy, and endorsed a full set of unclassified algorithms to be used for securing the communications network. The NSA obviously believes that in the conflict between communications surveillance and communications security, we need to have communications security.

What needs to happen? I agree that law enforcement has a problem. Law enforcement needs to be more entrepreneurial. Instead of the one-size-fits-all of CALEA, it needs more tailored solutions.

It is already using transactional information. Chief Marshall described all of the information currently available on the PDAs and so on. That was not information available at the time that the wiretap laws were passed.

Transactional information is what enabled us to capture Khalid Sheikh Mohammed, the designer behind September 11th. It enabled us to capture the July 21st bomber who fled from London to Rome. It is what enables U.S. Marshals Service to have cut the time to catch fugitives from an average of 42 days to 2.

I think we should augment the FBI going dark effort. I know that is expensive in a time of financial austerity, but we are going to have to pay for this, and we don't want to pay for it by increasing security risks or threatening innovation.

I agree that with new communications technologies there is a need for law enforcement access to legally authorized surveillance. But let us not do it in a way that makes things more dangerous and unsecures the U.S.

Thanks very much. I would be happy to take questions.

[The prepared statement of Ms.. Landau follows:]

Going Dark:
Lawful Electronic Surveillance in the Face of New Technologies

Testimony of Susan Landau

Fellow, Radcliffe Institute for Advanced Study, Harvard University
February 17, 2011

Mr. Chairman and Members of the Committee:

Thank you very much for the opportunity to testify today on "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies." My name is Susan Landau, and I am currently a fellow at the Radcliffe Institute for Advanced Study at Harvard University. For the last half dozen years I have studied the risks that occur when wiretapping capabilities are embedded in communications infrastructures, and written about them in the *Washington Post, Scientific American*, and elsewhere. My book detailing these dangers, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, has just been published by MIT Press. I am also co-author of *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 1998).[1]

My comments represent my own views, and not those of any of the institutions with which I am affiliated.

Today I want to speak to you about the security threats raised by extending the Communications Assistance for Law Enforcement Act to IP-based communications. The intent of proposals to extend CALEA to IP-based communications is to secure the nation. Rather than doing so, surveillance mechanisms built into communications infrastructure threaten to create serious vulnerabilities for national security and present threats to innovation.

---

[1] Additional biographical information relevant to the subject matter to the hearing: Prior to being at the Radcliffe Institute, I was a distinguished engineer at Sun Microsystems. At Sun I was involved in issues related to cryptography and export control, security and privacy of federated identity management systems, and in developing our policy stance in digital rights management. I serve on the National Research Council Computer Science and Telecommunications Board and on the advisory committee for the National Science Foundation's Directorate for Computer and Information Science and Engineering. I also served for six years on the National Institute of Standards and Technology's Information Security and Privacy Advisory Board and was a member of the Commission on Cyber Security for the 44th Presidency. I hold a PhD in theoretical computer science from MIT.

A Genuine Problem

Law enforcement is entirely correct that it faces a problem. Rapidly changing communications technologies have created complex challenges to legally authorized interception. This problem began with the break-up of AT&T. Rapid innovation coincided with a soaring number of service providers and suppliers of communications technology. Legally authorized interception has only become more complex with the Internet and the rapid innovation in IP-based communications.

At the same time, it is important to realize that advanced telecommunications provide capabilities to law enforcement unexpected at the time the original wiretap statutes were passed. Both CallerID and cell phones have proved remarkably useful to investigators. Location information from cell phones found the main plotter of the terrorist acts on September 11th, Khalid Shaikh Mohammed, one of the July 21st London bombers when he fled to Rome, and has enabled, for example, the U.S. Marshals Service to drop the average time to find a fugitive from forty-two days to two. Transactional data---the who, when, where---of a communication is a very rich source of information for investigators, and can likely be used even more to even greater value. While there is a genuine problem with intercepting some communications, the FBI now has access to more communications, and more metadata about communications, than ever before in history.

Building in Intercept Capability Creates New Security Risks

But if law enforcement has a problem, a solution that expands the Communications Assistance for Law Enforcement Act (CALEA) to new IP-based communications is one that creates new security risks. Building wiretapping into communications infrastructure creates serious risk that the communications system will be subverted either by trusted insiders or skilled outsiders, including foreign governments, hackers, identity thieves and perpetrators of economic espionage. This risk is not theoretical.

For a period of ten months in 2004-2005, over one hundred senior officials of the Greek government, including the prime minister and the heads of the ministries of interior, justice, national defense, were eavesdropped upon as a result of a breach in wiretapping capability built into a switch[2]. We know how it was done.

Vodafone Greece had purchased switches from the Swedish manufacturer Ericcson; these switches are designed to allow lawful interception. Vodafone Greece had not purchased the wiretapping capability. But in an update to the switch, the wiretapping capability was automatically added, though a user interface to allow Vodafone Greece to easily access that capability---and the capability to audit the interception---was not. Intruders modified twenty-nine different blocks of computer code to initiate the wiretapping of the targets, and this added software included a capability for further surreptitious updating. The

---

[2] Vassilis Prevelakis and Diomidis Spinellis, "The Athens Affair," *IEEE Spectrum*, July 2007 at 18-25.

breach was discovered when some texts had gone awry. But while we know how the breach occurred, we do not know who did it.

Meanwhile between 1996-2006, Telecom Italia appears to have suffered an insider attack in which six thousand people were the target of unauthorized wiretaps[3]. The number of people wiretapped is so large that it means at least one in ten thousand Italians was wiretapped---and that **no large business or political deal was ever trnly private**. Massive dossiers were collected on politicians, financiers, businesspeople, bankers, journalists and judges. It appears that the motivation for the interception was monetary, that is, bribes and blackmail, and was instigated by authorized users of the system. The case is still in trial.

In 2010, an IBM researcher, Tom Cross, discovered that a Cisco architecture for IP networks based on standards published by the European Telecommunications Standards Institute for law-enforcement interception was not sufficiently specified and that is was possible to spoof the system[4]. In particular, criminals could fool the system into allowing them to install unauthorized wiretaps. Just as in the Greek Vodafone case, it was possible to bypass the audit mechanisms. Systems based on these standards were already in use.

The FBI itself has not been immune from problems with implementing wiretap systems. The DCS3000 system (previously known as Carnivore) was an FBI system for delivering ISP wiretap and pen register data to bureau investigators. Because the information was to be used both in investigations and prosecutions, the chain of evidence had to be unimpeachable. But DCS3000 used an auditing system that shared user logins and could easily be spoofed. In addition, system auditing depended on an easily forged manual log sheet. The system was highly vulnerable to insider attacks. It was exactly poor auditing mechanisms that allowed Robert Hanssen to check what the FBI knew about him---and here were poor auditing systems being built into FBI wiretapping systems in the mid 2000s.

The problems at Vodafone Greece, Telecom Italia, with the Cisco interception architecture, and at the FBI all occurred against the wider background of increasing national concern over cybersecurity. Wiretapping built into a communications application or switch is an architected security breach. Rather than securing us, such capabilities endanger us.

What Cybersecurity Risks Does the U.S. Face?

At the time, CALEA's passage was sought because of wiretapping's value in fighting against "drug trafficking, organized crime, violent crime, kidnapping, crimes against

---

[3] Piero Colaprico, "Da Telecom dossier sui Ds Mancini parla dei politici,"*La Repubblica* January 26, 2007.

[4] Tom Cross, "Exploiting Lawful Intercept to Wiretap the Internet," Black Hat DC 2010, February 2010.

children, and public corruption."[5] Since then, we have witnessed a dramatic change in both the nature of communication and the nature of the threats against the United States. It is worth taking a small step back in time to put these shifts in context.

In the early days of the Cold War, the Soviet Union spied on the U.S. military, but over time shifted to spying on defense contractors and other parts of U.S. industry, and other nations did also. Not only do enemies of the U.S. spy on us, but our friends do as well, and they share the information with companies in their own countries. For example, as a result of an unknown insider supplying secret corporate research and business plans to the Japanese consulate in San Francisco, Fairchild Semiconductor was badly weakened, and needed U.S. government help to survive a takeover bid by Fujitsu. A 2003 FBI study estimated an annual $200 billion cost to the U.S. economy as a result of economic espionage.

Beginning in this decade, the world shifted in two fundamental ways that substantively changed the nature of this type of industrial espionage; it was made cheaper, and there was a very large customer for the information. The growth of the Internet and computing technology has greatly simplified the ability of spies, especially those at a distance, to get "inside" a company. The other change is China. Well aware of the information infrastructure asymmetry between China and the U.S., China is seeking to use the asymmetry to its advantage. Other nations also exploit our heavy dependence on cyber infrastructure, but China seems particularly active in doing so.

The first public notice of Chinese intrusions into U.S. computers came with the 2004 "Titan Rain" infiltrations of four U.S. defense installations that occurred in the space of eight hours. Using unpatched software to access the military sites, the intruders, who had obviously been "inside" their targets previously, rapidly packed up files of interest and exfiltrated them, first to Taiwan and Korea, then to southern China. Sensitive helicopter and flight-planning software were among the files removed.

Since that time, such cyberexploitations have become constant occurrences, and many U.S. companies and government sites have been targeted. The modus operandi is always the same. Some software vulnerability---unpatched software, a user opening a targeted mail that contains malware (or that directs the user to a site with malware)---allows the intruder in. The intruder spend time carefully studying the site and finding the files of interest. At some point, the intruder efficiently ships out copies. This is carefully done. By the time the corporate or government site becomes aware that there has been an intrusion, it is often too late. The data has been shipped to China. Organizations that have been exploited in this way cut across large swaths of American industry and government, including such leading members as Google, Lockheed Martin, NASA, Northrup Grumman, Oak Ridge

[5] Louis Freeh, Testimony, Joint Hearing of the Technology and Law Subcommittee of the Senate Judiciary Committee and the Civil and Constitutional Rights Subcommittee of the House Judiciary Committee. Subject: wiretapping. Witness: FBI Director Louis Freeh. March 18, 1994.

National Laboratory. Nor is the Department of Defense immune. Major General William Lord, the air force's chief information officer, reported that "China has downloaded 10 to 20 terabytes of data from the NIPRNet, DoD's non-classified IP Router Network."

How serious is this threat? In September 2010, U.S. Deputy Secretary of Defense William Lynn wrote in *Foreign Affairs* that, "Although the threat to intellectual property is less dramatic than the threat to critical national infrastructure, it may be the most significant cyberthreat that the United States will face over the long term. Every year, an amount of intellectual property many times larger than all the intellectual property contained in the Library of Congress is stolen from networks maintained by U.S. businesses, universities, and government agencies."

It is likely that the cost of economic espionage is many times higher than the numbers reported in 2003. U.S. national strength depends not only on military capabilities, but even more fundamentally on economic strength. Cyberexploitations now constitute a very serious national-security threat. Mandating surveillance capabilities in new communications technologies could greatly exacerbate that threat. As Congress considers how to respond to wiretapping needs of law enforcement, it is instructive to consider how the U.S. handled the related cryptography issue in the 1990s.

Mistakes the U.S. Made in the 1990s

The 1990s were the times of the "Crypto Wars," in which the U.S. government[6] effectively controlled the use of strong encryption domestically through export-control regulations. These regulations required an export license for products with strong cryptography[7] if the cryptography was being used to provide confidentiality. The regulations sharply dampened---if not completely closed off---the market for products with strong forms of cryptography. Few companies wanted to produce products that could not be exported, or that could be exported only if they were admittedly less secure than the version sold within the United States. The fear, uncertainty, and doubt surrounding the use of cryptography in systems---and the ability to export the resulting product---meant that developers often eschewed cryptographic solutions. And sometimes products that fell within the regulations could not be exported anyway.

An egregious example was a DNSSEC implementation. DNSSEC is an Internet protocol that helps ensure a user is getting to the right website (e.g., a real Bank of American

[6] In fact the effort to control encryption was entirely through the executive branch. Congress introduced a number of bills to liberalize the cryptographic export-control regulations, and the loosening that occurred in 2000 may have happened partially because of bills being considered in Congress at the time.

[7] Strong cryptography is a sliding term meaning those types of cryptography that are difficult to break with current technology. In the early 1990s, 56-bit DES constituted strong cryptography, but by the end of the decade, a $250,000 special-purpose machine built by the Electronic Frontier Foundation was able to decode a message encrypted with 56-bit DES in a matter of hours, and the system was no longer considered strong.

website and not a spoofed one). The U.S. government thinks the security this provides is a good thing, and has pushed for adoption. Since 2009 all federal civilian agencies are required to deploy it (and the military intends to do the same). But in the 1990s the U.S. policy was confused.

Although export-control regulations were clear that products that used cryptography for authentication purposes---this was the case for DNSSEC---could be exported, when it was pointed out that the same cryptography could also be used for confidentiality purposes, permission to export the DNSSEC product was rescinded. U.S. government actions actively prevented the technology from shipping---a move counterproductive to U.S. security. Such actions meant that engineers and managers were unsure whether products using strong cryptography would be permitted for export---even if they met the rules. Rather than risk wasting time and money, the products were developed without the security measures. The result is that we're still paying for that weak security eleven years after the U.S. government changed its posture on cryptographic export controls, and, with some exceptions, permitted the export of products with strong cryptography. When that change occurred, it happened with the support of the National Security Agency (NSA).

