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

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 truly 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.