Making Sense from Snowden:

What's Significant in the NSA Surveillance Revelations

Susan Landau

On 6 June 2013, British newspaper *The Guardian* reported on a secret US National Security Agency (NSA) program to collect domestic telecommunications metadata—the who, what, and when of phone calls—from Verizon Business Networks Services.[1] A day later, the paper revealed details about PRISM, an NSA program that targeted the Internet communications and stored data of "non-US persons" outside the US and those communicating with them, and the extent to which US companies cooperate with the government.[2] More leaks followed, with details about the US government spying on Chinese computers, news that the NSA and its British counterpart GCHQ had used a monitored Internet café to eavesdrop on the communications of political leaders attending the 2009 London G20 summit,[3] that the British were themselves conducting massive intercepts of domestic communications, and that the NSA had been collecting metadata from domestic Internet communications.[4]

These revelations all stemmed from classified government documents provided by Booz Allen Hamilton employee Edward Snowden, whose motivation was his concern over the NSA's collection of personal data: "When you see everything, you see them on a more frequent basis, and you recognize that some of these things are actually abuses … eventually you realize these things need to be determined by the public, not by somebody who is merely hired by the government."[4]

Snowden believed much more was being collected than US laws justified: "NSA and intelligence community in general is focused on getting intelligence wherever it can by any means possible. It believes, on the grounds of sort of a self-certification, that they serve the national interest. Originally we saw that focus very narrowly tailored as foreign intelligence gathered overseas. Now increasingly we see that it's happening domestically and to do that they, the NSA specifically, targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyses them and it measures them and it stores them for periods of time simply because that's the easiest, most efficient, and most valuable way to achieve these ends."[4]

Snowden's act had extraordinary implications, and the US government's response was swift and sharp. NSA Director General Keith Alexander said that Snowden had caused "irreversible damage" to the US,[5] while Senate Select Committee of Intelligence Chair Dianne Feinstein said Snowden's action was treasonous.[6] Snowden was indicted on charges of espionage—somewhat surprising as "leaks of classified information to the press have relatively infrequently been punished as crimes," according to a Congressional Research Service report.[7] A warrant has been issued for Snowden's arrest.

Other members of the US government see the situation differently. Former Vice President Al Gore said, "[The NSA surveillance] in my view violates the Constitution.… The Fourth Amendment language is crystal clear. It isn't acceptable to have a secret interpretation of a law that goes far beyond any reasonable reading of either the law or the Constitution and then classify as top secret what the actual law is."[8]

In March 2013, during hearings on national security threats, Senator Ron Wyden asked Director of National Intelligence James Clapper whether the NSA collected "any type of data at all on millions or

Copublished by the IEEE Computer and Reliability Societies
1540-7993/13/$31.00 © 2013 IEEE

hundreds of millions of Americans." Clapper's answer was, "No; not wittingly."[9] After the NSA documents became public, Senator Rand Paul stated that, "Clapper lied in Congress, in defiance of the law, in the name of security. Mr. Snowden told the truth in the name of privacy."[10]

Did Snowden cause irreparable harm, or did he reveal facts that should be publicly examined? What are the facts, anyhow? This article seeks to put the Snowden revelations in context, explaining what's new, why it matters, and what might happen next.

Putting the Revelations in Context

To understand what's happening here, we must penetrate the deep thicket of national security wiretapping. This area is so densely overlaid by laws and secret rulings that even the lawmakers who created it can't always see inside. Let's clear some of the underbrush to get a feel for the general shape of the forest.

Governmental Powers

Limiting government's power is fundamental to the US political system. During the American colonial period, the British government searched properties using writs that specified neither the goods being sought nor their location. Anger over these unrestricted searches played an important role in the period leading up to the American Revolution, and the specificity required by the Fourth Amendment arose in response: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Wiretaps are searches. To comply with the Fourth Amendment, the two primary US wiretap statutes, Title III of the 1968 Omnibus Crime Control and Safe Streets Act and the 1978 Foreign Intelligence Surveillance Act (FISA), require a specific, articulable reason for wiretapping. Title III taps require probable cause that the suspect is committing, has committed, or is about to commit a serious crime, whereas FISA taps require that there be probable cause that the target is a foreign power or an agent of a foreign power, and that the purpose of the tap is foreign intelligence. Use of a wiretap is typically a last resort—that is, when the information sought can't reasonably be obtained by other means.

After the surveillance abuses of Richard Nixon's presidency were brought to light, a special Senate committee was created to investigate illegal and improper activities conducted by government intelligence agencies. The Church Committee, named for its chair, Senator Frank Church, uncovered a well-hidden, 40-year history of excessive government surveillance whose targets included reporters, Congressional staffers, Supreme Court Justices, members of the administration and the opposition, and law-abiding citizens engaged in peaceful political protest.[11] Oversight had been essentially nonexistent. The Church Committee investigation recommended rules to rein in excessive and improper government surveillance done in the name of "national security." Many were incorporated into FISA. Although there might have been surveillance abuses post-FISA, those that have come to light were relatively small in scale until after 11 September 2001.

