

Making Sense of Snowden, Part II: What's Significant in the NSA Revelations

Susan Landau, Google

When *The Guardian* began publishing leaked documents from the National Security Agency (NSA) on 6 June 2013, each day brought startling news. From the NSA's collection of metadata records of all calls made within the US¹ to programs that collected and stored data of "non-US" persons² to the UK Government Communications Headquarters' (GCHQs') interception of 200 transatlantic fiberoptic cables at the point where they reached Britain³ to the NSA's penetration of communications by leaders at the G20 summit, the pot was boiling over. But by late June, things had slowed to a simmer. The summer carried news that the NSA was partially funding the GCHQ's surveillance efforts,⁴ and *The Guardian* had, under pressure from the UK government, destroyed hard drives containing the secret files leaked by NSA contractor Edward Snowden.⁵ But the general focus had shifted to governments: What was legal? Appropriate? Would anyone choose—or be able—to rein in the NSA's extensive surveillance efforts?

Everything changed in September, when *The Guardian* detailed NSA compromises of internationally used cryptographic standards.⁶ Although for decades the NSA was rumored to have weakened specific deployments, compromising

a widely used cryptographic standard has vastly wider impact, especially because industry relies so heavily on secure Internet commerce. Then *The Guardian* and *Der Spiegel* revealed extensive, directed US eavesdropping on European leaders⁷ as well as broad surveillance by its fellow members of the "Five Eyes": Australia, Canada, New Zealand, and the UK. Finally, there were documents showing the NSA targeting Google and Yahoo's inter-datacenter communications.^{8,9}

I summarized the initial revelations in the July/August issue of *IEEE Security & Privacy*.¹⁰ This installment, written in late December, examines the more recent ones; as a Web extra, it offers more details on the teaser I wrote for the January/February 2014 issue of *IEEE Security & Privacy* magazine (www.computer.org/security). The road through this complex story has many technical, policy, and legal twists and turns. I begin with a brief background on wiretap law. Then to explain the significance of the new revelations, I focus on three main threads of the new story—collection of stored metadata, surveillance of communications content, and security hacks—revealing what we've learned from the more recent set of leaked documents. (The Electronic Frontier Foundation has a full set of leaked documents to date at <https://www.eff.org/nsa-spying/nsadocs>.)

Unless otherwise stated, bylined articles, as well as product and service descriptions, reflect the author's or firm's opinion. Inclusion does not necessarily constitute endorsement by the IEEE or the IEEE Computer Society.

THE PLAYERS: A GLOSSARY

- **FISC:** the Foreign Intelligence Surveillance Court. FISC is the US court responsible for authorizing foreign intelligence wiretaps under the Foreign Intelligence Surveillance Act and its amendments. FISC operations are conducted in secret.
- **Five Eyes:** an intelligence-sharing alliance between Australia, Canada, New Zealand, the US, and the UK (sometimes called the “club between English-speaking powers,” as described in *The Guardian*). There are agreements that members of the Five Eyes don’t spy on one another, but according to one of the leaked documents, the rules changed in 2007. The NSA was permitted to unmask and store incidentally collected information on British citizens (J. Ball, “US and UK Struck Secret Deal to Allow NSA to ‘Unmask’ Britons’ Personal Data,” *The Guardian*, 20 Nov. 2013). (“Incidentally collected information” means the individual was not a specific target of surveillance and data had been collected incidentally.) A draft 2005 NSA document discussed unilaterally conducting intelligence operations against Five Eyes citizens; it’s unclear whether this policy was implemented.
- **GCHQ:** Government Communications Headquarters, the UK signals and communications intelligence agency.
- **NSA:** the National Security Agency, the US government agency responsible for collecting signals and communications intelligence. The NSA also has responsibility for protecting US military, diplomatic, and intelligence communications.
- **NIST:** the National Institute of Standards and Technology. Originally known as the National Bureau of Standards, NIST is the US Department of Commerce organization tasked with, among other things, the development of federal civilian agency computer security standards and guidelines, including the development of cryptographic standards.

Wiretap under the Law

US wiretap law must comply with the Fourth Amendment, which requires that warrants “particularly describe the place to be searched, and the persons or things to be seized”; note, however, that the amendment doesn’t necessarily apply outside the US.

In 1990, the US Supreme Court ruled that non-US persons do not enjoy Fourth Amendment protections outside the US (*United States v. Verdugo-Urquidez*, 494 US 259, 1990), and US foreign intelligence wiretap law distinguishes between US persons and non-US persons. (A US person is a US citizen, a permanent resident, a US-based corporation that doesn’t include a foreign government, or a group consisting mainly of the previous categories.) Outside the US, a target is treated as a non-US person unless there is evidence to the contrary, whereas inside the US, a target is assumed to be a US person unless there is evidence to the contrary. Not unexpectedly, this distinction in protections for US and non-US persons doesn’t sit well with the rest of the world.

The basic US wiretapping laws, Title III of the 1968 Omnibus Crime Control and Safe Streets Act and the 1978 Foreign Intelligence Surveillance Act (FISA), lay out wiretap warrant procedure; both require specific, articulable cause for the highly invasive search. Because wiretaps are a secret form of search, the warrant process is intended to be particularly rigorous. FISA wiretap warrants are adjudicated by the Foreign Intelligence Surveillance Court (FISC), whose deliberations are secret.

Relying on the rationale that FISA didn’t require warrants for radio communications where the broadcast reached outside the US,¹¹ after the September 11, 2001, attacks, the Bush administration began a program permitting warrantless wiretapping if one end of the communication was believed to be outside the US. This was eventually formalized in the 2007 Protect America Act and then in the 2008 FISA Amendments Act.