The ultimate result of the export-control policies of the 1990s was a delayed deployment of security measures. The policy was very short sighted, buying the U.S. additional security during part of that decade, but at the cost of long-term insecurity for U.S. computer and communications infrastructure. Let's not repeat it.

It is essential that legal extensions of CALEA to IP-based communications not cause the same problems as the misguided cryptographic export-control regulations of the 1990s.

In this context, it is worth nothing that in 2005 the NSA endorsed a full set of unclassified algorithms that may be used for securing a communications network. Clearly there is a conflict between communications intelligence and communications security---and the NSA is voting on the side of communications security.

Insecurities of Communications

When AT&T was the communications infrastructure, the communications network was centralized. Wiretaps were relatively easy to place---they went in the telephone central office, which held the switch closest to the subscriber---and also relatively easy to protect---for they were placed in the brick buildings that housed these switches. Turning on a wiretap meant having access to the switch. While one could wiretap an individual by placing alligator clips somewhere between the central office and the target's phone, one could not do wholesale wiretapping on a large group of people in that way.

The computer and communications revolution had a profound impact on communications surveillance. This revolution changed the paths through which communications traveled, changing how and where wiretaps could be placed, and changing the delivery mechanism for the surveillance. All of these changed the risks introduced by communications interception.

These same technological changes have also meant that communications surveillance itself creates insecurities. The switches that enable wiretapping allow remote access; this is standard operating procedure and is a CALEA requirement for phone networks. But such remote access can be used by others, and was, in fact, the basis for the illegal Greek Vodafone surveillance. One might expect that communications providers---ISPs, designers of new communications applications---could protect their systems even when wiretapping capabilities are built in, but this is unlikely to be the case. In the U.S., there are hundreds of communications providers, many of them very small (e.g., with fewer than one hundred employees). Companies producing new communications applications are similarly often small (e.g., start-ups with few employees). These providers lack the expertise and capability to fully secure their systems. Building secure software is hard.

Much more information traverses the network than when people communicated by point-to-point telephone calls. This exposure puts the nation at risk. Consider, for example, the fact by studying the queries on influenza-like illnesses, Google Flu Trends was able to spot flu outbreaks two weeks ahead of the Center for Disease Control. However, unless we secure our communication nodes, others can look in too. In 1972, the Soviets were monitoring transmissions between the wheat traders and the U.S. Department of Agriculture, and were able to corner the wheat market because they knew more about our production than the U.S. government did. What if someone were monitoring communications to Google and determined that the U.S. was about to suffer a flu pandemic and used that information to corner the market for the flu vaccine? After all, communications to Google are not typically encrypted and could easily be wiretapped by rogue software at a communications switch.

Electronic Surveillance Policies That Hurt Competitiveness and National Security

As we contemplate new laws for enabling access to authorized surveillance, two things should be clear:

- Communications security should not be weakened by building in backdoors to facilitate surveillance;
- The computer and telecommunications environment should continue to support innovation.

The first is extremely difficult to achieve if laws require that methods be built into the system to accommodate authorized surveillance. By design, interception, legally authorized or not, breaks security. Ensuring that the interception architecture is correctly designed is very difficult. What makes the situation even worse is that failure has a high cost. If a Lockheed Martin or a Northrup Grumman fails to adequately secure its networks, the cost can be thousands of their proprietary files stolen. But if a communications switch or application is inadequately secured, that cost occurs for the

millions of communications that utilize that switch or application.

Proposals have been floated that new Internet communications applications should be "wiretap vetted" prior to deployment. As I have already explained, building surveillance technologies into communications technology is a very risky business. It is very bad for competition. It is also very bad for innovation. One of the remarkable aspects of Internet innovation is how few resources are needed to develop a project. From Facebook, which started in 2004 with a handful of employees, to the newest Google communication application, speak-to-tweet --- a combination of Twitter, Google, and SayNow that enables Twitter messages to be delivered through voicemail (and which was developed over a weekend in January to enable Egyptians to communicate during the time that Egypt cut connections to the Internet), the Internet has enabled innovation to occur rapidly and with a minimum of resources. Two Stanford computer science graduate students with an idea on search, a Harvard undergraduate with a thought about social networking---these are ideas that rapidly and effectively launched technologies and companies in highly competitive environments.

It is important to realize that innovation is not exclusively an American phenomenon; it happens all across the planet. Skype was developed in Estonia for example. Requiring that Internet applications with communications systems---from means anything from speak-to-tweet to Second Life to software supporting music jam sessions---be vetted first will put American innovation at a global disadvantage. For American competitiveness it is critical that we preserve the ease and speed with which innovative new communications technologies can be developed. I do not need to tell you how crucial innovation is to our nation's long-term economic growth and security.

What is the Problem that Needs Solving?

Let me be clear. This is not an argument against wiretapping, which has proved invaluable in cases ranging from Aldrich Ames to Najibullah Zazi. This is an argument against building against building wholesale wiretapping capability into the core of our emerging and highly diverse communications infrastructure. To do so would be needlessly dangerous; it amounts to developing for our enemies capabilities they might not be able to build on their own---and capabilities that they may well use against us.

The critical national-security problem facing computer and telecommunications is not law enforcement's ability to conduct authorized surveillance; it is our lack of cybersecurity. It makes no sense to pursue wiretapping solutions that put U.S. cybersecurity at risk. This does not mean that we should not pursue solutions that enable legally authorized wiretaps, but that **solutions to the current difficulties faced by law enforcement must not be solved in a manner that puts U.S. communications at serious risk of being eavesdropped upon by outside parties, whether criminals, non-state actors, or other nation states.**

The issue is that the FBI and state and local enforcement have, on occasion, run into situations where new communications technologies have thwarted legally authorized

wiretaps. The fundamental question is how we as a society should work to solve the problem. One solution proposed by law enforcement and implemented by CALEA for the public switched telephone network required that these technologies have wiretapping capabilities built into them. As the Greek Vodafone experience showed, that is a dangerous solution. Tom Cross showed how the same type of solution can also be dangerous for IP-based communications networks (such as those currently supporting Voice over IP).

CALEA applied to IP-based communications is a solution answering the wrong question. The issue is not how does law enforcement force the technology to provide wiretapping capability. The issue is how can law enforcement wiretap a communication using new technology? Changing focus enables us to see new solutions.

With the rapid technology innovation occurring in communications, the FBI needs to be entrepreneurial. Rather than making every component of the communications infrastructure vulnerable to intrusion, a lawful wiretapper could install carefully controlled equipment in select places for the specific duration and target of the wiretap---much like the physical taps that used to be placed on individual subscriber lines in a telephone central office.

In the new environment that law enforcement faces, law enforcement needs to be ahead of the game. Currently the FBI and local law enforcement are case-based agencies, and investigators tackle a new communications technology when it turns up in a case. It can be very difficult to develop the correct surveillance technology in time to aid an ongoing investigation. That approach is the wrong way to be doing things.

In particular, the bureau's surveillance skills need to be ahead technologically on new communications systems. The bureau is making these efforts in its "Going Dark" program. That is the right direction to pursue and it should be pursued with even greater vigor. I recommend that the bureau further augment its research arm so that it can learn about new communications technologies as they are being developed and deployed, and so it can determine ways to intercept communications over those technologies when there is legal authorization for an intercept. This is not a new recommendation. This was a recommendation made in 1996 by the National Research Council's report on cryptography policy[8]---a recommendation that was not followed at the time. It is good that the FBI has recently started the Going Dark program. I would like to see that program put a strong emphasis on technologists with advanced communications and communications surveillance training.

It is undoubtedly the case that proposing that the FBI expand a research branch studying new communications and surveillance technologies is a risky suggestion in these difficult economic times. But the fact is that communications interception costs, and if we don't pay one way, we will pay in another. If interception is imposed in a CALEA-like

---

[8] Kenneth Dam and Herbert S. Lin, eds., *Cryptography's Role in Securing the Information Society,* National Academy Press, at 333-335.

manner, the costs shift to communications providers. If interception is done by requiring that developers of new communications technologies work with the government to provide interception capabilities before deploying, the costs shift to the start-ups and developers---and will have high negative impact on innovation. So this proposal of a strengthened research arm may actually be in the end the most cost-effective way of accomplishing what needs to be done. More importantly, it is a way of enabling legally authorized surveillance capabilities without putting U.S. communications systems at risk by designing wiretapping capabilities into them.

Summing Up

Law enforcement has legitimate concerns about its continued ability to wiretap in the face of rapidly innovating communications technologies. But in an increasingly globalized and networked economy and with increasing cyberexploitations aimed at the U.S. government and U.S. industry, expanding surveillance capabilities into communications applications and infrastructure is a dangerous step. Rather than strengthening the U.S., such a direction would create long-term national-security risks. It would provide for our enemies that which they might not be able to build for themselves: a ready-made system for wiretapping U.S. domestic communications.

By augmenting the FBI's research into interception technologies, the U.S. would accomplish several important societal goals:

- We would preserve law enforcement's capability to conduct legally authorized interceptions.
- We would continue to have the U.S. be a welcoming environment for computer and telecommunications innovation.
- We would work towards the goal of increased cybersecurity, rather than undermining it.

I agree that with the new communications technologies, there is a need for law-enforcement access to legally authorized surveillance. But it must be done in a way that does not undermine U.S. values or U.S. national security. If we take the approach that I am proposing, then not only will costs likely be lower---developing technology in a hurry is always likely to cost more---but the protection provided will be better, and most importantly, it will be without the risks coincident without further extending CALEA mandates to the Internet environment.

Thank you very much. I would be happy to take questions.

Mr. GOWDY. Thank you.

Because I am merely keeping the seat warm for my distinguished colleague from the great State of Arkansas, Mr. Griffin, I would call on my equally distinguished colleague from the great State of Virginia, Mr. Scott.

Mr. SCOTT. Thank you.

Ms. Caproni, are you asking for any surveillance authority over and above what you have now—requirement for warrant, probable cause, and all of that?

Ms. CAPRONI. No, we are not. We believe that the authority that we have to conduct court-authorized wiretaps, which appears in Title III as well as in FISA, is more than adequate.

Mr. SCOTT. And when you have a wiretap and the technology doesn't let you listen in, that is the problem we are dealing with, right?

Ms. CAPRONI. Correct. We are dealing with the problem of we have a wiretap order. So a court has authorized us to conduct the surveillance. But when we serve it on the provider, the provider tells us they don't have the ability to isolate our target's communication to the exclusion of all others and deliver them to us in a secure manner.

Mr. SCOTT. And Chief Marshall, good to see you. As indicated, their recommendation that a technological way to get into the conversation be required to be part of cell phones or whatever else. Is that right, Chief Marshall?

Mr. MARSHALL. Yes, sir. I mean, there is so much—there is valuable data that is contained in every—most criminals are using their cell phone in one way, shape, fashion, or form.

Mr. SCOTT. Now, Ms. Landau, if law enforcement can get into a conversation, what would prevent anyone else who is a skilled hacker, what would be the problem for them getting in?

Dr. LANDAU. You want a tailored solution for the problem. So the problem with the case in Vodafone Greece is that the wiretapping capability was built into the switch, and it was easy to go in and turn the switch on instead of off. Not completely trivial, but easy.

And what you want to do, what I am proposing is that it not be built in in a way that decreases the security of all communications.

Mr. SCOTT. Well, how can the law enforcement get into a conversation and a skilled hacker not be able to? Can you construct it in such a way that only law enforcement can listen in and not others?

Dr. LANDAU. That is right. It used to be that you had to go——

Mr. SCOTT. That is right you can, or you can't?

Dr. LANDAU. You can. You can. But you can't have it done in a method that makes it possible to just automatically turn it on remotely, deliver it. You have to make it more specially tailored.

Mr. SCOTT. Is this hard? I mean, Chief Marshall, as he indicated, is from a small city. They don't have a lot of high-tech people sitting around. Is that something that is easy to put together?

Dr. LANDAU. No, it is not easy to put together, which is why I applaud the FBI effort to do much better information sharing with State and local law enforcement. I think that the FBI should be the one taking the lead in developing those capabilities, and doing that information sharing is absolutely crucial.

Mr. SCOTT. Now this back door would be required in domestically produced cell phones, for example. Could we require imported phones to have this same capability?

Dr. LANDAU. I don't want to see a back door. I want to see specially tailored capability, and those are different requirements. We can require what we want about systems sold here. The question is how they can operate here and——

Mr. SCOTT. Well, can a phone, imported phone be hacked into by law enforcement and not hacked into by others?

Dr. LANDAU. It depends on how you do the hacking. And that is really the question. If you build the system in a way that simplifies the hacking and makes it very easy for somebody to get in, and that is the problem with applying CALEA to IP-based communications. It is simply too easy to do that. Then you run into trouble.

Mr. SCOTT. Well——

Dr. LANDAU. So I am arguing for something that is more expensive. But you are measuring the cost of a more expensive tailored solution against the national security cost of risking communications of everybody going through that switch or that application being accessible.

Mr. SCOTT. If we could require this technology be placed in phones that are imported, we could have no ability to require that for phones that are manufactured outside of the United States and reportedly sold outside of the United States?

Dr. LANDAU. That is right. But the question is where you do the tapping. You could do it at the phone. You could do it at the switch. You can do it at many places along the pathway.

In the case of a cell phone, you can do it at a switch. That is how we do it now.