While they're occurring, wiretaps constitute secret searches. Once they're completed, some information about Title III wiretaps becomes public through the annual *Wiretap Reports* (www.uscourts.gov/Statistics/WiretapReports/WiretapReports_Archive.aspx). FISA wiretaps lack such transparency; indeed, almost everything about FISA wiretaps is secret. In particular, the proceedings of the Foreign Intelligence Surveillance Court (FISC), which decides on applications for FISA wiretaps, are classified.

The Fight over Metadata

The 1986 Electronic Communications Privacy Act (ECPA) governs

Glossary

- Federal Bureau of Investigation (FBI): US national security and intelligence agency that conducts domestic investigations.
- Inspector General: an independent investigative official in a government agency whose responsibility is to detect and deter abuse, misconduct, and fraud and to ensure integrity of the agency's mission.
- National Security Agency (NSA): US agency charged with supplying the government with information security capabilities—its lesser known function—and information from signals intelligence. The NSA's remit is foreign intelligence.
- National Security Letter (NSL): an administrative letter issued by the FBI requiring the recipient to produce certain information to federal investigators. Some NSLs are issued with gag orders requiring that information concerning the NSL be shared only with the recipient and legal counsel.
- Probable cause: sufficient reason, based on known facts, to believe that with greater than 50 percent probability, a crime has been, or is likely to be, committed.
- Subpoena: formal document issued by a party to litigation requiring the presence of a person or production of some information (for example, telephone subscriber information).
- Telephony location data: cell phones work by accessing a local cell tower; the sector of the cell tower is the location data provided to the telecommunications provider. Finer-grained location data is provided by GPS, but it's typically shared only with applications providers.
- US person: a US citizen, permanent resident, corporation incorporated in the US that doesn't include a foreign government, or a group consisting mainly of US citizens and/or permanent residents.

The Initial Justification for "Warrantless Wiretapping"

The leaked draft National Security Agency (NSA) Inspector General Report described the start of the warrantless wiretapping program from the agency's perspective:

> After the 2001 terrorist attacks, the NSA sought to use contact chaining to track terrorists, many of whom were communicating via U.S. webmail accounts. At that time, the U.S. was a major crossroads for Internet communications; 99% originated, terminated, or transited the U.S. (the percentages are significantly lower now). The Department of Justice had previously informed the NSA that a FISA order was needed for contact chaining. But in the post September 11th environment, the intelligence agency believed that obtaining even emergency FISA orders would obstruct timely intelligence. NSA Director General Michael Hayden suggested that enabling the agency to collect communications with one end outside the United States without a warrant "would increase NSA's speed and agility."

The White House authorized warrantless wiretapping for a "limited period." In time, the effort was seen as permanent, and processes and technologies were put in place to accommodate the shift.

the real-time capture of calling data—so-called pen register and trap and trace—as well as the collection of call data records (CDRs) and stored content such as email. At the time of ECPA's passage, telephones were essentially stationary, and such metadata wasn't deemed worthy of much legal protection. Because call metadata is shared with third parties—telephone companies—as well as being business records, it isn't subject to the same Constitutional protections as content. Consequently, metadata can be obtained by the government on the basis that it's relevant to an ongoing investigation; there's no requirement of probable cause. But law hasn't kept pace with technology. People carry their mobile devices all day long, and the result is that cell phones disclose far more personal information than stationary ones did in 1986. For an example of how revelatory that data is, see what the newspaper *Zeit Online* deduced from the Deutsche Telekom records of German Green Party politician Malte Spitz (www.zeit.de/datenschutz/malte-spitz-data-retention).

In the wake of September 11, the criteria to conduct surveillance, whether electronic or otherwise, loosened. This included the criteria for a Federal Bureau of Investigation (FBI) field office to obtain a National Security Letter (NSL), a request for records issued by the investigative agency (and thus without judicial oversight as part of the process). NSLs are typically accompanied by gag orders preventing the recipient from disclosing the fact that an NSL was issued.

Shortly after the 2001 terrorist attacks, President George W. Bush expanded the NSA's authority to warrantlessly wiretap international communications with one end outside the US. (A partial rationale for this was technical.[12] FISA permitted warrantless wiretapping of radio communications if one end of the communication was outside the US; it was intended that this loophole be addressed by a further law, but it never was. With fiberoptic cables replacing radio, the ability to conduct such warrantless wiretapping disappeared.) In 2005, *The New York Times* exposed the warrantless wiretapping, and great hue and outcry ensued. Civil liberties groups and members of Congress were outraged, and one member of the FISC resigned in protest.[13] But with the Bush administration arguing that the tapping was crucial to protect against terrorism, the warrantless wiretapping continued. In 2007, the Protect America Act established a legal basis for this wiretapping for a scant six months (later briefly extended). The 2008 FISA Amendments Act (FISAAA) provided a further extension (and gave the telephone companies retroactive immunity for participating in the warrantless surveillance as well as creating prospective immunity for FISAAA activities). As long as no US person is directly targeted, rather than providing the protection of individualized warrants, the FISAAA permits warrants to be issued for "classes" of taps.