Other nations also instituted wiretapping laws that eliminated warrant requirements for international communications. For example, the UK’s 2000 Regulation of Investigatory Powers Act also permits warrantless wiretapping if one end of the communication is outside the UK. Because of the vagaries of communications paths, purely domestic UK traffic may exit and then reenter the nation’s boundaries, resulting in also subjecting domestic traffic to warrantless wiretapping. Similarly, in 2008, Sweden passed its New Signal Surveillance Act permitting warrantless access to communications transiting the country; there are indications it did so at the request of the US.¹²

The distinction between searches of content and searches of metadata is an important one in US wiretapping law. There are strong legal protections for US persons regarding searches of communications content. But communications metadata isn’t considered as private as content because it’s shared with third parties—the telephone companies and ISPs that deliver it—and US law provides significantly lower legal protections to metadata. It is to the metadata search I now turn.

Stored Metadata

In spring 2006, *USA Today* reported that the US government was collecting the phone call records of “tens of millions” of Americans with data provided by AT&T, Verizon, and Bell-South.¹³ In part because there was no hard evidence of the metadata collection, public interest stayed focused on the warrantless wiretapping disclosed several months earlier by *The New York Times*.¹⁴ Interest changed when *The Guardian* displayed a FISC order requiring the Verizon Business Network to deliver daily telephony metadata for all domestic calls.¹⁵

US law allows collection of some stored metadata through a subpoena or National Security Letter; much greater collection occurs under the USA PATRIOT Act. Metadata collection simply requires that the information be relevant to an ongoing investigation, a relatively low level of proof. How much data is collected under this program? According to the NSA, the agency “touches” 1.6 percent of the 1,826 Pbytes traversing the Internet daily, and of this, only 0.025 percent is “selected for review” (www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf). This figure is a bit misleading, as much Internet traffic consists of movies, music, and other forms of file sharing (such as downloads of open source operating systems, large datasets including medical imagery, and NASA data).

After the initial leaks, the Obama administration emphasized that the government wasn’t warrantlessly wiretapping domestic calls. But in an age of ubiquitous mobile communications, metadata is what matters. Metadata lays bare an individual, revealing what he or she does. Metadata provides location information, showing where people were and whom they met (or, at least, whose cell phone was nearby). Analysis of metadata can expose organizational structure, whether a merger is imminent, a person’s sexual orientation, or even job loss or pregnancy.^{16–20} But while changes in technology—mobile phones, smartphones, apps that rely on location—vastly changed the importance and value of metadata, US law hasn’t kept up, instead permitting the government’s collection of such information with minimal legal protections. After the 9/11 attacks, even these protections lessened substantially, although this fact was not immediately obvious—even to lawmakers.

In the 2001 USA PATRIOT Act, Congress authorized the collection of business records to protect against international terrorism and clandestine intelligence activities; the expectation was that this would target only people under suspicion. So the collection of bulk telephony metadata was a surprise to many people, including members of Congress. The data was collected daily, operating almost like real-time collection. And the order appeared to permit the collection of location data; it specified that the “trunk identifier” could be collected. Both a draft 2009 NSA Inspector General report later released by Snowden¹¹ and an explicit denial by Department of Justice Deputy Attorney General James Cole—“We don’t get any cell site or location information as to where any of these phones

were located”²¹—indicated otherwise. In August, *The Washington Post* reported that the NSA had made a number of errors and mistakenly collected thousands of records of calls to which it was not entitled.²² Let’s unpack these three issues—bulk collection of metadata, collection of location data, and errors and mistaken collection—separately.

The FISC permits no wholesale data mining of communications metadata. A search must be based on “specific and articulated facts, that an identifier is associated with specific foreign terrorist organizations” (www.fas.org/sgp/news/2013/06/ic-back.pdf). The NSA was permitted to query the database based on an identifier satisfying a reasonable and articulable suspicion (RAS) criterion. Using the identifier as a seed, the NSA could search the metadata for numbers called by that number (or target emails mailed by a seed email address), the numbers called by those numbers, and finally numbers called by those numbers (so three “hops” from the seed). RAS requirements meant that the NSA couldn’t search the database for “interesting” patterns of communication, such as those employed by a terrorist group. In 2012, 288 unique identifiers met the RAS standard permitting a database search.²³

Other controls were in place. Only 22 NSA employees were allowed to search the database.²⁴ Moreover, information pertaining to a US person wasn’t to be disseminated outside the NSA unless one of seven people holding senior positions at the NSA approved doing so—though a leaked Memorandum of Understanding between the US and Israel indicates this rule isn’t always upheld (www.theguardian.com/world/interactive/2013/sep/11/nsa-israel-intelligence-memorandum-understanding-document).

Terrorists typically conduct short calls, use burner phones (prepaid phones exploited for brief periods of time and discarded), collaborate on Internet documents (thus not actually “sending” such documents to each other), and work to avoid discovery. The Bush administration sought to work around this terrorist tradecraft by authorizing various wiretapping programs after the 9/11 attacks; this included bulk collection of stored telephony and Internet metadata. The argument for bulk collection was that only through having the full metadata could the NSA track the terrorists; otherwise, “it might not be possible to identify telephony metadata across different networks,” as Principal Deputy Assistant Attorney General Peter Kadzik noted in a letter to Representative F. James Sensenbrenner Jr. on 16 July 2013. NSA Director General Keith Alexander claimed that bulk metadata collection “will substantially increase NSA’s ability to detect and identify the [terrorist-affiliated] Foreign Powers and those individuals affiliated with them” (www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf).