Mr. SCOTT. So if you had an out of the country phone and brought it into the United States, the capability would be in the system, not in the phone itself?

Dr. LANDAU. That is correct.

Mr. SCOTT. And American manufacturers would, therefore, not be at a disadvantage?

Dr. LANDAU. That is correct.

Mr. SCOTT. Mr. Chairman, I yield back.

Dr. LANDAU. But there is currently not a problem typically with wiretapping cell phones. The problem is with IP-based communications.

Mr. GRIFFIN [presiding]. I recognize Mrs. Adams for 5 minutes.

Mrs. ADAMS. Thank you, Mr. Chair.

Ms. Caproni, you have listened to Dr. Landau, and are you concerned at all about her concerns?

Ms. CAPRONI. We share some of the same concerns, and I am little concerned that some of the answers to the questions to Representative Scott may have left a misunderstanding of how we conduct intercepts.

There is no—the attacking of the device or hacking into a device, if we had a court order, is sometimes permitted. That is sometimes the best way to do it. It is not the normal way to conduct a wiretap.

We want the wiretap and the device that conducts the wiretap to be under the control of the provider. So, to that extent, I think Dr. Landau and I may actually agree that we don't want the inter-

cept solution to be somewhere where it can be gotten to by third-party actors.

Mrs. ADAMS. Manipulated.

Ms. CAPRONI. Correct. The lawful intercept solution should be under the control of the provider, and the provider is responsible for security. There is always risk from insiders. That is a risk that companies manage all the time, particularly big communication providers. So they need to manage that risk.

And we will look, obviously, very hard at the issue of the security associated with anything that we propose to deal with this problem. So security is a legitimate concern. I think we may disagree that having a lawful intercept solution under the control of a provider increases that risk in any kind of a material way.

Mrs. ADAMS. Chief, you have heard the concerns, and I preface this by I will tell you I am a past law enforcement officer. And it did send some red flags up to me when I start reading the breaches and everything else and on the security level of it. I would like to hear your opinion.

Mr. MARSHALL. Yes, ma'am. Thank you.

We certainly don't want to circumvent the stringent legal process involved in, one, obtaining those intercepts, whether it is voice and/or data. Again, I think we are, particularly at the local and State level—you know, I represent all of law enforcement. The bulk of our membership is really at the local and State level, and it is where law enforcement actually takes place on a day-to-day basis in this country.

We need a place, particularly for the smaller and mid-sized agencies that don't have the capabilities to be able to go out, to be able to get those tools, to be able to retrieve that data. We need that place that we can make that call, that we would have that one-stop shop, if you would. That would at least, it may not have the information but would at least be able to direct us to be able to get that information.

In terms of, at the same time, I agree with Ms. Caproni's statement that it is—that I think that this is the industry or the provider would have that, and they would only be providing that when you had that lawful intercept order, that judicial order. For us, it is about going dark. It is most of the criminal element are using and exploiting the ability of the communication tools that are out there. They change every day. It is amazing to me.

I waited 2 years to get a Verizon phone. I finally ordered one. Came into the D.C. area last night, turned on the TV, and I found out that they have got the new generation. Generation 5G is now going to be out in June. That is the problem. I have already done my order. So it is too late.

But that is the problem, and that is what we are seeing, that this is just—this changes so quickly.

Mrs. ADAMS. Technology is changing rapidly.

Ms. Caproni, leaving it at the provider, are you at least the least bit concerned that a possibility could arise, and is there a way to check the auditing system, if it is at the provider, so that we don't have a Greece or an Italy?

Ms. CAPRONI. I think the answer to that is yes, and the providers who provide lawful intercept to us also have responsibilities for the

general security of their system. The providers are responsible for making sure that their systems are not being hacked into overall.

Mrs. ADAMS. Correct.

Ms. CAPRONI. As well——

Mrs. ADAMS. But are you aware if any of the systems currently have that switch that they just haven't turned on?

Ms. CAPRONI. I am not sure about the specific switch that Dr. Landau was talking about. She references two instances where that switch has been compromised. I would say that switch has been deployed to literally hundreds of thousands of telephone companies throughout the world.

So two out of hundreds of thousands, that is a balance. We will obviously be looking, though, at security issues.

Mrs. ADAMS. Okay.

Ms. CAPRONI. We are concerned—we would not propose anything to solve this problem that would appreciably change the security situation that exists in our telecommunication or the Internet system.

Mrs. ADAMS. That is what I wanted to hear. Thank you.

Mr. GRIFFIN. Chairman emeritus Conyers is recognized for 5 minutes.

Mr. CONYERS. Thank you, Mr. Chairman.

To our distinguished chief of police and the president of the International Association of Police, you don't have much personal contact with these kinds of issues of cryptography going on, do you?

Mr. MARSHALL. No, sir. We don't have it in terms of the cryptography. We do, however, have the issue surrounding cell phones and being able to extrapolate that data because, as we have found, they are using—anymore it is not even about voice, it is also about texting. It is IM messages. It is all of those things.

Mr. CONYERS. Yes.

Mr. MARSHALL. Those are pieces that we need that would help, would significantly help our crime-fighting capabilities. The unfortunate——

Mr. CONYERS. Okay. Let me get to the point that I am working at. Have you had much contact or experienced problems with Federal or State law enforcement officials seeking to conduct electronic surveillance and you were stymied because you wanted access to encrypted information that was unavailable from the communications service that you were using?

Mr. MARSHALL. Yes, sir. We have, and it happens every day throughout the law enforcement community, an inability for us to be able to retrieve that data. In other words, if I seize a cell phone, I don't have the capabilities—as you well understand, I don't have the capabilities to be able to do it except with some off-the-shelf products that are, frankly, obsolete.

I send it to the State lab. They then have to go do the search to try to find the newest, the latest and greatest tool to be able to get that. Quite often, they come back that they are unable to do it. And that, unfortunately, is something that is happening with my law enforcement colleagues in agencies across this country.

Mr. CONYERS. Dr. Landau, we have all agreed there is a problem here, and it is complicated. It is expensive and could also be very

dangerous to our national security. What would your recommendations as first steps be in terms of dealing with this?

Dr. LANDAU. So I think that Ms. Caproni and I will find that we agree more than we disagree. I think it is imperative that the FBI, which is in a positive to develop solutions to emerging communications technologies, have a very good information-sharing system with State and local law enforcement because they clearly are overwhelmed and cannot manage that on their own.

I think transactional information, which has become much more valuable as emerging technologies come out, should be used even to greater extent than it is at present. And I think the research arm of the going dark program has to be expanded so that the FBI does the same kind of thing that the NSA does, finds out the emerging communications technologies and figures out solutions to the wiretapping before there is a case. So that when the case comes, they are ready with the solution.

And so, I think that we would find we agree quite a bit.

Mr. CONYERS. Well, Ms. Caproni, you are here under I think you have come out from under the cloud that the whole Federal Bureau of Investigation was under the last time you were here, namely, that the IG had found out that you had been abusing the national security letters and that you promised to clean it up.

And my general counsel says that he feels satisfied about it. I don't sound like I am too satisfied about it. But you are here now telling us that and it is being recommended by our own witness that you need more resources to effect this more satisfactory communication with Federal and State law enforcement officials. Is that correct?

Ms. CAPRONI. Congressman, the FBI is always eager to have additional resources. Resources will help, but resources to the FBI standing alone is not going to solve this problem.

The reality is that we have ways and we know how certain intercepts can be done. Our technicians know how to do that. But these systems need to be deployed within the provider's system.

And I think from both the privacy perspective and in kind of real life what you want, you don't really want the FBI crawling around in providers' systems to install the wiretap solution. We want them to develop and deploy the wiretap solution. We think——

Mr. CONYERS. I ask unanimous consent for one additional minute, Mr. Chairman.

Mr. GRIFFIN. Go right ahead.

Mr. CONYERS. Thank you very much.

Well, then that gets us to my back door comments when I started off. Do you recall that I was saying the back door way won't work?

Mr. CAPRONI. Congressman, I actually wrote that down, that you were concerned about building back doors into systems. And let me make one thing clear. The FBI's view is that this is not about back doors into systems.

In fact, quite the contrary. We don't want a back door. What we want is for the provider to isolate the transactions and isolate the communications that the court has authorized us to get and to hand those communications and no others to us through the front door.

Mr. CONYERS. All right. Great.

Ms. CAPRONI. We do not want a back door——

Mr. CONYERS. That sounds good.

Dr. Landau, do you agree or disagree?

Dr. LANDAU. I disagree. It is a bit of word play here. Ms. Caproni said, look, the Telecom Italia and the Vodafone Greece case were only two cases out of thousands of deployed switches.

If it were the President of the United States or the Speaker of the House instead of the prime minister of Greece, would we still be saying only two switches out of thousands deployed? Surely not.

When you build wiretapping capability into an application, when you build it into a switch, you are creating a serious security risk. I would say in light of the cyber exploitations we have been seeing nationally the last half dozen years, that is not a risk we can afford.

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

Mr. GRIFFIN. Thank you.

The Chair recognizes Mr. Gowdy for 5 minutes.

Mr. GOWDY. Thank you, Mr. Chairman.

Ms. Caproni, to those who may misapprehend and fear that you are seeking an expansion of the Bureau's legal authority in this realm, alleviate those fears for them.

Ms. CAPRONI. I will do the best I can. We are not looking for any new authority. We believe that the authority that we have to conduct wiretaps that appears in Title III on the criminal side and in FISA on the national security side are adequate to our needs.

But what we are concerned is that we are losing ground to actually be able to gather the information that we are authorized to gather. For example, Dr. Landau is focusing on and suggests that we should rely more on transactional data. Transactional data is valuable. It is useful to us. It is not the same as the actual conversation, the content of the conversation, which is critically important, again, from both the national security and public safety perspective.

But I would also point out that even gathering transactional data, like PIN register data, which is the most basic information. Who is the telephone calling? Who are the two sides of the communication? Under the J standards that has been adopted by industry, under CALEA, we can't get basic PIN register data.

So while we may know that a telephone is texting, we don't know what the telephone number of each side of the transaction is. Without that very basic information, our investigations are stymied. We need that information in order to keep the public safe.

Mr. GOWDY. Cite for me the specific remedies you are seeking and Congress's authority to grant them to you.

Ms. CAPRONI. Congressman, the Administration is still working on what the solution would be, and we hope to have something that we can work with Congress on in the near future.

Mr. GOWDY. I take it by your title, counsel, that you are legally trained?

Ms. CAPRONI. I am.

Mr. GOWDY. No doubt better than me. So help me with the authority that Congress would have to, as I understand it, dictate to telecommunications companies changes that they have to make.

Ms. CAPRONI. Well, CALEA, which was enacted in 1994, already requires telecommunications companies to have a wiretap solution built into their system. There are some issues with CALEA and some ways that I think with the experience of 16 years with it, it could be improved, and I think that would be part of—conceivably, that would be part of what we would recommend is how to make the CALEA process for those companies that it covers more productive, and it would better accomplish the goal that Congress created in '94.

As to providers that aren't covered by CALEA, I think that is the bigger challenge. And that is where, through the interagency process, there is a lot of discussion about what is the right way to walk the line, which is an important line, between having providers have the ability to execute a wiretap order when it is delivered to them and not squashing innovation and not hurting the competitiveness of U.S. companies.

We have a very active discussion in the interagency about how to walk that line. I think it is going to be something that Congress is going to be incredibly interested in. Is there a way to accomplish these two goals?

I am optimistic that there are ways to incentivize companies to have intercept solutions engineered into their systems that are safe and secure and not make their system more vulnerable to outside attacks while still encouraging the sort of innovation that we have seen in the American market.

Mr. GOWDY. Chief, let me thank you for your service and ask you are there specific instances that you can cite within the confines of an open hearing where you or members of your membership have had investigations thwarted because of inadequacies in our information-capturing systems?

Mr. MARSHALL. Thank you, Congressman.

I don't have specific instances. I have talked to a number of my colleagues around the country who indicate that this happens on almost a daily basis.

I know that we are just inundated with our case logs. We are also—because of the budgets, we have been forced to make reductions. And because of some of those case reductions, when we are trying to do some of these investigations, particularly in terms of retrieval of data that is being stored on phones or other electronic devices, they simply can't do it.

When we send it, for example, in my agency, we send it, we send it to the Virginia State lab, who then contacts the Federal partners, typically the FBI. The problem is, is they also have their own case log. And because of the number of small industry agencies or small providers that are continuing to pop up with the new electronic, what ends up happening is we get the report back that it simply can't be found.

And that happens every day.

Mr. GOWDY. Thank you, Chief.

Thank you, Mr. Chairman.

Mr. GRIFFIN. Mr. Johnson is recognized for 5 minutes.

Mr. JOHNSON. Thank you, Mr. Chairman.

Law enforcement wants us to extend the CALEA requirement to more communications like Skype, encrypted BlackBerry devices,

and social networking sites like Facebook and Twitter. It is important, I believe, that we move with caution when it comes to expanding CALEA, which may also provide opportunities for hackers and foreign adversaries to gain access to these systems.

I have a couple of questions. Number one, how big is the problem, Ms. Caproni, that you are trying to solve? In rough numbers, how many times in the last year did Federal and State law enforcement officials seek to conduct electronic surveillance and were stymied because the communications it wanted to access were encrypted or were unavailable from the communications service that carried them?