The documents Snowden released shed light on numerous issues. Section 215 of the 2001 USA Patriot Act authorizes the collection of business records, which is standardly interpreted to mean driver's license records, hotel records, car rental records, credit card records, and so on. It can also be used for phone records, but the government used Section 215 to justify requests for domestic telephone metadata delivered in bulk, not individualized requests, as had been anticipated by the law's sponsor. For several years, Senator Wyden and Senator Mark Udall unsuccessfully sought to make this secret interpretation of the law public.[14]

Although obtaining NSLs wasn't particularly difficult, in the months after the 2001 terrorist attacks, agents in the FBI's New York field

Ignoring the Law: The FBI and the Journalist

Freedom of the press is a crucial lynchpin of American democracy. Thus the Code of Federal Regulations has stringent conditions regarding government investigations of journalists. Before the government can subpoena a reporter's telephone billing records, investigators must try all other reasonable forms of investigation. And no one less than the Attorney General can approve the issuing of a subpoena for a journalist's phone records.

These binding rules were badly broken in 2004 when the FBI investigated *The New York Times* and *Washington Post* correspondents reporting from Jakarta on Islamic terrorism. FBI agents asked for records under exigent circumstances. Seeking 38 days of call records, law enforcement investigators received 22 months' worth. One telecommunications provider gave the FBI records on 1,627 calls, even though only three were within the investigatory period; the FBI downloaded information on all 1,627.[1]

Discovering who's talking with a reporter severely compromises that reporter's ability to work. Who would talk with a journalist about sensitive information if they knew law enforcement could track their every move? That chilling effect is the reason behind the restrictive rules in the Code of Federal Regulations—although this might be hard to believe in an era of months-long collection of AP journalists' phone records in order to track leaks.[2]

References

1. Office of the Inspector General, Oversight and Review Division, "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," US Dept. of Justice, Jan. 2010; www.justice.gov/oig/special/s1001r.pdf.
2. C. Savage and L. Kaufman, "Phone Records of Journalists Seized by US," *New York Times*, 14 May 2013, p. A1.

office used "exigent letters" to request immediate access to domestic telephone records. These letters stated that appropriate subpoenas had already been submitted to the US Attorney General's Office, but ECPA has no provision for exigent letters, and the follow-on legal process sometimes didn't happen. The FBI's access to the CDRs created many problems, including a frequent lack of legal follow-up with an NSL, subscriber data provided without an FBI agent's written request, a lack of specificity on the requested data, exigent letter requests in the absence of an emergency, requested "sneak peeks" without a written request, and inappropriate investigations of journalists.[15]

The FBI's Inspector General issued a stinging report on the FBI's use of exigent letters, detailing violations of the law,[15] but apparently there were no other consequences. This lack of response may have indicated that the government didn't risk much in stretching surveillance law past what was legally permissible.

What's the Problem?

As I write this in early July, more revelations are likely to come, but my focus here is on the big ones revealed so far—the shipping of domestic communications' metadata to the NSA (including sender and receiver email and IP addresses),[16–18] the PRISM program's collection of Internet communications stored by cloud service providers, and the spying on Chinese computers and on allies, including on communications sent during the G20 meeting.

Metadata and the NSA

Although the law provides less protection for metadata than content, metadata can be even more revelatory than content itself—for example, it can reveal who attended church versus an Alcoholics Anonymous meeting. Why was the NSA doing bulk collection of telephone metadata? Why couldn't the FBI use NSLs to obtain the CDRs from Verizon—and other telephone companies—as needed? Why were there daily updates of the data? How was the data being used?

There was much that was confusing. The Verizon FISC order appears to have specified that the company was to deliver location data, but the government explicitly denied that it was collecting it.[19] However, a draft NSA Inspector General (IG) report leaked by Snowden made it clear that, in the bulk collection of metadata of international Internet communications, IP addresses of the facility being tapped were also being collected.[12] Other documents show that the NSA collected metadata of domestic Internet communications from 2001 through at least 2011.[18] Because the NSA wasn't allowed to collect the communications content of US persons without a warrant, the agency used location, specifically the IP address, as a way to determine if a subject was a "US person" (and thus what action could be taken). Although not 100 percent accurate, such addresses can reveal location.[20]

The leaked IG report described the purpose of the telephony metadata as "contact chaining"—finding the phone numbers "two degrees of separation" from the original target, that is, numbers called by the target, and then numbers called by those numbers[12]—lending credence to NSA statements that telephony metadata use was minimal (300 uses in 2012, according to the agency) and that there was no collection of telephone location information. In

addition, the leaked report gave a rationale for collecting telephone metadata: in a fast-moving crisis, even emergency FISC orders weren't sufficiently timely to allow the NSA to track terrorists, who change phones and numbers frequently. It also described minimization, at least in broad terms, justifying the need for a strong effort to ensure collection of foreign communications that were likely to include communications between al Qaeda and its affiliates.