Decisions on collection have been largely hidden from the public. In 2004, there was a showdown over the legality of the bulk collection of Internet metadata¹¹; the White House turned to the FISC for a decision. Judge Colleen Kollar-Kotelly granted broad power to the state: “[T]he Court finds that any

ambiguity on this point should be resolved in favor of including the proposed collection [of stored metadata] within these definitions, since such an interpretation would promote the purpose of Congress” (www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf). This momentous decision was made in secret.

The court decided bulk collection wasn’t a problem. Judge Kollar-Kotelly ruled, “the Government need not make a showing that it is using the least intrusive method possible.” In a later opinion (www.emptywheel.net/2013/11/20/the-john-bates-internet-metadata-opinion-probably-dates-to-july-2010), FISC Judge John Bates concurred, ruling that because determining in advance what information investigators was needed was impossible, bulk acquisition of stored metadata was appropriate.

The court should have considered alternatives. Using AT&T decades’ worth of call records—including those of calls that pass through AT&T switches—the US Drug Enforcement Administration and AT&T coordinated to track drug dealers.²⁵ AT&T is able to trace burner phones as well new phones added by the target (www.nytimes.com/interactive/2013/09/02/us/hemisphere-project.html). AT&T holds the bulk metadata while government investigators obtain information on particular individuals through subpoenas.²⁵ Could a similar method of leaving the data with communications providers work for tracking terrorists? There is evidence that NSA has already experimented with such an effort (<http://justsecurity.org/2013/10/11/nsa-call-records-database-fingerprinting-burners>).

The Verizon court order appeared to allow the collection of location data. After months of denials by intelligence officials that the NSA was collecting such information, Director of National Intelligence James Clapper acknowledged in October that the NSA had run a pilot project to collect cell phone location data. Clapper claimed that the “data was not used for any other purpose and was never available for intelligence analysis purposes.”²⁶ This was less than the full story. In December, leaked documents revealed an international cell phone location tracking program.²⁷ Through collection of 5 billion records daily, the NSA tracked hundreds of millions of devices, determining their precise location. That the NSA tracked terrorists through cell phone location has been known for more than a decade;²⁸ what’s different here is scale. Rather than focusing on specific terrorist targets, the NSA was conducting a sweeping global collection. The process meant that the NSA also collected purely domestic communications, an anticipated but not deliberate collection.²⁷

In August, *The Washington Post* reported that the NSA “had broken privacy rules or overstepped its legal authority thousands of times”; the paper reported a 2008 programming error that resulted in collecting all communications with area code “202”—the area code for Washington—rather than “20”—the country code for Egypt.²² While the actual number of incidents may seem large—2,716 for the year April

2011 through March 2012—in the context of the amount of data being collected through the metadata program, these errors are in the noise.

Other mistakes, however, were serious. Between 2006 and 2009, agents trawled the database to check if numbers of potential concern satisfied the RAS criteria. The NSA should have had “access to the archived data only when NSA has identified a known telephone number for which ... [there is a] reasonable, articulable suspicion that the number is associated with [blanked-out] organization.”²⁹ But “archived data” meant data stored within the NSA’s analytical repositories³⁰; analysts thought they could query the metadata with numbers received from an alert list. Some domestic numbers from the alert list were used to access the metadata and “produced a sufficient level of suspicion that NSA generated an intelligence report about the telephone number to the FBI and CIA”³⁰—and these had not satisfied the RAS criterion prior to use. Unintentional as the actions might have been, NSA agents were conducting fishing expeditions. In a March 2009 opinion, FISC Judge Reggie Walton noted that the RAS requirement had been “so frequently and systematically violated that it can be fairly said that this critical element of the overall BR [Business Records] regime had never functioned effectively (<https://www.eff.org/document/br-08-13-order-3-2-09-final-redactedex-13-ocr>). For the next six months, NSA could access the metadata only with a FISC order specifying the query; this restriction was lifted once NSA demonstrated it had developed proper procedures for access.”³¹

NSA development of intelligence “product” proceeds through seven steps—access, collection, selection, exploitation, analysis, reporting, and dissemination—with targeting potentially playing a role in each. Access, of course, may take various forms, from a highly specific FISA court order served on a provider in the US through massive nonspecific collection at a fiberoptic cable outside the country. One of the major issues regarding NSA collection is retention. Title III wiretaps for criminal investigations require active minimization, meaning not collecting the communication if it isn’t germane. But FISA collection permits post-acquisition minimization, and the FISC has allowed several-year retention of the unanalyzed communications data (www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf).

Section 702 of the FISA Amendments Act replaced the individualized warrant requirement of FISA with a “targeting” requirement (50 U.S.C.A. section 1881a(a)), which casts a wider net than individualized warrants. Targeting permits acquiring communications not only to or from a subject but also about the subject.³² If one end of a communication is believed to be outside the US—and the NSA appears to spend considerable effort to determining whether this is the case—under section 702, it isn’t just the target that can be the object of warrantless wiretapping but anyone who discusses the target (www.theguardian.com/world/interactive/2013/jun/20/exhibit-a-procedures-nsa-document).