And secondly, as you know, governments around the world have recently shown a strong interest in accessing the communications of BlackBerry business users whose emails are currently encrypted with a key not known to BlackBerry's parent company or the wireless carrier or anyone other than the company employing the individual user.

Several countries have threatened to ban the use and sale of BlackBerry devices unless BlackBerry's parent company provides them with intercept capabilities. The ability of American business people to communicate securely, particularly when they travel abroad, is obviously of great importance to our own economic well-being.

If the emails of a U.S. businessman or woman can be monitored by the Saudi, Indian, or Indonesian governments when they travel abroad, we risk losing the intellectual property advantage that is at the very core of our economy. However, if we force BlackBerry's parent company to give U.S. law enforcement agencies intercept capabilities over these business users, it will likely be quite difficult for the company to keep saying no to those other governments.

Is providing U.S. law enforcement agencies with this access worth it if it means that foreign governments will then be able to get the same intercept capabilities in their own countries?

Ms. CAPRONI. So there are several questions in that question. Let me try to take them one at a time.

First, let me start with law enforcement or at least FBI has not suggested that CALEA should be expanded to cover all of the Internet. In fact, the subject of how you would achieve the goal that we are talking about is very actively being discussed in the interagency. That might be a solution. That might not be a solution. So we are not really suggesting that.

But let us turn directly to encryption. Encryption is a problem, and it is a problem that we see for certain providers. It is not the only problem. And if I don't communicate anything else today, I want to make sure that everyone understands that this is a multifaceted problem. And encryption is one element of it, but it is not the entire element.

There are services that are not encrypted that do not have an intercept solution. So it is not a problem of it being encrypted. It is a problem of the provider being able to isolate the communications and deliver them to us in a reasonable way so that they are usable in response to a court order.

Mr. JOHNSON. Well, that is not to minimize, however, the encryption problem.

Ms. CAPRONI. Absolutely not. But what I do want to say is, as we said in the written statement, that we are not looking, and we think this problem—there are individual encryption problems that have to be dealt with on an individual basis.

The solution to encryption that is part of CALEA, which says if the provider isn't encrypting the communications, and so they have the ability to decrypt and give them in the clear, then they are obligated to do that. That basic premise that provider-imposed encryption, that the provider can give us communications in the clear, they should do that.

We think that is the right model. No one is suggesting that Congress should reenter the encryption battles that were fought in the late '90's and talk about sequestered keys or escrowed keys or the like. That is not what this is all about.

For individuals who put encryption on their traffic, we understand that there would need to be some individualized solutions if we get a wiretap order for such persons.

The other thing I would note, and I thought at one point you were referencing the public reports that we do relative to how often encryption is encountered in Title III collection. What we find is that our agents know, for instance, that BlackBerrys are encrypted. So if their target is using a BlackBerry, they are not going to get a Title III order for that.

Title III orders, for those of you who were never AUSAs, Title IIIs are a lot of work to obtain. It requires an awful lot of work from the agent's part, a lot of work on the AUSA's part. They are not going to do that to get a Title III order on a BlackBerry that they know has encrypted traffic, and therefore, they would not be able to get any usable proceeds from that Title III.

So you see very low numbers in terms of the report of the number of times that we encounter encryption. But I think it is because agents, and I think Chief Marshall sort of referenced this, they will see a problem. And agents, rather than just sort of—and police officers, rather than throwing up their hands and saying, "Well, I can't do it," they will figure out another way to get to where they need to go.

And it may not be a Title III. It may be that they will then approach the problem from a different direction because they know that a Title III is simply not going to be productive use of their time.

Mr. JOHNSON. Thank you.

Mr. GRIFFIN. Thank you.

Mr. Quayle is recognized for 5 minutes.

Mr. QUAYLE. Thank you, Mr. Chairman.

Ms. Caproni, I want to go back to the back door issue that we were talking about earlier so that we can just clear up any misconceptions. But as you know, a lot of the public reports say that solving the problem that we have would create the back door to the Internet, where law enforcement would have the key to all communication systems in the U.S.

Is that accurate? Would the Government have direct access to these communication systems?

Ms. CAPRONI. No, that is not accurate. In fact, the way that we execute wiretaps is we go to the provider who is providing the com-

munication service. We serve the order on them. We ask them to isolate the communications and deliver them to us.

To some extent, actually, what Dr. Landau I think is proposing, although it is not entirely clear, that is for the FBI to individually have solutions, that we then deploy the intercept solution throughout the Internet. That is actually a much less privacy protective way of doing an inception.

It is also not as accurate. With packet-switched communications, you have to collect all of the packets or you can't put the message back together. So there would always be the question of where would you deploy the device if we were simply deploying it in the Internet?

It is for that reason that we want to do the collection with the provider. We want to be able to serve our order on the provider, which then puts a third party in the mix. We serve our order on the provider. The provider figures out what account it is, isolates that account and delivers those communications to us and only those communications to us.

So there is no wiretapping of the Internet. It is really just our ability to serve a targeted order on a targeted account on a particular provider.

Mr. QUAYLE. Okay. And with those communications that the Government would be seeking, has a court reviewed and authorized you to obtain those communications? And also could you briefly go through that process so everybody knows how that is done?

Ms. CAPRONI. Absolutely. So looking at a Title III, because that is the authority in a criminal case, the agent and the AUSA have to put together an affidavit that establishes probable cause to believe that the target is engaged in particular criminal activity. They are committing felonies. They are using the targeted facility to commit the felony, that evidence will be—of the felony will be obtained if we intercept their communications.

They also have to show that other investigative techniques have been tried and failed or are too dangerous to use or would likely fail. So this is really a last-resort type of technique.

The court considers that. They issue an order. It lasts only for 30 days. During the period of that 30 days, law enforcement has to report back to the judge to tell the judge how the wiretap is going, what sort of evidence is being collected.

The wiretap itself has to be minimized. So they will do real-time review of the traffic that is coming in. If it is not evidence of a crime so that they are not authorized to keep it, it gets minimized. So they don't keep that information. So they only keep the information that is actually relevant to their investigation, and it is evidence of criminality.

Mr. QUAYLE. Okay. And just so we are brief, so there is no warrantless wiretap?

Ms. CAPRONI. Absolutely not.

Mr. QUAYLE. Okay. And a final question for Chief Marshall. What role does State and local law enforcement play in the research and development of interception solutions? Do you feel that State and locals have had adequate voice in this process to address this issue?

Mr. MARSHALL. Thank you for the question.

Yes, we are putting together and we actually met about a year and a half ago with the FBI and other Federal justice agencies and a significant portion represented at the State and local level to discuss this problem. Because at the State and local level, we don't have the same level of resources, particularly the smaller and mid-sized agencies don't have the same resources to be able to do these.

So we rely on our Federal partners to be able to do it. At the same time, we also know that we are increasingly seeing the difficulty in being able to achieve that. That was why a year and a half ago, when we started meeting, we ended up meeting, looking at the problems, particularly at the State and local level, and coming up with this proposal for the NDCAC.

And the NDCAC actually, its proposed governance—and we are still continuing to work some of that out—but it would have a significant proportion would be relegated at the State and local so that we have that representation, that we have that voice, that we have that ability to be able to share some of the solutions that have been developed by some of—and for the most part, they are usually some of the major metropolitan areas.

But we have that place that we can all put in that we would be able to share those best practices and strategies and also be able to have a voice in this problem. This is a problem for all of law enforcement, not just for the FBI. It is not just for the DEA. This is a problem whether it is a 5-member department or 5,000.

Mr. QUAYLE. All right. Thank you.

Mr. GRIFFIN. Chairman emeritus Conyers is recognized for another question.

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

Dr. Landau, I would like to feel a little bit more comfortable with you commenting on the question of our colleague Mr. Quayle in terms of the back door question that he initially asked. Do you remember what that was?

Dr. LANDAU. If he could restate it, that would be great.

Mr. GRIFFIN. We are playing musical chairs.

Mr. QUAYLE. Oh, great. What was that?

Dr. LANDAU. Restate your back door question.

Mr. QUAYLE. Okay. Basically, would the solutions to the problem that we are talking about actually provide a back door to the Internet where law enforcement could have a key to all communications systems in the U.S.?

Dr. LANDAU. So Ms. Caproni said that I talked about building the wiretapping into the fabric of the Internet, and certainly not. Earlier, I said that I couldn't speak for Harvard, and that is absolutely true. Let me point out that I also can't speak for the NSA.

The NSA has been pushing hard for communications security within the United States. It pushed out in 2005 a set of recommendations on how to secure a communications network using publicly available cryptography developed through the National Institute for Standards and Technology.

It is pushing that land mobile radio be available. Secure, interoperable land mobile radio can be purchased over the counter in a place like Radio Shack, and we know that it is not just local law enforcement and first responders who will be using those systems.

So if the NSA can function in that environment, I would certainly hope that the FBI can learn to function in that environment. I am saying that building wiretapping into a communications infrastructure, whether a switch or an application, building interception into that communications infrastructure is a dangerous model, whether you are Vodafone Greece, Telecom Italia, or the United States.

Thank you.

Mr. CONYERS. Could I give, Mr. Chairman, the representative from the FBI the last word on this in this discussion?

Ms. CAPRONI. I am sorry. On the discussion of whether it is a back door?

Mr. CONYERS. Yes. Just what Dr. Landau just commented on.

Ms. CAPRONI. I think what she is suggesting is that there should be security for information, and we agree with that. I mean, that is not—we are not suggesting that communications should be insecure. We are suggesting that if the provider has the communications in the clear and we have a wiretap order, that the provider should give us those communications in the clear.

But, for example, Google, for the last 9 months, has been encrypting all gmail. So as it travels on the Internet, it is encrypted. We think that is great. But we also know that Google has those communications in the clear, and in response to a wiretap order, they should give them to us in the clear.

Dr. LANDAU. No problem there.

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

Mr. QUAYLE [presiding]. Thank you.

The gentle lady from California, Ms. Chu, is recognized for 5 minutes.

Ms. CHU. Thank you, Mr. Chair.

For Ms. Caproni and Mr. Marshall, today you have described difficulties in gaining assistance from companies in complying with lawful wiretap orders under 18 U.S.C. 2518. Title III orders include a requirement that all providers furnish the applicant forthwith all information, facilities, and technical assistance necessary to accomplish this interception.

Have you pursued contempt motions against any providers who have failed to comply with these lawful orders?

Ms. CAPRONI. Our approach with industry is one of cooperation. So we try to work with the companies to get them to develop a solution that will work.

Our sense has been that it is very difficult on the one hand to be cooperative and to work with a company who tells you we are trying, we are trying to figure out how to do this so that it will work and not interfere with our solution—with our general system, to at the same time be hauling those people into court. It seems to interfere with the cooperative relationship.

So, no, we have not hauled any of these providers into court on an order to show cause why they should not be held in contempt.

Ms. CHU. Mr. Marshall?

Mr. MARSHALL. Yes, ma'am. My answer is a little bit more basic. No, we have not pursued that because we typically do not have any direct involvement. We don't have the involvement directly with industry.

In other words, we are working through our lab or we are working, if it would be a Title III, it would be worked through our Federal partners, whether it is a task force application or something of that nature.

I will say, and I certainly I would stress this, I think that this has to be a partnership with industry. Industry, we want industry to be involved in a collaborative effort to come up with a solution. We understand that certainly there are costs involved, but a piece of this is it also has to be about what is good for public safety and being able to have that ability to be able to keep our crime-fighting capabilities at least up to the level that we have.

Ms. CHU. Ms. Landau, how do you respond to that?

Dr. LANDAU. So I am mystified in some sense by the discussion because while I certainly understand the going dark issue, and I hear the FBI and local law enforcement saying we are having problems, what I am not hearing are specific types of solutions. Ideas were floated last fall about getting rid of peer-to-peer and Skype, getting rid of encryption or making keys required to be stored.

And as we saw in Ms. Caproni's testimony, the written testimony, the FBI is no longer asking for any re-architecting the Internet, no longer asking at least for certain changes on encryption. So I am a little confused.

I understand that there are serious problems, and I agree that the new technologies sometimes do cause those problems. But there aren't concrete suggestions on the table. The only one being better research at the FBI, and I think that is important.

I want to tell a little story, which is a couple of weeks ago when the situation was developing in Egypt and all the communications were cut off with the rest of the world, all the Internet communications, Google sat down with Twitter over a weekend and developed Speak to Tweet.

That was a handful of engineers. You could speak into a call. It could be translated into a Tweet message, and that was a way for the Egyptians to communicate with one another. That is terrific.

I was delighted to see that innovation was happening here. It was happening with a handful of engineers. And that is the way many systems are developed in the U.S., whether you are talking about Google, which started with two engineers at Stanford, or Facebook, with a handful of people at Harvard.

So I don't quite understand what the FBI is pushing for, other than saying we are having a problem. We would like to augment our research arm, which I think is good. We would like industry to deliver things when they have it in the clear.

Industry, when they are capable of delivering it in the clear, should be delivering it in the clear. So, thank you.

Ms. CHU. Okay. Last question. If we do grant the FBI the authority it seeks, will this stop sophisticated criminals and terrorists from encrypting their communication, or will they simply start using communication tools provided by companies or programmers outside the U.S.?

And what do we do when criminals start using secure communication tools provided by developers associated with the WikiLeaks organization, who will ignore requests by U.S. law enforcement agencies?

Ms. CAPRONI. Thank you for that question.