On one hand, we see care in collection (at least for US persons), but on the other, the leaked IG report is the only public description we have of the purpose behind the NSA's bulk collection of communications metadata. Ultimately, however, the collection of telephony metadata is an interpretation of Section 215 tantamount to a secret law. Such metadata includes location data, but the location data from cell towers, not from GPS (which is shared with application providers and is viewed as content). Even the less finely grained cell tower information—and some of it can be quite precise[21]—gives the government unparalleled power over its people, which isn't consistent with a government that Abraham Lincoln described as "for the people, by the people, and of the people."

PRISM

For those who read very carefully, the extent of the PRISM program wasn't a surprise: a 2012 report prepared for the European Parliament warned that "any data-at-rest formerly processed 'on premise' within the EU, which becomes migrated into Clouds, becomes liable to mass-surveillance."[22] Yet for many people around the world, the program's revelation was a startling look at the extent of NSA data collection. It became clear that under Section 702, there was also significant collection of data of US persons. To explain these aspects, let's dig a little deeper into wiretap law.

The Fourth Amendment offers protection only to "US persons." Originally, no warrant was needed to wiretap outside the nation's borders (FISAAA now requires one for targeting a US person overseas). FISAAA gives the US government warrantless access to the communications and data of non-US persons stored in the US (for example, US cloud providers). Government documents clarify that the basis for permitting an investigation isn't terrorism, but the person's status as a non-US person: "For traditional FISAs you must have probable cause that the target is a 'foreign power' or agent of a 'foreign power.' For section 702, however, there must a reasonable belief that the target is a NON-USPER located outside the United States" (www.aclu.org/files/pdfs/natsec/foia20101129/FAAFBI0536.pdf). US law doesn't grant the same rights to non-US persons, at least for those overseas. This is in contrast to, for example, the European Court of Human Rights, which recognizes the right of liberty and security for each person regardless of citizenship.

Under laws and regulations based on the EU Charter of Fundamental Rights and the European Convention on Human Rights, Europe has spent several decades establishing privacy protections for personal data, including transborder flows. NSA eavesdropping on non-US persons greatly undermines these protections. It's quite impossible for an individual to be the first owner of his or her personal data if the US government has secretly collected such information. The PRISM documents mention "direct access" to Microsoft, Yahoo, Google, Facebook, and other US technology companies, but that might be a casual claim rather than a precise statement. Several of the companies in question have clarified that this occurs only under legal process—and not through direct access at company servers.[23] Nonetheless US companies providing cloud services worried they would face an exodus of international customers due to the NSA surveillance.

Concerns by European leaders were about both the invasion of privacy to their citizens as well as the extensive spying on political organizations.[24] Based on other documents released by Snowden, the German newspaper *Der Spiegel* alleged that the NSA had eavesdropped on EU offices, and EU President Martin Schulz warned, "If the allegations prove to be true, it would be an extremely serious matter which will have a severe impact on EU-US relations" (www.europarl.europa.eu/the-president/en/press/press_release_speeches/press_release/2013/2013-june/html/schulz-on-alleged-bugging-of-eu-office-by-the-us-authorities).

One impact from the Snowden disclosures will likely be felt on US efforts to promote a free and open Internet. This foreign policy objective was opposed by several nations that seek to control the freedom of expression that the Internet allows. There was strong pushback, for example, at the recent International Telecommunication Union meeting in Dubai, with a proposal for moving the Internet under the ITU's regulated framework.[25] With the release of the NSA surveillance documents, President Barack Obama's administration has lost much of its moral leadership in this area.

The revelations about Section 702 also had domestic fallout. Minimization procedures, intended to keep the government from acquiring, retaining, or disseminating data that it isn't supposed to have in the first place, don't seem designed to accomplish that task. Purely domestic communications were to be destroyed unless the com-

munication was believed to have foreign intelligence information, contain evidence of a crime, or be encrypted[26]—a rather startling choice, given that these communications were collected without a particularized wiretap warrant.

While the US was the main focus of the Snowden revelations, documents about UK surveillance also appear to have been released. According to *The Guardian*, "GCHQ was handling 600m 'telephone events' each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time."[27] British law, specifically the 2000 Regulation of Investigatory Powers Act, requires a warrant to tap targets, but, as with FISAAA, a clause allows the interception of broader classes of traffic if one end of the communication is outside national borders. Fiberoptic cables create oddities in network traffic: internal UK communications may be routed so they travel outside the country, making the communication subject to warrantless surveillance. The close intelligence relationship between the UK and the US means that the US has benefited from this eavesdropping.