Overtargeting arose in what the NSA calls “‘upstream collections’ of Internet transactions containing multiple communications” (www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf). (“Upstream collection” means tapping on the Internet backbone, rather than at Internet providers.) This can happen when someone uses a Web interface for email and receives a response with information about multiple communications. Under section 702, only one piece of mail of the “multi-communication transaction” (MCT) needs to be to, from, or about a target for the entire MCT to be read by an NSA employee. Thus many of the transactions contained in the MCT might have no relation at all to the NSA selector. Yet the NSA had no procedure for removing information about the extraneous domestic communications that had nothing to do with the target. Complaining that the “NSA’s proposed handling of MCTs tended to maximize the retention of such information” (www.aclu.org/files/assets/november_2011_fisc_opinion_and_order.pdf), the FISC concluded that the MCT targeting and minimization procedures violated the Fourth Amendment (www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%208.pdf). In 2011, the NSA suspended the program for “operational and resource reasons,” and it has not been resumed.³³

That was only part of the problem. Senators Ron Wyden and Mark Udall observed that even if the original collection was accidental, the NSA could still keep and use the data.³⁴

Access occurred largely with the cooperation of US communications providers. Only after the *USA Today* article were communication carriers served with a FISC order; previously, collection relied solely on NSA requests.¹¹ As of this writing, no providers have challenged FISC orders on bulk collection of metadata (www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf).

In mid-December, a federal district court decision turned the situation on its head. Because information about the NSA bulk metadata collection was public, private citizens had standing to challenge the surveillance. Several did so. Writing that “plaintiffs have a substantial likelihood of showing their privacy interests outweigh the Government’s interest in collecting and analyzing bulk telephony metadata,” Judge Richard Leon ordered the government halt the bulk metadata collection. He immediately stayed his opinion pending government appeal—and urged the government be ready to halt the program “when, and if” that decision occurs (*Plaintiffs v. Obama et al. Defendants*, United States District Court for the District of Columbia, Civil Action 13-0851 [RJL]). Two days later, the NSA review panel appointed by President Obama recommended that the government end the program of bulk collection of telephony metadata and replace it with one in which the providers or a private third party do the storage.²³ Meanwhile, in late December, in a different district court case, the NSA metadata collection was ruled legal (<http://online.wsj.com/public/resources/documents/clapper.pdf>).

Content Collection

Immediately after the initial Snowden disclosures, foreign leaders protested the widespread NSA warrantless wiretapping of non-US persons; this issue was already previously known (www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/study_cloud_/study_cloud_en.pdf). Many nations are heavily involved in their own surveillance against other countries, and the complaints quickly grew muted—except for Brazil. There, the NSA’s targeting of the oil and gas company Petrobras—South America’s largest firm—caused great consternation.³⁵ Brazilians were concerned that information was being shared with Petrobras’s competitors. There is no evidence that the US government shares the fruits of espionage with US private industry—and a lot to indicate that it does not¹⁰—and there is certainly an argument that gathering intelligence on Brazil includes gathering intelligence on Petrobras.³⁶ Nonetheless, the Brazilians were furious, feeling basic rules had been violated.

Brazilian president Dilma Rousseff canceled a planned US visit and state dinner with President Obama, a highly unusual move. When news came out that the Brazilian government had been spying on other governments, the government claimed that the situation was different because the spying was in “legal compliance” with Brazilian laws.³⁷ That particular argument may not be very useful. Although the scale of NSA spying may be unprecedented, the actual surveillance could well be in “legal compliance” with US laws (the decision in December 2013 by District Court Judge Leon regarding illegality applies only to domestic communications).

The damped silence over US spying on foreign leaders ended in late October, when *The Guardian* and *Der Spiegel* reported massive surveillance of close US allies. The US had targeted German Chancellor Angela Merkel’s cell phone since 2002, when she was running to become the Christian Social Union’s candidate for chancellor.³⁸ The US embassy in Berlin, which overlooks the Reichstag, appears to host a major NSA listening installation. Such use is illegal in Germany; the Germans were incensed.

At least with respect to leaders of close US allies, NSA spying appears to have crossed the line from routine espionage efforts to a vacuum cleaner effort, with *The New York Times* describing the effort as “no morsel too miniscule” to collect.⁷ Allies were angry, and even some NSA friends backed away. Former NSA Inspector General Joel Brenner commented that “routine targeting of close allies is bad politics and is foolish.”⁷ Then the story got even worse.

Security Hacks

In June, leaked documents disclosed that the GCHQ had been tapping hundreds of transatlantic fiberoptic cables, and in September, we learned the value of those taps. The NSA was compromising various forms of cybersecurity, including cryptography. On one level, this isn’t a surprise; after all, a key goal for a signals intelligence (SIGINT) agency is intelligence.

ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curves, proposed independently by Neal Koblitz and Victor Miller in 1985 for use as public-key cryptosystems, achieve the same level of security as the RSA algorithm but with a decidedly shorter key length (N. Koblitz et al., “The State of Elliptic Curve Cryptography,” *Design, Codes, and Cryptography*, vol. 19, 2000, pp. 173–193). For instance, elliptic curve cryptography (ECC) using a 244-bit key is as secure as RSA with a 2,048-bit key (A. Lenstra and E. Verheul, “Selecting Cryptographic Key Sizes,” *J. Cryptology*, vol. 14, no. 4, 2001, pp. 255–293). This feature gives ECC a clear advantage over RSA in low-power, small memory devices.

The mathematics of elliptic curves is based on points lying on a particular elliptic function ($y^2 = x^3 + ax + b$, for points x , y , a , and b in a finite field). An arithmetic can be defined that consists of “adding” points that lie on the curve; this operation gives the set of points (with an added “point at infinity”) a group structure. Point multiplication—adding a point to itself multiple times—is reminiscent of RSA exponentiation in that it’s computationally easy to do. Inverting that operation, that is, finding the discrete log of a point, is computationally difficult, an aspect that provides the security of ECC.

Not all elliptic curves lead to secure cryptosystems, so various standards organizations provide curves that are strongly believed to be secure. The public part of ECC is the curve (that is, the parameters a and b), the underlying field (which is either a prime field or one of characteristic two), and a generator point G . The fact that various speedups for determining discrete logs over finite fields don’t extend to elliptic curves’ ECC computations enables the use of a smaller key size than RSA computations of the same strength.

