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 Domestic 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.