NSA Spies

Snowden also revealed that the NSA hacked into at least 63 servers at Tsinghua University, China's leading technical school and home of one of six backbone networks in the nation.[28] Snowden claimed that the NSA compromised Chinese telecommunications networks and had access to millions of text messages.[29] This type of spying, and the NSA's capabilities to exploit it, surely isn't a surprise: the NSA has conducted network exploitation efforts since the 1990s.[30]

But the situation is complicated by active Chinese cyberexploitation of US industry.[31] The issue has been ongoing for years, but, in May, the US explicitly accused the Chinese government of infiltrating sites belonging to US military and defense contractors and stealing massive amounts of industrial technology.[32]

The Chinese had a different and, to them, equally strong complaint against the US. The US is one of the few nations in the world to criminalize economic espionage (the theft of a trade secret if intent is to benefit a foreign government) while it views free speech as a protected right. In China, the situation is that economic espionage isn't illegal, but free speech is not permitted. US efforts to press an international free speech agenda have been viewed by the Chinese government as encroaching on national sovereignty.

Snowden's revelations occurred at an inconvenient time for the US government. While the fact that the US was inside the Chinese communications networks isn't all that surprising, the specificity of the revelations diminish the US government's ability to take the high road on the cyberexploitation issue. Unlike much of the information Snowden has released so far, the specifics on China had little to do with privacy and security of individuals—and much to do with US national security.

As for the GCHQ-NSA spying on the G20 leaders during the 2009 London summit, it's not necessarily surprising that the spying occurred, though the fact it happened through the use of an "ersatz" Internet café is an interesting detail. There might be a question as to whether this information should have been released by Snowden, but there doesn't appear to have been much of a secret nature here that was made public.

What's the Point?

A question for any surveillance regimen is its effectiveness, and this is where the NSA has made substantial claims. At hearings on 18 June, NSA Director General Alexander said that American surveillance had helped prevent "potential terrorist events over 50 times since 9/11."[33] (This was later amended to 54, of which 42 were terrorist plots, and 12 were "material support" to terrorists; 13 of these involved the US.[34]) At first glance, details seem to be lacking, but that's fairly normal—intelligence agencies don't

Cyberexploitation of Industry

Many nations, including US allies such as France, Germany, Israel, Japan, and South Korea, as well as less friendly nations such as Russia, conduct economic espionage against the US. But the Chinese cyberexploitation against US industry has been of a vastly larger scale than earlier efforts by other countries.

A critical distinction between the NSA penetration of Chinese systems and foreign agency exploitation of US industry is what's done with the data. Some evidence indicates that the economic spying done by other nations' intelligence services is directly given to industry within that nation. Hard as it may be to believe, the US government doesn't share the intelligence gained about foreign companies with their US competitors.[1] It's difficult to prove a negative, but all signs point to the intelligence being shared only within the government—with trade negotiators, for example—and occasionally with the public, such as when the US government becomes aware of other nations' unfair trade practices.

Reference

1. W.A. Owens, K.W. Dam, and H.S. Lin, *Technology, Policy, Law, and Ethics Regarding US Acquisition and Use of Cyberattack Capabilities*, Nat'l Academies Press, 2009, p. 26.

expose sources and methods. The three cases briefly mentioned were a group of men who helped fund a terrorist group in Somalia, a group of men arrested in 2004 with a plan to blow up the New York Stock Exchange, and the case of Najibullah Zazi, who plotted to blow up New York City subway cars before he was arrested in 2009.

Digging deeper into the details reveals a different story. The support of the Somali terrorist group was an US$8,500 contribution to al Shabab, admittedly a terrorist group in Somalia—but that's not an amount of money that would justify major wiretapping efforts. The stock exchange plot was described as "nascent," and the group wasn't prosecuted on the charge, although one member was convicted of sending money to al Qaeda. The Zazi plot, however, was serious. Zazi came under FBI surveillance after he communicated with an email address in Pakistan linked to terrorists; that address was supplied to the US by British intelligence.[35] So although a FISA tap was placed on Zazi, it occurred as a result of standard investigative techniques, not from NSA metadata collection or PRISM.

Many cases that federal prosecutors have trumpeted as major terrorism plots have turned out to be less serious than originally described. Examples include three Detroit men whose house "contained airport-employee identification badges and a date book with hand-drawn diagrams of aircraft and runways"[36] that the government later petitioned to have thrown out; a Brooklyn mosque that was ostensibly funneling millions of dollars to al Qaeda,[37] charges that were later determined to be groundless; and seven Miami men allegedly plotting to blow up Chicago's Sears Tower, which was later described as an "overcharged gang case"[38] involving "the pipe dream of a few men with almost no ability to pull it off on their own" (www.washingtonpost.com/wp-dyn/content/article/2006/09/01/AR2006090101764.html). In the absence of details of the 50 plots that Alexander mentioned at the hearings, it's impossible to know how many were really disrupted through the use, even peripherally, of the NSA surveillance tools, and how many were either not serious or in fact disrupted through other means. All we know is that of the 50 cases, 10 "might have involved" domestic telephone records.[39] A 2009 report on the Bush administration's warrantless wiretapping by the Inspectors General of the Department of Defense, Central Intelligence Agency, FBI, NSA, and the Office of the Director of National Intelligence concluded that the tapping generally played a limited role in the FBI's counterterrorism efforts.[40]

Where Does This Leave Us?