But given the national security risks of cyberexploitation and cyberattack, the NSA’s willingness to undermine fundamental aspects of cybersecurity was startling—and reckless.

To put the situation in context, let’s briefly step back to the period when cryptography escaped the NSA’s control. In 1975, the National Bureau of Standards—later renamed the National Institute of Standards and Technology (NIST)—standardized the 56-bit symmetric-key algorithm, the Data Encryption Standard (DES), as in Federal Information Processing Standards (FIPS), enabling it to be used for computer security by US civilian agencies (it was also widely adopted by industry). A year later, Whitfield Diffie and Martin Hellman invented public-key cryptography and digital signatures, beginning a two-decade battle between the US government, academia, and industry over the public’s use of strong cryptography (cryptography difficult to break through brute force). The NSA unsuccessfully sought to restrict publication of cryptographic research.³⁹ But a combination of US government export controls on strong cryptography and NSA interference in developing civilian security standards stymied the development of secure communications systems for the better part of several decades.

In the midst of these disputes, Congress passed the 1987 Computer Security Act, which made NIST responsible for developing security standards for use in civilian agencies. Yet under its technical “advisory” role provided by the law, for more than a decade, the NSA remained largely in charge. For example, the NSA prevented the popular RSA algorithm from becoming the Digital Signature Standard (DSS), arranging instead for an NSA-developed technique to become the DSS. The conflict came to a head in the mid-1990s with the proposal that Clipper, an NSA-designed symmetric-key cryptographic algorithm that escrowed keys with federal agencies, become FIPS.³⁹

Clipper was a failure—it became a standard but was barely used—and this period marked the beginning of the end of NSA dominance of the standardization process. In 1997, NIST launched a well-respected effort to replace DES with a much stronger standard, the Advanced Encryption Standard (AES); in 2000, the US loosened its export controls on strong cryptography.⁴⁰ AES’s success led NIST to conduct a similar competition to replace the hash standard SHA-1, whose weaknesses had become evident by 2005.⁴¹ In 2007, NIST moved ahead on a Secure Hash Algorithm (SHA) competition, in an open process similar to that which had made the AES effort such a success. In 2012, NIST announced that SHA-3 would be Keccak, a Belgian-Italian submission. Then NIST surprised the cryptography world: in August 2013, it proposed standardizing an abbreviated Keccak that would diminish the algorithm’s preimage resistance (ability to find an element that hashes to a particular image).⁴² This change didn’t trouble the Keccak designers, but others had objections. Then came Snowden’s remarkable revelations.

It appeared that the NSA had subverted NIST’s standardization process. The algorithm in question was the Dual Elliptic Curve Digital Random Bit Generator (EC-DRBG), a random bit generator based on elliptic curve arithmetic. Random numbers are crucial for cryptography, but generating them properly is difficult. The usual method is to take some genuinely random numbers and, through a mathematical function, stretch them into a longer pseudorandom number. NIST’s Special Publication SP 800-90 presents four ways of doing this.⁴³ Three were standard techniques using hash functions and block ciphers. One, the Dual EC-DRBG, used public-key cryptography, specifically, the elliptic curve cryptography (ECC) algorithm. Its inclusion was odd because public-key cryptography algorithms run significantly more slowly than hash functions and block ci-

phers. An algebraically based generator is frequently included because it enables proofs of security (that is, proofs of some security features; this was the case, for example, with AES).⁴⁴ But no such proofs were offered with Dual EC-DRBG. (Although none of the quoted documents specified that Dual EC-DRBG was the standard in question, various smoking guns strongly pointed in that direction.)

Two oddities stood out about Dual EC-DRBG: there was no explanation of how two default parameters in the system were chosen, and the random bit generator provided more bits than was safe, biasing the outcome—and enabling guessing the input without too much work (<http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html>). The concerns were justified. Months after the standard was published, two Microsoft researchers, Dan Shumow and Niels Ferguson, showed that if an attacker knew the relationship between the two parameters, then the extra bits put out by the random bit generator would let him or her predict future random bits (<http://rump2007.cr.yp.to/15-shumow.pdf>).

How did NIST approve a standard with such a glaring weakness? Leaked NSA documents explained: “[NSA’s] SIGINT enabling project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products’ designs. These changes make the systems in question exploitable” (www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html). The signals intelligence agency worked to “[i]nset vulnerabilities into commercial encryption systems ... [i]nfluence policies, standards, and specifications for commercial public key technologies.”

In December, Reuters reported that NSA paid RSA Security US\$10 million to make Dual EC-DRBG the default algorithm in its BSAFE toolkit (www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220), a decision that, notably, was made in 2004 by its business personnel and not the company’s cryptographers. With NSA and some vendors of security products seeking to have Dual EC-DRBG made into a standard, NIST did so.

After the Reuters article appeared, RSA Security denied it had engaged in a “secret contract ... to incorporate a known flawed random number generator” into its product (<https://blogs.rsa.com/news-media-2/rsa-response>). The company’s blog posting explained neither why Dual EC-DRBG was made the default despite being significantly slower than alternatives nor why Dual EC-DRBG continued to be used after Microsoft researchers had raised concerns about its security in 2007. (Interestingly, Microsoft had not originally included support for Dual EC-DRBG in Vista. According to *Wired*, support was added after a major customer requested it; even then, the algorithm wasn’t made the default.)