There will always be criminals, terrorists, and spies who use very sophisticated means of communications that are going to create very specific problems for law enforcement. We understand that there are times when you need to design an individual solution for an individual target, and that is what those targets present.

We are looking for a better solution for most of our targets, and the reality is, I think, sometimes we want to think that criminals are a lot smarter than they really are. Criminals tend to be somewhat lazy, and a lot of times, they will resort to what is easy.

And so, long as we have a solution that will get us the bulk of our targets, the bulk of criminals, the bulk of terrorists, the bulk of spies, we will be ahead of the game. We can't have individual—have to design individualized solutions as though they were a very sophisticated target who was self-encrypting and putting a very difficult encryption algorithm on for every target we confront because not every target is using such sophisticated communications.

Ms. CHU. And Dr. Landau, any response?

Dr. LANDAU. Thank you.

So I am glad to hear, actually, the specific issue now of individualized solutions versus better solutions for bulk. And certainly, in some cases, and the one that Ms. Caproni mentioned about getting the unencrypted gmail that gmail obviously has at the other end or you couldn't read your gmail when you logged on, in that case, in that particular architecture, I suspect it is very easy for Google to deliver that mail, and I suspect it does it forthwith.

But we are arguing about the issue of developing individualized solutions for wiretapping versus creating bulk solutions, what the FBI calls better solutions for bulk when we have a national security threat of downloading and exploiting U.S. industry, U.S. military, U.S. national labs, U.S. civilian agencies.

And I don't think we can possibly build into the various communications infrastructures wiretapping solutions that will allow that type of bulk when it is so easy to subvert software and so easy to subvert IP-based solutions.

Thank you.

Mr. QUAYLE. The Chair recognizes the gentleman from Virginia, Mr. Scott, for one additional question.

Mr. SCOTT. Thank you.

I am a little confused. Ms. Caproni, you indicated that you don't want the access through the phone itself, but through the system, which would require—are you looking for real-time access or a copy of conversations?

Ms. CAPRONI. We are looking for—I am sorry. Primarily, what we are talking about here today is real-time interception. Part of what Chief Marshall has talked about is actually information that would not be collected in real time, information that is stored on your cell phone or your smart device, whatever.

But the bulk of what I have been talking about today is electronic surveillance. So capturing the communications in real time.

Mr. SCOTT. And having somebody in the industry go around trying to find this would take obviously someone on company payroll and expense. Who is paying for this expense, and how much is it?

Ms. CAPRONI. So we are responsible, and we are typically billed for the cost of electronic surveillance. So we will reimburse. But they have to have a solution.

So they have to have the ability to find——

Mr. SCOTT. But law enforcement will pay the costs of the finding and making access to the communication?

Ms. CAPRONI. Let me just double check, but I am pretty sure that is right.

Yes.

Mr. SCOTT. And so, that would come out of Chief Marshall's budget?

Ms. CAPRONI. Yes, I am sorry, Chief.

Mr. SCOTT. And does Chief Marshall have to have somebody on staff technologically sophisticated to figure out what to ask for and how to do all this?

Ms. CAPRONI. Well, that actually is an issue is different providers want orders to be worded slightly differently, and that actually is one of the things that we think the NDCAC, or I can't remember what, the DCAC, this center that we are talking about would provide. It would provide the ability to be a single point of contact.

So law enforcement, if they are doing a wiretap, let us say, of an RCN account that they have never done before, we would probably have a relationship with RCN. We would know how the order should be worded. We would know who in the company it should be served on.

So we would provide that intermediary so that every law enforcement agency in the country doesn't have to have that level of expertise. So it could be much more tailored, and they would have one-stop shopping, and we would serve as an intermediary or the center would serve as a useful intermediary between industry and law enforcement.

Mr. QUAYLE. The Chair recognizes the gentleman from Georgia, Mr. Johnson, for one additional question.

Mr. JOHNSON. Thank you, Mr. Chairman.

CALEA's purpose is to require that telecommunications carriers and manufacturers of telecommunications equipment modify and design their equipment to ensure that they have built-in surveillance capabilities, thus allowing Federal agencies to surveille in real time electronically.

And that calls for individualized solutions to communications like Skype or encrypted BlackBerry devices and social networking sites. Am I correct about that? Am I on track?

Ms. CAPRONI. CALEA doesn't cover social networking sites.

Mr. JOHNSON. Okay. All right. But as far as Skype and BlackBerry devices, it is applicable to?

Ms. CAPRONI. So Skype is not a U.S. company. So it is not covered by CALEA, or it may not be covered by CALEA because it is not a U.S. company. The same with REM.

Mr. JOHNSON. Okay. So non-U.S. companies would not be subject to any extension of CALEA. You are seeking—what are you seeking here today? That is really, I think, Ms. Landau's point, and that is my point also. What is it exactly that you would want Congress to do, or are you asking Congress for anything?

Ms. CAPRONI. Not yet.

Mr. JOHNSON. Or did we just simply invite you here to tell us about this?

Ms. CAPRONI. You invited me, and we came. But we don't have a specific request yet. We are still—the Administration is considering—I am really here today to talk about the problem. And I think if everyone understands that we have a problem, that is the first step, and then figuring out how we fix it is the second step.

The Administration does not yet have a proposal. It is something that is actively being discussed within the Administration, and I am optimistic that we will have a proposal in the near future.

Mr. JOHNSON. So you mean I have been worried for the last 24 hours about some legislation or some issue that I could have worried about later, I guess? I am still worried about it.

Ms. CAPRONI. I am sorry to have put you through a sleepless night. I am sure we will have many others once we get a proposal on the table to consider.

Mr. JOHNSON. Well, I will tell you, life becomes so complicated that it is almost impossible to keep from worrying.

Thank you.

Ms. CAPRONI. I agree.

Mr. QUAYLE. I am going to recognize myself for one additional question.

Ms. Caproni, I was just curious. Do you know if the number of court-ordered electronic surveillance have actually gone down or up than the previous years? You don't have to be specific. But do you know if they have gone down or up?

Ms. CAPRONI. I think they are going up a little bit, and the raw numbers may not be as revealing as the sort of services that are being asked for now. So we are seeing more sophisticated and difficult services, like VOIP is coming up more and more in wiretaps.

I think the absolute number of wiretaps may be about the same or going up slightly.

Dr. LANDAU. I actually know the answer, which is that I believe, according to the wiretap report, it has been steadily increasing with perhaps a little bump down in 2009. But a quite steady increase.

What is also increasing quite substantially is the number of PIN register requirements, PIN registers being asked for.

Mr. QUAYLE. Thank you.

Well, I would like to thank our witnesses.

Mr. CONYERS. Mr. Chairman?

Mr. QUAYLE. Yes?

Mr. CONYERS. Before we——

Mr. QUAYLE. Another one?

Mr. CONYERS. Yes, one final question. Is the ACLU correct in worrying about once we start trying to get into this question it is going to spin out of control, and all the things that may have kept Hank Johnson up last night is going to keep all of us up?

I ask Dr. Landau that because there are some up here that say, well, let us help the FBI out, and we will give them the legislation that we think they need. And there are others that say, well, if you do that, you are going to get something much worse back. And there we get into this legislative turmoil.

Dr. LANDAU. Thank you very much for the question.

So I really said I was going to talk about security, but I will take that privacy question. When you make it easy to wiretap, when all you have to do is flip a switch, it becomes much easier for privacy to be violated. So what we saw, and I know this is not the issue being discussed now. But what we saw during 2001 was a single opinion by a single relatively low member of the Department of Justice about warrantless wiretapping.

It was not reviewed by other members of the Department of Justice, and it instituted the warrantless wiretapping. So the point is that when you make it simple to wiretap, when you make it technologically simple to wiretap, it can be abused.

Mr. CONYERS. Thank you, Mr. Chairman, for your generosity.

Ms. CAPRONI. I am sorry. May I respond to that question?

Mr. QUAYLE. Yes. Ms. Caproni, could you please respond to that?

Ms. CAPRONI. Representative Conyers, there are a lot of things that keep me up at night. One thing is the privacy of people who are communicating on the Internet. One is the security of the Internet. FBI is responsible for cyber attacks. We investigate them all the time. The security of the Internet is extremely important to the FBI.

But I also get kept up by worrying that we have got criminals running around that we can't arrest and can't prosecute because we can't actually execute a wiretap order. And that criminal may be a massive drug dealer. They may be an arms trafficker. They may be a child pornographer or a child molester.

Those are things, real-life things that keep us up at night because we need the authority—I am sorry. We have the authority, but we need the actual ability to conduct the wiretap so that we can keep the streets safe.

I worry about things like a Mumbai-style attack where, God forbid, the attackers are using communications modalities that we don't have an intercept solution for.

Mr. CONYERS. So what is a little privacy invasion compared to all those big things that you could or are worrying about, right?

Ms. CAPRONI. Remember, what we are talking about is court-authorized wiretaps. So the privacy of people that are being invaded is only being invaded if an Article III judge has said that probable cause has been established and that the Government has the right to intercept these communications.

Mr. QUAYLE. Well, I would like to thank all of our witnesses—since we are kind of diverging off topic. I want to thank all of the witnesses for their testimony today.

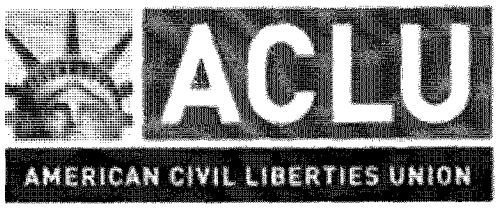
And without objection, all Members will have 5 legislative days to submit to the Chair additional written questions for the witnesses, which we will forward and ask the witnesses to respond as promptly as they can so that their answers may be made part of the record.

Without objection, all Members will have 5 legislative days to submit any additional materials for inclusion in the record.

Mr. SCOTT. Mr. Chairman? Mr. Chairman? I would ask unanimous consent that a statement from the ACLU, the Center for Democracy and Technology, and other industry and privacy advocates be included in the record.

Mr. QUAYLE. Without objection.

[The information referred to follows:]



Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

Before U.S. House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

February 17, 2011

Going Dark: Lawful Electronic Surveillance in the Face of New Technologies

Chairman Sensenbrenner, ranking member Scott and members of the Committee, On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates nationwide, we write to oppose any expansion of the Communication Assistance to Law Enforcement Act (CALEA). The original CALEA law, passed in 1994, was aimed at making surveillance of telephones simpler by building wiretap capacity into every telephone switch network.

While no formal legislative proposal exists, some reports have suggested law expanding this law to the internet and internet communications providers. Such an expansion would raise serious concerns for privacy, innovation and human rights around the globe. Further, evidence in the public record does little to support the need for any expansion.

Background

Details regarding a proposed expansion to CALEA have largely come from two articles in the *New York Times*.[1] The first, dated September 27, 2010, states:

> Federal law enforcement and national security officials are preparing to seek sweeping new regulations for the Internet, arguing that their ability to wiretap criminal and terrorism suspects is "going dark" as people increasingly communicate online instead of by telephone.
>
> Essentially, officials want Congress to require all services that enable communications — including encrypted e-mail transmitters like BlackBerry, social networking Web sites like Facebook and software that allows direct "peer to peer" messaging like Skype — to be technically capable of complying if served with a wiretap order. The mandate would include being able to intercept and unscramble encrypted messages.[2]

The article describes the proposal in more detail as consisting of three related requirements:

- Communications services that encrypt messages must have a way to unscramble them.
- Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts.
- Developers of software that enables peer-to-peer communication must redesign their service to allow interception.[3]

Put another way, this proposal is aimed at requiring companies to re-engineer their communications software so that it has a surveillance backdoor that can be effortlessly accessed by law enforcement. Also, one of the core security protections of the internet – encryption – must be weakened by building in an eavesdropping capacity for a third party who is not privy to the communication.

---

[1] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, NEW YORK TIMES, September 27, 2010.
[2] *Id.*
[3] *Id.*

The scope of such a proposal is striking. A significant percentage of all software designed for the internet is aimed at communicating in some way. Email, instant message, Skype, posts on social networking sites – all are communications methods. Gaming consoles allow conversation among multiple players. Also, less obvious software – like word processing programs that allow log in from anywhere with internet access – can be used to communicate. Encryption is ubiquitous across the web for authenticating the validity and security of communications. Moreover, this is not just a design mandate for the U.S. – foreign governments will certainly demand similar access.

Details in the CALEA articles raise broad concerns.

1. Privacy invasions

The essence of a CALEA expansion would be the building of a surveillance back door into every online communication. A real world analogy helps to explain why this is so problematic. Imagine if the government required every home to be built with cameras and microphones pre-installed. It would provide little reassurance to know that the government would have to get a search warrant to turn those cameras on. We understand intuitively that government surveillance of private activities would be much too easy.

In addition, this proposal would switch the burden for surveillance from the government to companies (and through them to their customers, the American people). Every customer would be paying to have surveillance capability pre-installed and ready to go at a moment's notice. As a practical matter the cost to law enforcement of surveillance has provided real privacy protection by forcing law enforcement to determine if investigations are practical and appropriate uses of resources.

Perhaps most importantly, this proposal is a dramatic expansion of a dangerous idea – that the private sector should be responsible for building the government's surveillance infrastructure. We rely on others – often private companies – to provide the vast majority of services and goods we consume every day. CALEA was an expansion of private sector surveillance to phone service. We have already seen similar problematic expansions of this idea in banking and air travel.[4] The internet is a large and growing presence in our lives – it is deeply troubling to imagine it as the subject of easy and pervasive government scrutiny.