The documents Snowden released raise many questions about US government collection of data about private citizens. In the UK, the public, press, and politicians vigorously debated the Communications Data Bill, a law that would require ISPs and telecommunications providers to keep metadata records for 12 months (as of this writing, the bill has been withdrawn). The US has had no discussion of such a bill; something more draconian simply happened through a secret interpretation of the law.

We don't know what issues were raised by Congressional overseers or the FISC. But we do know oversight can make a difference. Consider the following:

- The leaked 2009 NSA IG details a situation in which the NSA General Counsel wasn't allowed to examine the Department of Justice's (DoJ) opinion on the legality of the warrantless wiretapping, an opinion drafted by a junior lawyer later found to be flawed: "Given the method of collection, bulk Internet metadata was prohibited by the terms of the FISA and Title III."[12] The new order devised by the DoJ and overseen by the FISC was more precise, specifying over which data links the NSA could collect Internet metadata and limiting the number of people who could view that data.
- After *The New York Times* reported on the warrantless wiretapping in 2005, one telephone company, unwilling to rely only on an agreement with the NSA, sought a court order compelling it to turn over telephony traffic. The FISC order applied more stringent rules for access and oversight than had previously been in place.[12]

In short, oversight matters, and it has been repeatedly lacking here.

Consider how little is known about the use of NSLs. Between 2004 and 2012, more than 118,000 NSLs were issued on US citizens—the public reports don't include data on non-US persons—40,000 to 50,000 of which were for subscriber information (http://epic.org/privacy/wiretap/stats/fisa_stats.html). Because of the gag order, it's difficult to trace how many of these resulted in arrests or convictions, but some earlier work done by the ACLU notes that of the 143,000 NSLs issued between 2003 and 2005, none resulted in criminal referrals for terrorism (www.aclu.org/national-security/surveillance-under-patriot-act).

Part of the problem is overclassification. Several years ago, J. William Leonard, former head of the Information Security Oversight Office, a position described by *The New York Times* as "the government's former classification czar," filed a formal complaint against the NSA and DoJ, complaining of "deliberate and willful" overclassification in a case involving a govern-

ment leaker[41] (the case was later dropped). The Snowden case aside, routine government overclassification is a well-acknowledged problem.[42] By allowing abuses to remain hidden and impeding information sharing, overclassification can create risks to national security and obstructs the democratic process.[42] Most important, it creates distrust in government. Of course, intelligence investigations must go forward in secrecy, but not all aspects must be so cloaked. An example of this is FISC opinions, which are currently classified; not even redacted summary opinions are publicly available.

Ultimately, the rules of data minimization should be subject to a public discussion, especially when they directly affect the public. Section 702, for example, allows collection of traffic data sans warrant. The minimization procedures don't prevent other uses of the collected domestic traffic data, which undermines the fundamental aspect of the Fourth Amendment—namely, that "no Warrant shall issue, but upon probable cause." The FISC allows bulk collection of cell phone location, something that the NSA has stated it does not exercise. But what if the NSA were to change its policies? Nothing in the law would prevent it from collecting such data. Is that appropriate, given the revelatory properties of location information? It might be impossible to discuss all operational details of data minimization rules, but the discussion of policy issues should happen in public.

Many people have urged the formation of a new Church Committee with remit to conduct a full—and public—investigation of the surveillance's extent, the problems with oversight by both the FISC and Congress, the minimization procedures being used, and how to rectify these issues. Such an investigation could well include recommendations for changes in the way that the FISC issues its opinions. The investigation should carefully examine how to conduct collection in our era of big data and cheap storage.

Another issue to be aired as a result of the Snowden affair should be an examination of the "surveillance industrial complex." In the effort to downsize the federal government, much intelligence work has been moved to the private sector, which some members of government are now rethinking. "We will certainly have legislation which will limit or prevent contractors from handling highly classified and technical data, and we will do some other things," said Senator Feinstein as chair of the Senate Select Committee on Intelligence.[43] Of course, although the extent that such work was outsourced might not have been known outside military and Washington circles, it was well known within. It remains to be seen how much change will actually occur.

Several bills are already proposed, including one by Senate Judiciary Committee Chair Patrick Leahy that would narrow the scope of collection of telephone metadata, terminate Section 702 of FISAAA early in 2015, and institute formal reviews of both Sections 215 and 702 (the annual *Wiretap Reports* on Title III surveillance provide valuable public oversight). Earlier this year, Representatives Zoe Lofgren, Ted Poe, and Suzan DelBene put forth an ECPA reform bill to require warrants for cell phone location. Some of these bills will now get more attention.

After Snowden's release of the NSA documents, Assistant Senate Majority Leader Dick Durbin remarked, "As I said when I offered my amendment [on requiring that the government could issue a Section 215 order for an American's records only if there were some connection to a suspected terrorist or spy] in 2009, 'someday the cloak will be lifted and future generations will ask whether our actions today meet the test of a democratic society—transparency, accountability and fidelity to the rule of law and our Constitution.' Today, that cloak has been lifted and this important debate must begin again" (www.durbin.senate.gov/public/index.cfm/pressreleases?ID=23b8bfde-c0cc-4ec0-85d0-4ecf660486bc).