The leaked documents showed that the NSA viewed its role in pushing through a 2006 draft security standard as “an exercise in finesse.”⁴⁵ (While the subversion of Dual EC-DRBG

enables the NSA to read traffic that relies on the Dual EC-DRBG for random bit generation, this attack doesn’t enable those without the knowledge of the relationship between the parameters to do so.) It appears that the NSA’s SIGINT division viewed corrupting cryptography standards as a goal. If other governments had done such a thing, the US would have been outraged. The NSA’s actions damaged communications security infrastructure, communications security companies, and the communications security standardization process.

As a result of the compromise of Dual EC-DRBG, some implementations of SSL/TLS weren’t secure against the spy agency. More specifically, if Dual EC-DRBG was used to generate the “Client Cryptographer Nonce” at the beginning of an SSL connection, the NSA could predict the “Pre-Master Secret” used in the SSL RSA handshake, enabling it to decrypt the encrypted transmission (<http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html>).

The NSA’s audacious actions badly damaged trust in NIST and its standards process, previously viewed as objective and effective. The standards agency responded immediately, deprecating the Dual EC-DRBG standard⁴⁶ and starting a formal review of its own standards development process (<http://csrc.nist.gov/groups/ST/crypto-review/index.html>). NIST believed the revised Keccak to be secure, but in an effort to reestablish trust with the cryptography community, NIST recommended Keccak be adopted as originally proposed (<http://csrc.nist.gov/groups/ST/hash/sha-3/documents/kelsey-email-moving-forward-110113.pdf>).

Other security technologies were also in the NSA’s gun-sights; one such was Tor (www.torproject.org), a service for anonymizing Internet communications. Tor was originally developed at the US Naval Research Laboratory but is used today by journalists, human rights workers, and law enforcement officers (who might want to hide their affiliation while performing investigations into, say, chat rooms). It is used, in short, by those with reason to hide with whom they are communicating. Because of Tor’s value to human rights and military personnel working overseas, it has been funded by the US Department of State and various US government agencies.

Tor developers have long understood that an adversary with capability for monitoring a high percentage of network traffic can compromise Tor’s capabilities, and indeed, the NSA has been able to identify Tor users through studying traffic patterns (www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document). The agency is then able to read traffic of those users through exploiting vulnerabilities on their system (for example, by downloading software that subverts the browser’s intent). But Tor’s robustness also came out clearly; in a presentation entitled “Tor Stinks,” the NSA concluded, “We will never be able to de-anonymize all Tor users all the time” (www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document).

Documents leaked in December show that NSA had broken GSM, an algorithm developed in the 1980s for securing

communications on G2 networks (<http://apps.washingtonpost.com/g/page/world/how-the-nsa-pinpoints-a-mobile-device/645/#document/p1/a135574>). Beginning in 1999, academic cryptographers developed increasingly better attacks on GSM (<http://cryptome.org/a51-bsw.htm>), and thus newer 3G and 4G networks employ stronger cryptography. But GSM nonetheless remains in wide use in many parts of the world, and thus NSA's attack is effective.

The concern about commerce and economic security continues with more recent leaks. In June, leaked documents showed that since July 2009, the GCHQ had been able to collect 2.5 Gbits per second of data flowing through the transatlantic fiberoptic cables (access was 10 Gbits per second in 2010 and has been steadily increasing since then; <http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553>). It was clear that the NSA was processing communications of interest, say, from another's government's trade mission or defense ministry. There were other documents of interest as well. October leaks showed that the NSA was collecting inter-datacenter traffic at both Google and Yahoo.⁸ (Disclaimer: I work for Google, but the opinions expressed in this article are mine and not those of my employer. Furthermore, any material presented here concerning Google comes solely from public sources.) This wasn't front-end access with a warrant; it was back end and apparently without the companies' knowledge. *The Washington Post* reported that the NSA had collected 181,280,466 new records in the previous 30 days (some of which was metadata).⁸

Concerns about NSA data collection run high among Internet companies, and many were deeply angered by the NSA actions.⁴⁷ Google's Chief Legal Officer, David Drummond, wrote, "We do not provide any government, including the U.S. government, with access to our systems. We are outraged at the lengths to which the government seems to have gone to intercept data from our private fiber networks, and it underscores the need for urgent reform."⁴⁸

Months earlier, Google had begun encrypting inter-datacenter communications, and the initial NSA leaks caused the company to accelerate efforts.⁴⁹ After the October news, both Yahoo and Microsoft announced their intent to do the same.^{50,51}

Such protections are aligned with the companies' interests—namely, security of their users' data—and their earlier legal stance. Unlike telecommunications providers, which not only didn't challenge the broad collection of stored metadata but in some cases provided unlimited access to undersea cables,⁵² the Internet companies have been more active in their response. Yahoo contested a FISC order (this wasn't known until the Snowden leaks), and since 2010, Google has been publishing transparency reports, revealing the number of government requests for criminal data the company receives as well as general figures about National Security Letters. Other Internet companies have since joined that effort. The Internet companies are pressing for permission to publish more de-

tailed data regarding their responses to FISA orders; meanwhile, the president's review committee urged legislation authorizing "telephone, Internet, and other providers" to begin issuing transparency reports.²³

The long-term impact—loss of trust in US Internet and security companies and consequent loss of business—doesn't appear to have been factored into the NSA's decision to conduct the interception. Early reports claimed that the interception could ultimately result in US companies losing tens of billions of dollars because of avoidance of US-based datacenters (www2.itif.org/2013-cloud-computing-costs.pdf). One can expect a similarly severe impact on the US cybersecurity industry as a result of the NSA activities at RSA Security.

Is All This Surveillance Effective?

The threat of surveillance helps keep terrorists off electronic communications, a clear win. But does surveillance provide any further protection?