2. Human rights around the world

An expansion of CALEA by the United States would set an international standard. If the U.S. builds backdoors into internet communications devices, other governments – many of them repressive regimes like China and Iran – will want similar access. We have already seen the pivotal role that new technologies like Twitter and Facebook can play in promoting change. Both of these technologies are frequently cited as important ingredients in the Green Revolution in Iran and the recent mass protests in Egypt.

[4] See 49 CFR Parts 1540, 1544 and 1560 (Secure Flight Program Rules) and 31 CFR Part 103 (Financial Crimes Enforcement Network Rules).

In fact, internet freedom is a key objective of U.S. foreign policy. In a January 2010 speech, Secretary of State Hillary Clinton said:

> President Obama held a town hall meeting with an online component to highlight the importance of the internet. In response to a question that was sent in over the internet, he defended the right of people to freely access information, and said that the more freely information flows, the stronger societies become. He spoke about how access to information helps citizens hold their own governments accountable, generates new ideas, encourages creativity and entrepreneurship. The United States belief in that ground truth is what brings me here today.
>
> Because amid this unprecedented surge in connectivity, we must also recognize that these technologies are not an unmitigated blessing. These tools are also being exploited to undermine human progress and political rights. ... And technologies with the potential to open up access to government and promote transparency can also be hijacked by governments to crush dissent and deny human rights.
>
> In the last year, we've seen a spike in threats to the free flow of information. China, Tunisia, and Uzbekistan have stepped up their censorship of the internet. In Vietnam, access to popular social networking sites has suddenly disappeared. ... So while it is clear that the spread of these technologies is transforming our world, it is still unclear how that transformation will affect the human rights and the human welfare of the world's population.[5]

It would be ironic and saddening if these technologies – created and introduced in the United States – were converted from tools for freedom to tools of oppression with the assistance of misguided U.S. policies.

3. Effect on security and innovation

In addition to these core civil liberties concerns, the ACLU believes that the internet is one of the greatest tools for exercising an individual's constitutional rights. Any proposal that threatens the robustness of the internet – as this proposal does – is a matter of significant concern.

A wide array of security experts have stated that any weakening of encryption standards would almost certainly make internet communications less secure. Professor Steven Bellovin of Columbia University recently described the problem very clearly:

> Cryptography, it turns out, is far more complex than one would think. It isn't enough to have an unbreakable cipher; one has to use the cipher precisely correctly, in a stylized exchange of messages known as a cryptographic protocol. If the protocol is designed

[5]Secretary of State Hillary Clinton, *Remarks on Internet Freedom* delivered at the Newseum in Washington DC January 10, 2010. http://www.state.gov/secretary/rm/2010/01/135519.htm

> incorrectly, it's often possible for an attacker to read encrypted messages even if the underlying cipher remains secure.
>
> ...
>
> The administration's proposal would add a third party to communications: the government. This demands a much more complicated protocol. ... Many previous attempts to add such features have resulted in new, easily exploited security flaws rather than better law enforcement access. In other words, instead of helping the government, the schemes created new opportunities for serious misuse. ... The odds on everyone getting this right are exceedingly low; others have created security flaws when trying. [6]

It's not just the government that uses these back doors; they can be exploited by bad actors as well. In 2005 hackers took advantage of a similar law in Greece to hack into mobile communications system and listen to the calls of high government officials including those of the Prime Minister.[7]

The proposal would also substantially stifle innovation. Dozens of new technologies have arisen since 1994 – from instant messaging, to video game systems, to Skype. Today almost any document or technology accessible via the internet allows communications. Imagine if, when all of these technologies were created, each had to comply with law enforcement rules – or, worse, be pre-approved by law enforcement. Many of these technologies might never have gotten off the ground.

4. There is no proof this system is necessary

The number of wiretap orders the government seeks every year is a matter of public record and that record does not support this level of privacy invasion. The 2009 Wiretap Report (which describes all federal, state and local Title III wiretap orders – the only orders at issue here) listed only 32 wiretap orders for computers and only one encrypted communication.[8] In the case of that encrypted communication, law enforcement was able to gain access to the clear text of the communication.[9]

The government already has the legal authority to demand assistance of anyone – from a landlord to an internet service provider – in executing a wiretap order.[10] A company that refused to comply with a lawful Title III order could be held in contempt of court. On its face, this entire, wide-ranging proposal is aimed at easing very few orders in a situation where the

---

[6] Steven Bellovin, *The Worm and the Wiretap*, SMBlog, October 16, 2010. http://www.cs.columbia.edu/~smb/blog/2010-10/2010-10-16.html

[7] Vassilis Prevelakis and Diomidis Spinellis, *The Athens Affair*, IEEE Spectrum, July 2007 http://spectrum.ieee.org/telecom/security/the-athens-affair/0

[8] The Report of the Director of the Administrative Office of the United States Courts on Applications for Orders Authorizing or Approving the Interception of Wire, Oral or Electronic Communications (2009 Wiretap Report), April 2010. See table 6. http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/Table6.pdf

[9] 2009 Wiretap Report pg. 5 http://www.uscourts.gov/uscourts/Statistics/WiretapReports/2009/2009Wiretaptext.pdf

[10] 18 U.S.C. 2511(2)(a)(ii).

government already has substantial power to compel compliance. There must be more effective and less invasive alternatives.

Conclusion

The Obama administration has failed to demonstrate the pressing law enforcement need for such a massive change to our laws. Moreover, the proposal would weaken the internet, stifle innovation, harm privacy, and create major new security vulnerabilities. Because the balance of harms weighs heavily against the proposal and because of the absence of any profound justification for such a change, we urge Congress to reject the Obama administration's proposal to expand CALEA to internet communications devices.

6

Mr. QUAYLE. This hearing is adjourned.
[Whereupon, at 12:50 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

WRITTEN STATEMENT OF SUBSENTIO, INC.

Joel M. Margolis
Senior Regulatory Counsel

Submitted to the U.S. House Committee on the Judiciary
Subcommittee on Crime, Terrorism and Homeland Security

March 28, 2011

Going Dark: Lawful Electronic Surveillance
in the Face of New Technologies

Subsentio, Inc. submits this statement to Chairman Sensenbrenner, ranking member Scott and members of the U.S. House Committee on the Judiciary regarding the hearing titled "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies" (the "Going Dark Proceeding") commenced on February 17, 2011 before the Subcommittee on Crime, Terrorism and Homeland Security (the "Subcommittee").

Subsentio is a trusted third party that partners with communications service providers ("CSPs") and law enforcement agencies ("LEAs") to bring CSPs into compliance with their lawful electronic surveillance obligations while protecting subscriber privacy. Based in Centennial, Colorado, Subsentio specializes in the design, installation, testing, and operation of lawful electronic surveillance solutions for wireline, wireless, Internet, and VoIP service providers nationwide.

Subsentio has nationally-recognized expertise in lawful electronic surveillance, otherwise known as lawful intercept or "LI." For many years Subsentio has served all three of the interests involved in LI: the interest of CSPs and their equipment vendors (collectively, "Industry") in maintaining network control; the interest of LEAs in solving crimes; and the interest of subscribers in communications privacy. Accordingly, Subsentio stands uniquely positioned as an honest broker in the Going Dark debate.

In the Going Dark Proceeding Congress heard testimony representing two opposing views on how the LI process should be controlled. One view included a proposal to require more Industry cooperation for LI. The other was a recommendation to discontinue Industry cooperation for LI.

The following analysis evaluates the LI dispute. Specifically, Subsentio will make the following points:

1. Industry cooperation is needed to deliver effective LI capabilities.
2. Industry cooperation is needed to ensure LI security.
3. Industry cooperation is needed to protect LI subscriber privacy.
4. Industry cooperation in LI should be implemented in the same manner as industry cooperation in similar government mandates.
5. LEA-made LI solutions should be used only in exceptional circumstances.

I. BACKGROUND: THE GOING DARK PROCEEDING REVISITS THE ISSUE OF LI SOLUTION CONTROL

Who should control the development and use of LI technology? For the past 17 years federal law has placed the reins of control primarily in the hands of Industry. CSPs have worked with their equipment vendors to design and build the hardware/software LI solutions and then install the solutions in their networks. When a court issues an order authorizing an LEA and CSP to monitor the communications of a criminal or terrorist suspect, the CSP activates its LI solution to monitor the named suspect for the given LEA. The solution automatically relays copies of the monitored communications to the LEA's monitoring center for the period of time specified in the order (e.g. 30 or 60 days). LEAs have relied primarily on this system of Industry cooperation to serve its LI needs.

LEAs have also devoted significant resources to developing LI solutions of their own. In that scenario the solution is not installed in any one CSP network. Instead it is temporarily attached to one or more networks *ad hoc* as they become subject to LI court orders. In the process, the LEA controls the capabilities and operation of the LI device.

The recently-initiated Going Dark Proceeding is reassessing the issue of LI solution control. In the Proceeding, LEAs have made a two-prong proposal. They seek to improve the existing system of Industry cooperation. At the same time, they want funding to develop their own LI solutions in surveillance cases with exceptionally difficult technical challenges. A computer security expert objects to the LEA proposal. She believes, primarily for reasons of network security, that LEAs should make their own solutions in all LI cases and Industry should have no duty of cooperation. The following explains the existing surveillance law and the two opposing views.

A. The CALEA Mandate

In 1994 Congress enacted the Communications Assistance for Law Enforcement Act ("CALEA"). At the time, LEAs were technically unable to implement certain kinds of LI on advanced networks. The purpose of CALEA was to preserve the ability of LEAs to conduct LI despite evolutions in CSP network technology.

In particular, the statute required mainstream CSPs to equip their networks with hardware/software solutions capable of providing technical support for court-ordered surveillance of criminal suspects who use those networks. The mandate also required CSP equipment vendors to assist the solution development process. Industry was permitted to fashion the solutions as it saw fit, provided the end product could isolate a specific suspect's communications and deliver them in real time to an LEA. The

delivered communications, depending on the court order, would consist of content (e.g. emails, voice calls) and/or the related signaling or transactional information (e.g. who communicated with whom, at what times and dates, and for what durations). Other parts of the statute protected subscriber privacy and prevented the government from ordering CSPs to develop LI capabilities that would interfere with their commercial technologies.

B. The FBI's Going Dark Proposal

In the Going Dark Proceeding, the Federal Bureau of Investigation (the "FBI") urged Congress to update and improve the Industry-focused CALEA statute. Additionally, the FBI requested funding for a National Domestic Communications Assistance Center (the "NDCAC") which would help LEAs develop and share "individually tailored" surveillance technologies of their own in exceptional cases as needed to track "very sophisticated criminals."

The two-pronged Going Dark proposal was described by FBI General Counsel Valerie Caproni in her February 17th Subcommittee testimony, which was accompanied by a written statement of the same date (the "Caproni Statement"). She added that Congress would soon see the Agency's proposed legislation. The FBI proposal was endorsed by the testimony of Chief Mark Marshall, President of the International Association of Chief of Police.

C. Opposition to the Going Dark Proposal

The opposing view at the Going Dark Proceeding was presented by Susan Landau, a Fellow at the Radcliffe Institute for Advanced Study, Harvard University. Ms. Landau is a cyber-security expert and published author on the security risks of lawful surveillance capabilities. Her testimony was also accompanied by a written statement (the "Landau Statement").

The Landau Statement acknowledges that law enforcement faces problems when trying to conduct lawful surveillance on rapidly changing communications technologies. However, Ms. Landau opposes further reliance on CALEA. She believes each time a CSP installs a CALEA solution in its network it creates an "architected security breach," which may be exploited by trusted insiders or skilled outsiders to conduct unauthorized surveillance.

In response to the current challenges of LI, Ms. Landau suggests the FBI should develop its own individualized solutions more proactively and with "greater vigor." She

would not require Industry to cooperate with the FBI to make the solutions because that would have a "high negative impact on innovation." Instead, she says, Industry should focus on keeping its networks as secure as possible.

In summary, the FBI envisions an approach to LI which would continue the policy of Industry cooperation, whereas Ms. Landau says the policy should end.

II. INDUSTRY COOPERATION IS NEEDED TO DELIVER EFFECTIVE LI CAPABILITIES

CSP networks are more complex than ever today. To meet the needs of LI on these networks, LI solutions have likewise grown more complex. Industry has unique technical expertise to address these complexities because Industry engineers know their own networks best. For this reason Subsentio agrees with the FBI that the CALEA framework of Industry cooperation in LI should be updated and improved.

A. The Needs of LI Have Grown More Complex

As explained above, Congress adopted CALEA because it recognized that advanced CSP networks had grown too complex for LEAs to conduct effective LI without Industry assistance. Since CALEA was enacted in 1994, network technology has grown vastly more complex. Today, each network is designed with its own architecture, services, features, and protocols, and these technical elements rapidly evolve. Therefore industry cooperation is needed now more than ever.