It was important to Snowden that the disclosure of secret NSA documents not end as Macbeth fears, as "a tale told by an idiot, full of sound and fury, Signifying nothing." That tale hasn't been fully written, and whether the release of the documents will lead to substantive changes in US surveillance is hard to predict. But through Snowden's efforts, a cloak has been lifted. The US can now have the discussion about surveillance it should have had when these laws were being passed. Perhaps Britain will as well. ■

Acknowledgments

I appreciate comments on earlier drafts from Matt Blaze, Steve Bellovin (for technical details only), Hilarie Orman, Shari Lawrence Pfleeger, Jenny Stout, and several unnamed sources. All errors are my own.

References

1. G. Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *Guardian*, 6 June 2013, p. 1.
2. G. Greenwald, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *Guardian*, 7 June 2013, p. 1.
3. S. Shane and R. Somaiya, "New Leak Indicates Britain and US Tracked Diplomats," *New York Times*, 16 June 2013, p. A7.
4. L. Poitras and G. Greenwald, "NSA Whistleblower Edward Snowden: 'I Don't Want to Live in a Society

That Does These Sort of Things,'" [video], *Guardian*, 9 June 2013; www.guardian.co.uk/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance.
5. M. Schwirtz and J. Preston, "June 23: Updates on Snowden's Asylum Pursuit," *New York Times*, 23 June 2013; http://thelede.blogs.nytimes.com/2013/06/23/tracking-snowden/.
6. J. Herb, "NSA Leak Is Treason, Says Feinstein," *The Hill*, 11 June 2013; http://thehill.com/homenews/senate/304635-nsa-leak-is-treason-says-sen-feinstein.
7. J. Elsea, "Criminal Prohibitions on the Publication of Classified Defense Information," Congressional Research Service, 13 Jan. 2013.
8. S. Goldenberg, "Al Gore: NSA's Secret Surveillance Not Really 'The American Way,'" *Guardian*, 15 June 2013; www.guardian.co.uk/world/2013/jun/14/al-gore-nsa-surveillance-unamerican.
9. G. Kessler, "The Fact Checker: James Clapper's 'Least Untruthful' Answer to the Senate," *Washington Post*, 12 June 2013; www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html.
10. C. Savage, "Democratic Senators Issue Strong Warning about Use of Patriot Act," *New York Times*, 16 Mar. 2012, p. A12.
11. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, "Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities: Supplementary Detailed Staff Reports on Intelligence Activities and the Rights of Americans: Book III, Report 94-755," US Government Printing Office, 23 Apr. 1976.
12. Office of the Inspector General, Nat'l Security Agency, Central Security Service, "ST-09-0002 Working Draft," Nat'l Security Agency, 24 Mar. 2009; www.guardian.co.uk/world/interactive/2013/jun/27/nsa-inspector-general-report-document-data-collection.
13. D. Johnston and N.A. Lewis, "Domestic Surveillance: The White House; Defending Spy Program, Administration Cites Law," *New York Times*, 23 Dec. 2005; www.nytimes.com/2005/12/23/politics/23court.html.
14. P. Black, M. Smith, and C. Schoichet, "Snowden on the Run, Seeks Asylum in Ecuador," *CNN Politics*, 24 June 2013; www.cnn.com/2013/06/23/politics/nsa-leaks.
15. Office of the Inspector General, Oversight and Review Division, "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," US Dept. Justice, Jan. 2010; www.justice.gov/oig/special/s1001r.pdf.
16. E. Holder, "Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to Be Located outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," 28 July 2009; www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.
17. K. Wainstein, "Proposed Amendment to Department of Defense Procedures to Permit the National Security Agency to Conduct Analysis of Communications Metadata Associated with Persons in the United States, Memorandum for the Attorney General," US Dept. Justice, Nat'l Security Division, 20 Nov. 2007; www.guardian.co.uk/world/interactive/2013/jun/27/nsa-data-collection-justice-department.
18. G. Greenwald and S. Ackerman, "NSA Collected US Email Records in Bulk," *Guardian*, 27 June 2013; www.guardian.co.uk/world/2013/jun/27/nsa-data-mining-authorised-obama.
19. US District Court, Southern District of Florida, Case 11-60285-CR-Rosenbaum, *United States of America vs. Daryl Davis and Hasam Williams, et al.*, "Government's Response to the Court's Order and Motion for a Protective Order Pursuant to Section 4 of the Classified Information Procedures Act and Rule 16(d)(I) of the Federal Rules of Criminal Procedure and Memorandum of Law" (redacted, unclassified version).
20. S.M. Bellovin et al., "Risking Communications Security: Potential Hazards of the 'Protect America Act,'" *IEEE Security & Privacy*, vol. 6, no. 1, 2008, pp. 24–33.
21. M. Blaze, "House Committee on the Judiciary, Subcommittee on the Constitution, Civil Rights, and Civil Liberties, Hearing on ECPA Reform and the Revolution in Location Based Technologies and Services, Testimony," 2 June 2010; http://judiciary.house.gov/hearings/pdf/Blaze100624.pdf.
22. D. Bigo et al., "Directorate-General for Internal Studies, Policy Department C: Citizens Rights and Constitutional Affairs, Fighting Cybercrime and Protecting Privacy in the Cloud, Study for the European Parliament," Oct. 2012; www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf.
23. A. Efrati, "Google Asks for Approval to Report NSA Data Request," *Wall Street J.*, 11 June 2013; http://stream.wsj.com/story/latest-headlines/SS-2-63399/SS-2-251865/.
24. M. Birnbaum, "Merkel, Other European Leaders Raise Concerns on US Surveillance," *Washington Post*, 10 June 2013; http://articles.washingtonpost.com/2013-06-10/