Too much data has been a problem. Apparently, "the steady stream of telephone numbers, email addresses and names" the NSA sent to the FBI in the period after 9/11 inundated agents, preventing them from focusing on the more serious leads.⁵³ Other agencies at other times have found the overwhelming amount of information has hidden the important nuggets from investigators.⁵⁴ Even the NSA has found too much collection: a leaked document regarding collection from internal Yahoo datacenters states, "Numerous S2 [signals intelligence] analysts have complained of ... the relatively small intelligence value it contains does not justify the sheer volume of collection" (<http://apps.washingtonpost.com/g/page/world/how-the-nsas-muscular-program-collects-too-much-data-from-yahoo-and-google/543/>). Diverting resources from more effective forms of investigation is not useful.

Evaluating effectiveness of the NSA wiretapping efforts remains difficult. It isn't always appropriate to explain how terrorist plots have been thwarted, for those discussions can expose too much about sources and methods. But it seems, in fact, that selective disclosure has been used to claim stronger results from the NSA surveillance than are justified.¹⁰ In October, some clarity finally emerged during a Senate hearing:

Senator Patrick Leahy: "We've heard over and over the assertion that fifty-four terrorist plots were thwarted by the use of section 215 and/or section 702 authorities. That's plainly wrong. ... These weren't all plots and they weren't all thwarted. ... The American people are getting left with an inaccurate impression of the effectiveness of NSA programs. Would you agree that the fifty-four cases that keep getting cited by the administration were not all plots and of the fifty-four, only thirteen had some nexus to the US? Would you agree with that, yes or no?"

General Alexander: "Yes."

Senator Leahy: "At our last hearing, Deputy Director Inglis

testified that there's only really one example of a case where, but for the use of section 215 bulk phone records collection, terrorist activity was stopped. Is Mr. Inglis right?"

General Alexander: "He's right. I believe he said two."

The Snowden leaks raise many questions about proportionate behavior. As more data emerges, clearly, along with privacy, effectiveness and proportionality should be key concerns.

Will Oversight Help?

Secrecy has created much of the problem of the NSA surveillance, from whether the collection follows the intent of Congress to issues of whether collection follows the rules laid down by the FISC. Secrecy prevents public discussion and public vetting. In its place has been the FISC and Congress, but there is serious question whether they have been able to conduct proper oversight.

One impact of the leaks has been an unprecedented release of previously classified FISC opinions. The July 2010 decision by FISC Judge Bates notes a number of problems with NSA collection of metadata (www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf):

- "During the initial period of authorization, the government disclosed that NSA's acquisitions had exceeded the scope of what the government had requested and that the FISC had approved";
- "'virtually every PR/TT [pen register/trap-and-trace—these collect communications from and to a device] record' generated by this program included some data not authorized for collection"; and
- "the extraordinary fact that NSA's end-to-end review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired."

In many cases, noncompliance went on for months, if not years. Although Judge Bates noted, "The history of misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection," the NSA was allowed to continue the bulk metadata collection program.

Such lack of control wasn't unusual. In an opinion issued in October 2011, Judge Bates noted that "the Court understood that acquisition of Internet communications under Section 702 would be limited to discrete 'to/from' communications between or among individual user accounts and to 'about' communications falling within specific categories. ... In conducting and granting these approvals, the Court did not take into account NSA's acquisition of Internet transactions, which now materially and fundamentally alter the statutory and constitutional analysis" (www.dni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%202.pdf). In other words, the FISC had consented

to certain type of Internet wiretapping without fully understanding what collection would consist of. As noted earlier, this program was voluntarily ended by NSA in 2011.

Oversight by Congress was less stringent, in part because elected officials may only check issues with cleared staff. Some members, especially Senators Wyden and Udall, tried hard to bring light to hidden corners; however, until the Snowden leaks, they were largely unsuccessful.

A recent statement by presiding FISC Judge Walton pointed out another concern: "The FISC does not have the capacity to investigate issues of noncompliance."⁵⁵ In fact, the decisions of other US courts are publicly disclosed, leaving noncompliance open to examination. That isn't possible for FISC rulings.

A Difference in Scale Creates a Difference in Kind

Every nation spies; scale is what differs here. No other nation has the surveillance capability that the US has, capability that has been augmented by relying on partners—not only the Five Eyes, but other countries as well.⁵⁶ In turn, these other nations have also benefitted from the extensive eavesdropping network.⁵⁷ The underlying question is to what purpose this capacity has been put.

The NSA's vast increase in SIGINT capabilities occurred in the wake of terrorist attacks and with the avowed goal of preventing future such attacks. However, the leaks show spying on allies, eavesdropping on US Internet companies' internal communications, and promulgating broken cryptographic standards. Surveillance capabilities have increasingly been used to achieve diplomatic advantage over allies and economic advantage over competitors.⁷

But what are the costs? The US has suffered a serious loss of ability to achieve goals through "soft power"⁵⁸; this includes a reduced capability to press for freedom of Internet protocols and communications. US Internet companies fear a sharp loss of business as other nationals eschew US-based services. And adoption of cryptographic standards could fracture as a result of the corruption of the NIST process with Dual EC-DRBG. The surveillance has caused a massive loss of trust: loss of trust in NSA, in NIST, and in the US government as an ally. It will have a severe impact in moving forward on efforts to increase cybersecurity.

Responses and Long-Term Implications

At the end of last summer, the leaks appeared to produce noise but little action. A close vote in Congress addressed the NSA's bulk collection of metadata but posed no serious threat to the NSA. The proposals offered by President Obama in August appeared relatively mild:

- changes to section 215 of the USA PATRIOT Act providing greater oversight, greater transparency, and constraints on use;
- an independent voice at the FISC to represent the civil lib-

erties side of cases;

- declassification of a number of materials including FISC decisions (some of which are quoted here);
- a Department of Justice explanation of the legal rationale for the section 215 bulk metadata collection; and
- an outside review board to examine intelligence and telecommunications.