The advanced nature of today's CSP networks poses many technical challenges to LI. For example, the increased broadband access speeds that accommodate data-intensive services such as on-line video can bury the data relevant to an LEA investigation and leave LEA collection equipment in the position of drinking from a fire hose. Also, the number of broadband applications for devices such as the Apple iPhone and Google Android has greatly multiplied, overwhelming the ability of LEAs to analyze the ones used by terrorists and criminal suspects. Next, it is more difficult than ever to identify who is using a given broadband service and correlate those suspect identifiers with their related communications. Messaging on social network sites poses its own set of LI challenges because they are not as accountable as traditional email. The international nature of today's IP services further complicates the LI task. Other obstacles are posed by encryption, third-party service platforms, cloud computing, techniques to make suspect communications anonymous, and the uncertainties of conducting an "IP traceback" to learn the origin of Internet packets. The government's

National Broadband Plan, which has expedited the deployment of broadband networks, has spread the above challenges to a larger scale.

B. Industry Engineers Know Best How to Develop LI Solutions for Their Own Networks

To cope with some or all of the above technical challenges, LEAs will need continued cooperation from Industry. A CSP's own engineers and equipment vendors know what LI capabilities are reasonably available in the CSP's particular network and how they can be delivered to an LEA. For example, they know the best places in the network to install the needed intercept access points, how to interpret network data (e.g. the particular string of numbers used in the network to indicate a suspect's handset location), how to correlate a suspect's communications content with the related signaling information, how to deliver the capabilities unobtrusively so the suspect does not become aware of the LI, and how to accomplish the LI without harming the network's commercial features. Much of the information needed to meet the above-listed technical goals is not even available to LEAs because it is proprietary in nature.

As long as each CSP remains responsible for its own network, as required by CALEA, the growing challenges of LI work can remain broadly distributed so that no one CSP or LEA is excessively burdened.

In situations where a CSP lacks expertise in LI engineering or the related needs of law enforcement and privacy, the FCC's rules expressly permit the entity to retain a CALEA trusted third party or "TTP." TTPs have the specialized expertise to make almost any network CALEA compliant.

C. Industry Can Develop LI Solutions in the Most Timely, Cost-Effective Manner

As stated in the Caproni Statement, it can take a long time for an LEA to devise its own LI solution for a network. During that time the suspects under investigation may carry out their criminal or terrorist plots. Equally undesirable, by the time the LEA activates the self-made solution on a given network, the suspects may be gone.

A CSP, by contrast, can leverage its technical expertise and familiarity with its network to develop LI tools more efficiently. The greater efficiency assures that LI solutions are produced in a more timely, cost-effective manner.

D. LEAs Face Disadvantages When Developing LI Solutions

To the extent that the FBI has tried to develop its own LI solutions, the Caproni Statement acknowledges that they have not kept pace with advances in network technology. The FBI has highly trained engineers but lacks the global wealth of proprietary technical expertise available in Industry.

Even if the FBI could develop an adequate LI solution for one type of network, it would be prohibitively difficult for the agency to do so for all the different networks nationwide, let alone modify those solutions fast enough to keep pace with network evolutions. Beyond that, it is unclear how the agency could adequately share the solutions and related training with all the thousands of LEAs nationwide.

An LEA-made solution also poses a risk of network disruption. Such a solution, because it is not built into the network, must be attached hastily to the network upon issuance of court-ordered surveillance. The urgency of the situation forces CSP engineers to divert resources from their commercial functions while they learn the unfamiliar solution, attach it, and configure it in a rush. The last-minute work leaves little time to address issues of network security or subscriber privacy and thus increases the chance of a security or privacy mistake.

Based on the above, the LI burden would be more manageable, timely and cost-effective if each CSP remains responsible for the LI functions of its own network, as CALEA currently requires.

III. INDUSTRY COOPERATION IS NEEDED TO ENSURE LI SECURITY

Ms. Landau asserts that when a CSP installs an LI solution it opens a dangerous "back door" to its network that constitutes an "architected security breach." The implication is that CSP-installed LI solutions are inherently insecure. In Subsentio's view, CSP-installed LI solutions are no more or less inherently insecure than other CSP network elements. Both commercial and non-commercial functionality may be used in a network securely, provided the CSP applies the appropriate technical designs and protocols. Subsentio further believes the needed designs and protocols are best controlled by Industry.

A. Industry Knows Best How to Ensure the Security of Commercial Monitoring Solutions

A CSP network contains a variety of solutions to serve subscribers. Some of the solutions monitor subscriber activity for commercial purposes, regardless of whether the

network happens to include LI capabilities. Among other things, these commercial solutions authenticate users, record their IP transactional logs, identify their handset locations, enable them to roam onto other wireless networks, manage their traffic flows, scan their email content for viruses, and guard against spam.

Each of these commercial solutions raises security concerns. For example, unauthorized employees and non-employees must not have the ability to access a subscriber's IP logs. Accordingly, Industry engineers build security safeguards into the solution designs to prevent unauthorized intrusions. CSPs reinforce the safeguards by adopting best practices, or "protocols," that their employees must follow to ensure that any solution access is authorized and accountable. Industry is best able to handle the security function because each CSP is uniquely familiar with its own security needs.

B. Industry Knows Best How to Ensure the Security of E911 Solutions

The Federal Communications Commission requires certain wireless CSPs to install solutions capable of identifying a subscriber's handset location and transmitting the location data to a public safety answering point ("PSAP") when the subscriber dials the 911 emergency number. The purpose of this "E911" public safety mandate is to help rescue individuals who are in danger but do not know their location or cannot communicate it. Law enforcement has relied on E911 technical cooperation from Industry to save countless lives.

Like commercial solutions, E911 solutions raise security concerns. Unauthorized intruders must not exploit the technology to spy on subscriber locations. Accordingly, Industry has leveraged its unique expertise to adopt technical designs and employee protocols that protect the security of E911 calls. Subsentio is unaware of any instance where an E911 solution has been breached.

The E911 mandate assists LEAs but LEAs do not develop E911 solutions of their own. Theoretically, if the FBI were given tremendous resources, it could devise E911 solutions. But the Agency probably could not do so more efficiently or securely than Industry's own engineers.

C. Industry Knows Best How to Ensure the Security of LI Solutions

A CALEA (built-in) LI solution also monitors subscriber activity. As described above, it can isolate a suspect's communications and relay copies of the data to an LEA monitoring center. Like commercial solutions and E911 solutions, LI solutions raise security concerns. Accordingly, Industry has used its unique expertise to keep LI solutions secure. Subsentio is not aware of any CALEA security breaches in the 17-year history of the statute.

If anything, LI solutions tend to be more secure than other solutions. This is partially due to CALEA, which requires CSPs to meet certain security standards. In addition, the LI functionality in a CSP network typically operates independently of the commercial solutions, thus minimizing the risk that a commercial solution operator will exploit the LI tools. Next, an LI solution is usually installed in a secure location in the network and accessible only with special user access controls. Also, the monitored data is most often transmitted via a secure VPN connection to the LEA monitoring site. Finally, the LI facilities are commonly run by a separate security staff which undergoes criminal background checks, receives special security training, and works under close internal supervision.

The Landau Statement cites two instances where a CSP-installed LI solution was breached: one in Greece and another in Italy. According to Ms. Landau, these intrusions demonstrate that CSP-installed LI solutions are inherently insecure.

Any breach of an LI solution is a serious matter. Unfortunately, so little is known about the LI subversions in Greece and Italy that Ms. Landau was unable to describe any details about the solution designs or the security protocols in force. A defect in either type of safeguard could explain either breach. Neither of the European break-downs can be blamed on CALEA because CALEA applies only in the U.S. In any event, two failures of CSP-installed LI solutions, among the numerous CSP-installed LI solutions worldwide, do not prove such solutions are inherently insecure.

D. LEAs are Not Well-Suited to Ensure LI Security

LEAs lack familiarity with all the different CSP network architectures and security vulnerabilities. As noted above, much of this information is proprietary and therefore unavailable to LEAs. An LEA could try to build security features into a one-size-fits-all LI solution. But the effort would probably not rival the kind of network-specific security analysis conducted by a CSP's own equipment vendor and network engineers. And as noted above, when a one-size-fits-all LEA solution is attached to a CSP network in the rush of an already-issued court surveillance order, there is little time to explore potential security flaws.

An example of a widely-used LEA solution is DCS 3000, also known as "Carnivore." Carnivore is designed to capture suspect data on Internet service provider networks. The Landau Statement expressly criticized Carnivore as insecure. This indicates LEA-crafted solutions are no more secure than those made by Industry.

E. Without Industry Cooperation in LI Security, Industry and LEAs May Work at Cross-Purposes

Ms. Landau's response to the risk of LI security is to discontinue the policy of Industry cooperation in the development and operation of LI solutions. Instead, she would have Industry focus exclusively on network security and let LEAs work alone to develop and use any needed LI tools.

Subsentio questions any LI policy that would have Industry and LEAs work towards divergent goals. If Industry focuses on network security without regard to the needs of LI, Industry and LEAs may work at cross-purposes, with CSPs increasingly strengthening their network security as LEAs persistently try to overcome it. In such a struggle, Industry engineers would always enjoy an advantage based on their superior knowledge of their own networks. Thus, replacing the existing system of Industry-LEA cooperation with Industry-LEA competition would most likely frustrate the implementation of lawful surveillance.

IV. INDUSTRY COOPERATION IS NEEDED TO PROTECT LI SUBSCRIBER PRIVACY

Preserving Industry cooperation in the LI process is also important to protect subscriber privacy. Industry plays an important privacy protection role in both the development and use of LI products.

A. Industry Protects Privacy at the LI Solution Development Stage

When Industry forms an LI solution for a communication service it typically starts by assigning the work to a technical standard-setting body. These standard-setting bodies include Industry lawyers and engineers with specialized training in the needs of LI. The bodies also include LEAs, although their participatory rights are minimal. The Industry experts design and publish the technical specifications for the desired LI solution. CALEA encourages the use of these groups by giving their publications legal "safe harbor" status. When published, the safe harbor standard may be used as a blueprint by a CSP's equipment vendor to build the hardware/software solution itself.

CALEA technical standard-setting bodies work hard to protect subscriber privacy. In particular, they ensure that LI solutions isolate and capture only the communications of court-identified criminal subjects and not other subscribers. They also restrict the solutions to deliver only the communications content and signaling information required by court orders. In addition, because the standards are published they are accountable to the public, including privacy experts.

The above-described privacy safeguards are absent when LEAs build LI solutions on their own. For example, an LEA solution may capture all packets in a suspect's broadband stream, regardless of the scope of data specified in the court order. The over-collection would not amount to a legal violation. LEAs may rely on their "minimization" authority to filter out the excess packets. Still, in this arrangement privacy is not the priority.

B. Industry Protects Privacy at the LI Solution Operating Stage

Once an LI solution is installed in a CSP network the CSP maintains control over its use. This control offers additional privacy protection. Specifically, the service provider can ensure that the solution delivers only the data specified in the order.

With an LEA-made solution the operating control rests with the LEA. As a result, a court order to intercept a suspect's VoIP traffic could lead to the collection of a suspect's entire broadband session, including not only VoIP calls but email, other text messaging services, Internet browsing patterns, and file sharing activities.

Notice the CALEA approach to LI, which gives Industry control over LI technology, creates a healthy separation of powers between Industry and LEAs and thereby ensures the technology is properly used.

V. INDUSTRY COOPERATION IN LI SHOULD BE IMPLEMENTED IN THE SAME MANNER AS INDUSTRY COOPERATION IN SIMILAR GOVERNMENT MANDATES

Despite the benefits of Industry cooperation in LI, many CSPs have not provided that cooperation because they have not brought their networks into compliance with CALEA. The main reason for the lack of compliance is because CALEA is difficult to enforce. As stated in the Caproni Statement, the CALEA enforcement clause requires that once an LEA uses alternative technologies to implement an LI order, a court may not enforce the statute against the non-compliant CSP. An LEA will almost always use alternative technologies, however inadequate, reasoning that something is better than nothing when it comes to solving an investigation. Consequently, the enforcement section of CALEA has never been invoked and its fines for non-compliance have never been imposed. The FBI proposes to remove this statutory Catch-22.

Subsentio agrees. When CSPs disregard their CALEA obligations they put public safety at risk. They also create competitive disparities between themselves and the many CSPs who expend resources to comply. CALEA enforcement should not be so lax that it effectively derails compliance. On the other hand, it need not impose heavy

liability on Industry. Subsentio suggests that the statute's enforcement mechanism could be improved in multiple ways, taking cues from other CSP mandates.

A. E911 Enforcement

As explained above, the FCC requires certain CSPs to equip their service offerings with E911 solutions. The FCC has enforced the E911 mandate with various accountability measures, including monetary fines. For example, in one case where a carrier failed to upgrade its network with an E911 solution, the FCC imposed a fine of $25,000.

Significantly, the E911 enforcement scheme contains no escape clause for non-compliant CSPs where a PSAP is able to rescue the E911 caller without the need for CSP cooperation, or where the rescue can be accomplished once the CSP informs the PSAP of the caller's billing address. Likewise the CALEA enforcement provision need not excuse a CALEA violation just because a second-best alternative happens to exist.

B. CPNI Enforcement

CSPs are generally required to protect the privacy of subscriber account information, known as customer proprietary network information, or "CPNI." In addition, covered entities must file an annual certification with the FCC to confirm their compliance with the CPNI mandate. If an entity fails to file the annual certification it is subject to an FCC fine of $20,000. A repeated violation would increase the fine to $25,000. The FCC has consistently imposed fines for violations of the annual certification rule.