world/39862553_1_u-s-citizens-surveillance-program-intelligence.
25. E. Pfanner, "US Rejects Telecommunications Treaty," *New York Times*, 14 Dec. 2013, p. B1.
26. E. Holder, "Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended," 28 July 2009; www.guardian.co.uk/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document.
27. E. MacAskill et al., "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," *Guardian*, 21 June 2013; www.guardian.co.uk/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa.
28. L. Lam, "Exclusive: NSA Targeted China's Tsinghua University in Extensive Hacking Attacks, says Snowden," *South China Morning Post*, 23 June 2013; www.scmp.com/news/china/article/1266892/exclusive-nsa-targeted-chinas-tsinghua-university-extensive-hacking.
29. L. Lam and S. Chen, "Exclusive: US Spies on Chinese Mobile Companies, Steals SMS Data, Edward Snowden," *South China Morning Post*, 23 June 2013; www.scmp.com/news/china/article/1266821/us-hacks-chinese-mobile-phone-companies-steals-sms-data-edward-snowden.
30. S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
31. "APT1: Exposing One of China's Cyberespionage Units," Mandiant Intelligence Center Report, Feb. 2013; http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf.
32. D. Sanger, "US Blames China's Military Directly for Cyber Attacks," *New York Times*, 7 May 2013, p. A1.
33. C. Savage, "NSA Director Says Surveillance Has Stopped Dozens of Plots," *New York Times*, 19 June 2013, p. 18.
34. P. Finn, "NSA Chief Says Surveillance Programs Helped Thwart Dozens of Plots," *Washington Post*, 27 June 2013; http://articles.washingtonpost.com/2013-06-27/world/40231068_1_alexander-collection-program-plots.
35. "British Spies Help Prevent Al-Qaeda Inspired Attack on New York Subway," *Telegraph*, 9 Nov. 2009; www.telegraph.co.uk/news/worldnews/northamerica/usa/6529436/British-spies-help-prevent-al-Qaeda-inspired-attack-on-New-York-subway.html.
36. D. Johnston and P. Zielbauer, "A Nation Challenged: The Investigation; 3 Held in Detroit after Aircraft Diagrams Are Found," *New York Times*, 20 Sept. 2001; www.nytimes.com/2001/09/20/us/nation-challenged-investigation-3-held-detroit-after-aircraft-diagrams-are-found.html.
37. E. Lichtblau and W. Glaberson, "Threats and Responses: Financing Terror; Millions Raised for Qaeda in Brooklyn, US Says," *New York Times*, 5 Mar. 2003; www.nytimes.com/2003/03/05/world/threats-responses-financing-terror-millions-raised-for-qaeda-brooklyn-us-says.html.
38. D. Cave and C. Gentile, "Five Convicted in Plot to Blow Up Sears Tower," *New York Times*, 13 May 2009, p. A19.
39. K. Dilanian and M. Hay Brown, "NSA Chief Says Programs Disrupted 50 Terrorist Plots," *Baltimore Sun*, 18 June 2013; http://articles.baltimoresun.com/2013-06-18/news/bs-md-nsa-surveillance-20130618_1_nsa-chief-washington-post-intelligence-community.
40. Offices of the Inspector General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency, Office of the Director of National Intelligence, "Unclassified Report on the President's Surveillance Program," Report 2009-0013-AS, 10 July 2009.
41. S. Shane, "Complaint Seek Punishment for Classification of Documents," *New York Times*, 2 Aug. 2011, p. A16.
42. E. Goitein and D. Shapiro, "Reducing Overclassification through Accountability," Brennan Center for Justice, New York Univ., 2011.
43. D. Sanger and J. Peters, "A Promise of Changes for Access to Secrets," *New York Times*, 14 June 2013, p. A18.

Susan Landau is the author of *Surveillance or Security? The Risks Posed by New Wiretapping Technologies* (MIT Press 2011) and coauthor of *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press 2007), and a former Sun Microsystems Distinguished Engineer. She has testified on wiretapping issues to Congress and has written extensively on the subject. Contact her at susan.landau@privacyink.org.

Got an idea for a future article or comments about this one?
Email lead editor Kathy Clark-Fisher at kclark-fisher@computer.org.