CALEA enforcement could be improved to incorporate a similar requirement. Each year a CALEA-covered CSP would be required to certify its CALEA compliance status, and a failure to certify could trigger a fine.

C. Disabilities Access Enforcement

Another federal mandate requires certain CSPs and their equipment vendors to make their services accessible to persons with disabilities. To enforce the disabilities access mandate, aggrieved parties may file formal and informal complaints before the FCC. If the FCC finds a violation it may impose remedial actions and sanctions on the non-compliant entity.

Congress recently broadened the disabilities access mandate to cover a broader scope of CSPs and manufacturers and strengthen its enforcement. One of the new enforcement terms requires the FCC to complete an investigation of a disabilities

complaint within 180 days. The FCC has opened a rulemaking proceeding to implement the new law.

Congress could impose a similar 180-day deadline to resolve CALEA complaints.

VI. LEA-MADE SOLUTIONS SHOULD BE USED ONLY IN EXCEPTIONAL CIRCUMSTANCES

Despite the advantages of Industry cooperation in the development and use of LI solutions, such cooperation may not always be sufficient. The Caproni Statement observes there are "very sophisticated criminals who use communications modalities that are virtually impossible to intercept through traditional means." In those circumstances, she believes, LEAs should be permitted to use individually tailored solutions such as those developed in the proposed NDCAC. She adds, however, that "individually tailored solutions have to be the exception and not the rule."

Subsentio recognizes the possible need for individually tailored LI solutions in exceptional circumstances. Some suspects go to such great lengths to evade lawful surveillance that no commercially available technology can capture their communications. In these rare situations a CALEA solution may miss certain types of communications content or signaling information. If so, LEAs may need to develop special LI solutions to capture the missing data. An NDCAC could provide the R&D for these special cases. Even in these cases, however, Industry cooperation may be needed.

Subsentio also agrees with General Counsel Caproni that individually tailored solutions should be the exception and not the rule. Such LEA-made solutions are no substitute for CALEA, as explained in Sections II through V above. Therefore, if a court orders surveillance on a suspect, and the suspect's CSP is not CALEA compliant, the LEA should not turn to the NDCAC. It should bring a CALEA enforcement action against the non-compliant entity. In exceptional circumstances an individually tailored solution could still be used.

VII. CONCLUSION

In the Going Dark Proceeding, Congress heard testimony from opposite perspectives. The law enforcement witnesses asked Congress for two forms of relief: to update and improve the CALEA statute, which requires LI solutions to be made by Industry; and to fund an NDCAC where LEAs may create their own individually tailored solutions in

exceptional circumstances. The opposing witness objected to CALEA and said all LI solutions should be made by LEAs without Industry cooperation.

Subsentio approaches the issue from a third perspective, one that serves all three interests involved: law enforcement, Industry, and privacy. In Subsentio's view, law enforcement's two-pronged approach would better meet today's LI needs.

The proposal to improve CALEA would ensure the kind of Industry cooperation that is critical to effective LI. Although network security is a valid concern when crafting any network solution, Industry already addresses these concerns as fully as possible with secure solution designs and accountable security protocols. Industry involvement in LI also helps protect subscriber privacy.

If Congress does nothing else for CALEA, it should remove or revise the limiting clause that has left the statute unenforced throughout its 17-year history. Giving CALEA the same enforcement powers as other, similar mandates would likely promote more widespread compliance. That, in turn, would enhance public safety and remove competitive disparities without imposing excessive burdens on industry.

The proposal to create the NDCAC also seems worthwhile, provided the institution is used only in exceptional circumstances, as law enforcement has proposed.

Subsentio looks forward to further progress in the Going Dark proceeding.

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

September 28, 2011

The Honorable F. James Sensenbrenner, Jr.
Chairman
Subcommittee on Crime, Terrorism and Homeland Security
Committee on the Judiciary
United States House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

Enclosed please find responses to questions for the record arising from the appearance of Valerie Caproni, General Counsel of the Federal Bureau of Investigation, at a hearing before the Subcommittee on February 17, 2011, entitled "Going Dark: Lawful Electronic Surveillance in the Face of New Technologies." We hope this information is of assistance to the Subcommittee.

Please do not hesitate to contact this office if we may provide additional assistance regarding this, or any other matter. The Office of Management and Budget has advised us that from the perspective of the Administration's program there is no objection to submission of this letter.

Sincerely,

Ronald Weich
Assistant Attorney General

Enclosure

cc: Representative Bobby Scott
Ranking Minority Member

**Responses of the Federal Bureau of Investigation
to Questions for the Record
Arising from the February 17, 2011, Hearing Before the
House Committee on the Judiciary
Subcommittee on Crime, Terrorism, and Homeland Security
Regarding "Going Dark"**

Questions Posed by Representative Scott

1. Given NSA's experience and vast expertise in promoting information security and assurance, the NSA Information Assurance Directorate could provide expert security vetting of any legislative proposal from the FBI to solve the Going Dark problem. Does the FBI plan to work with IAD on any wiretapping legislation it might propose?

Response:

The Administration has convened an interagency working group, which includes the Department of Defense and its components, to review the Going Dark problem and identify possible solutions. Any proposed legislation will be appropriately coordinated through the interagency process.

2. Security standards for federal civilian agencies have been the responsibility of the National Institute of Standards and Technology. Does the FBI plan to seek an FIPS from NIST for any type of IP-based communications that the FBI favors for solving the Going Dark problem?

Response:

The FBI does not intend to seek a Federal Information Processing Standard from the National Institute of Standards and Technology. The focus of the Going Dark initiative is not federal civilian agencies' security standards. Rather, it is the growing gap between the statutory authority of law enforcement to intercept electronic communications pursuant to court order and our practical ability to intercept those communications.

---

3. At one point during the hearings, you said that the FBI didn't want "back-door" access to communications, only "front-door" access. Please explain what is meant by that distinction.

Response:

The FBI only conducts electronic surveillance pursuant to lawful authority obtained under Title III or the Foreign Intelligence Surveillance Act (FISA). When the term "back-door" access is used, we believe it connotes surreptitious or clandestine access; in contrast, "front-door" access connotes access that occurs with the knowledge and assistance of the service provider. Back-door access, then, would occur if a system was entered and information removed without the knowledge of the system owner. Front-door access occurs when the government serves the provider with a court order openly and overtly and the provider knowingly provides the communications of the target, in accordance with the terms of the court order, to the government.

Within that definitional scheme, the current construct of the Communications Assistance for Law Enforcement Act (CALEA), Title III, and FISA presume front-door access. Although there may be unusual fact patterns in which court-authorized surveillance occurs without the knowledge of the service provider (for example, if the service provider is corrupt or is actively engaged in the criminal conduct under investigation), most of the time that the government is engaged in electronic surveillance, the service provider is knowingly engaged in effecting court-authorized wiretaps or assisting law enforcement to effect the wiretaps. The involvement of the service provider adds an element of privacy protection (for example, the service provider will receive and review a court order and configure the collection device to isolate the communications of the target to the exclusion of all others for delivery to the party conducting the wiretap). This construct has generally worked well through the years. While the FBI strongly prefers that front-door access continue to be the norm, in order for that construct to be successful service providers must have available to them a technological means of effecting court-authorized wiretaps in a timely and efficient way.

4. In the written testimony, you said that the FBI will not seek to re-architect the network. Does this mean the FBI will not be seeking changes in Internet protocols?

Response:

The FBI does not believe changes in Internet protocols are necessary or desirable.

5. What is the FBI's proposed legislative solution if the carrier/applications provider does not have access to the communications being sought (say because the communication is peer-to-peer)?

Response:

The FBI recognizes that it may not be possible to resolve all issues concerning electronic surveillance with particular carriers/providers through legislation, and the Administration will not propose legislation that would impose an impossible requirement on industry.

6. Will the FBI be seeking legislation requiring that all applications that include real-time communications be accessible by the provider? Does this means that all communications applications must be centralized? If not, what is the model being proposed?

Response:

The Administration has convened an interagency working group to review the Going Dark problem and identify possible solutions. The Administration does not yet have a position regarding what legislation may be proposed.

7. Encryption technology is only one aspect of the measures that a carrier could take to insure the security of the communications services it provides. Since the FBI is not seeking "fundamental changes to encryption technology," is the bureau seeking fundamental or other changes to any other aspect of the security measures that carriers provide?

Response:

No. The FBI is not seeking any fundamental or other change to any aspect of the security measures that carriers provide. The FBI believes carriers should safeguard their networks to the greatest extent possible while simultaneously ensuring law enforcement can conduct lawfully authorized electronic surveillance.

---

8. Will the FBI seek legislation restricting what types of cryptographic implementations could be used in real-time communications systems? How would this prevent the sophisticated user from applying end-to-end encryption to their communications?

Response:

The FBI recognizes that it may not be possible to resolve all issues concerning the government's ability to conduct court-authorized wiretaps through legislation. Very sophisticated users who apply end-to-end encryption may well be a challenge that can only be addressed on a case-by-case basis. In any event, the FBI will not be seeking fundamental changes to the current legal mandates with respect to encryption.

9. Will the FBI seek legislation constraining the security architectures that carriers may use?

Response:

The FBI does not intend to seek legislation that would constrain the security architectures that carriers may use. The FBI has a significant interest in maintaining the security of the Internet and would not propose legislation that would weaken or otherwise undermine that architecture.

10. It is standard practice to model threats against systems to assure security. What threat modeling does the FBI do against proposed CALEA architectures?

Response:

The FBI cannot and does not propose any specific CALEA architecture. It is generally within a service provider's discretion as to how the provider will meet the Assistance Capability Requirements of CALEA, whether by adopting a solution based on an industry-promulgated technical standard or by some other means. The solutions adopted by service providers are integrated into their networks, are managed, controlled, and activated by service provider personnel, and are maintained by service providers as they otherwise upgrade or modify their networks.

Statement of Concern about Expansion of CALEA

By *CDT*
Created *02/14/2011 - 3:01pm*
February 15, 2011

Recently, FBI officials have indicated that the Obama Administration may seek legislation to expand the scope of the Communications Assistance for Law Enforcement Act (CALEA) to a broad array Internet communications technologies. Currently, this 1994 law requires telecommunications carriers to design wiretapping capabilities into their networks, and the FCC extended these requirements to providers of broadband Internet access and interconnected VoIP services in 2005. Clearly, lawful electronic surveillance plays an important role in enabling government agencies to fulfill their obligations to stop crime and to protect national security. These goals, however, must be reconciled with other important societal values, including cybersecurity, privacy, free speech, innovation and commerce.

These threshold questions should be answered before consideration of any proposal to expand CALEA:

1. **What specific problems must be addressed?** As it was required to do when it proposed the original CALEA, the FBI must first identify the particular services or technologies most in need of additional surveillance capability and the frequency with which they thwart authorized government surveillance.
2. **Have alternatives to a CALEA-like mandate been pursued sufficiently?** After the specifics have been identified, alternative approaches to surveillance needs that do not involve technology mandates should be considered. Industry may voluntarily adopt practices that obviate some problems; others may be addressed by providing extra resources for the FBI to acquire additional expertise and for assisting state and local law enforcement.
3. **What is the narrowest, effective approach?** Only after addressing the first two elements could changes that are narrowly targeted be considered. Generalized or overbroad mandates would be difficult to implement, likely to foster avoidable litigation, and certain to have unintended results.

After these threshold questions are answered, policy makers should measure any proposal to extend the scope of CALEA mandates against all of the following principles:

Preserve trust: Consumer and business trust in the confidentiality of Internet communications is essential to online commerce, privacy and free speech. Changes to products and services that could undermine users' trust in the privacy and security of their communications should be avoided.

Safeguard cybersecurity: Requiring redesign of Internet communications technologies to facilitate surveillance would make them less secure and produce vulnerabilities exploitable by others, including foreign entities, perpetrators of economic espionage, malicious insiders, hackers and identity thieves, thus undermining cybersecurity goals.

Protect innovation and competitiveness: Extending CALEA mandates to Internet communications applications could stifle innovation, delay or prevent cutting-edge communication technologies from coming to market, and give foreign competitors an advantage over U.S. companies. Any requirement of governmental approval of such technology or applications before release must be rejected for the same

reasons.

Anticipate resultant international demands: New U.S. surveillance requirements could spur other countries to impose new mandates that are equally burdensome or worse, thereby undermining efforts to resist such demands by other countries.

Don't compromise encryption: Strong encryption is a foundation for data security, Internet commerce and personal communication. There should be no new requirements or restrictions that would introduce vulnerabilities or weaken the protection afforded by encryption and related security technologies.

Avoid unfunded mandates: The costs of implementing any new proposals should be borne by the government.

Protect privacy and promote accountability: Stronger technical capabilities resulting from extension or expansion of CALEA should be matched with stronger privacy protections such as enhanced judicial oversight, transparency, and audits to promote government accountability.

American Library Association [1]
Association of Research Libraries [2]
Americans for Tax Reform's DigitalLiberty.Net [3]
Business Software Alliance [4]
Center for Democracy & Technology [5]
Center for Financial Privacy and Human Rights [6]
Competitive Enterprise Institute [7]
Computer and Communications Industry Association [8]
EDUCAUSE [9]
NetCoalition [10]
Software and Information Industry Association [11]
TechAmerica [12]
TechFreedom [13]
U.S. Public Policy Council for the Association of Computing Machinery [14]

○