The autumn NSA revelations were politically devastating. These were followed by the DC District Court decision on bulk metadata collection and the report by the outside review board. The board made numerous recommendations for fundamental change in NSA collection, including substantively narrowing the rules under which third-party data can be collected by the government, much greater public disclosure of NSA data collection efforts, a requirement that surveillance of non-US persons outside the US be limited exclusively to national-security purposes, and, as mentioned earlier, end of NSA bulk collection of telephony metadata in favor of provider or third-party storage.²³

The confluence of the newest revelations, the court decisions, and the review committee's report may result in serious reform. Just as 1970s congressional activity—the Church Committee—developed controls on national security wiretapping, the time again seems ripe to revise controls on intelligence gathering. But what shape these may take is difficult to predict.

The NSA's surveillance hasn't occurred in a vacuum. Until the NSA leaks, cybersecurity and cyberexploitation had dominated discussions of communications security. They have—probably temporarily—taken a backseat to the news of the surveillance, but they remain as serious issues as they were previous to the leaks. Even though some companies have developed sophisticated technologies, the private sector can't go it alone on cybersecurity.

The nature of government's role remains to be seen. As the international need for cyber protections becomes even more crucial, signals intelligence agencies will be called in to help. Then the restrictions placed on the NSA may work in its favor, providing enough controls for its critics to trust its participation in this sphere.⁵⁹ Thus, perhaps the real issue to discuss now is the right restraints to place on an agency that may, in the end, be called on to provide civilian-sector cybersecurity (voluntarily, of course).

NIST must work to regain trust for its processes of creating security and cryptography standards. NIST brings depth and organization, as well as a reputation for handling pressure from industry, to the standardization process; volunteer groups such as the Internet Engineering Task Force don't have the capacity to step into that role. Although organizations in Europe and elsewhere would like to fill NIST's role, it's unlikely that they will be able to do so. But if NIST is to maintain its position, the agency must first convince the standards world that it is worthy of the trust placed in it.

The NSA revelations didn't end when *The Guardian's* editors destroyed their copies of the leaked documents. Copies of those files were in Brazil, where journalist Glenn Greenwald, who broke the story, resides, and in the US, where *The Guardian* had entered into a joint publishing arrangement with *The New York Times*. One of the great ironies of the Snowden documents is that because the US First Amendment guarantees freedom of the press, the US government must let publication continue.

That amendment, like others in the US Bill of Rights and in the UN Universal Declaration of Human Rights, illuminates much of what has gone wrong. In 2001, when the NSA's massive surveillance began, there was no bulk collection of stored metadata, no FISA Amendments Act allowing warrantless collection of communications where one end of the communication was outside the US, and no site in Utah capable of collecting many exabytes of data.⁶⁰ In 2001, the Internet might not have been the beacon of freedom and free speech that many idealists dreamed it could be, but it wasn't subject to a massive surveillance system either.

As long as criminal and terrorist activity exist, it won't be possible to abolish government surveillance. Yet communications systems can be designed with communications security in mind. Several important principles should govern the deployment of communications surveillance systems:

- Communications surveillance systems should be designed with the idea of providing long-term security.²⁰ Technology and laws come and go, but installed infrastructure persists for decades. As the preamble to the US Constitution observes, we should secure the blessing of liberty for posterity.
- Any suppression of communications privacy protections should occur only in periods of extreme emergency and must be for brief—and quite temporary—periods of time.²⁰ Over the past decade, warrantless wiretapping was directed first at Afghanistan, then at Iraq, and later expanded to become permanent.
- Communications surveillance shouldn't impede the working of the press. The press are our canaries in the coal mine; if journalists are routinely subjected to communications surveillance, the public will soon be.²⁰

In 1961, President John F. Kennedy said in his inaugural address that the US would “pay any price, bear any burden ... to assure the survival and the success of liberty.” The principles above, essential to freedom and liberty, were badly violated by the last decade's massive development of NSA surveillance, surveillance that was aided by a number of other nations. Whether it is now possible to use technical, policy, and legal means to wrest back a modicum of privacy and security in human communications remains to be seen. Doing so will require that governments, including the US, act on the principle that knowing everything may not be the best way to ensure global

security. Only then may it be possible to reestablish the level of communications privacy “necessary for freedom, security, human dignity, and the consent of the governed.”²⁰

Acknowledgments

Many thanks to Steve Bellovin, Matt Blaze, Robin Bloomfield, Jeremy Epstein, William Horne, Neil Immerman, Hilarie Orman, Shari Lawrence Pfleeger, and Lee Tien for their very useful comments. Any remaining errors are my responsibility.

References

- G. Greenwald, “NSA Collecting Phone Records of Millions of Verizon Customers Daily,” *The Guardian*, 6 June 2013.
- G. Greenwald, “NSA Prism Program Taps in to User Data of Apple, Google and Others,” *The Guardian*, 7 June 2013.
- E. MacAskill et al., “GCHQ Taps Fibre-Optic Cables for Secret Access to World’s Communications,” *The Guardian*, 21 June 2013.
- N. Hopkins and J. Burger, “Exclusive: NSA Pays 100 Million Pounds in Secret Funding for GCHQ,” *The Guardian*, 1 Aug. 2013.
- J. Borger, “NSA Files: Why The Guardian in London Destroyed Hard Drives with Leaked Files,” *The Guardian*, 20 Aug. 2013.
- J. Ball, J. Borger, and G. Greenwald, “Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security,” *The Guardian*, 5 Sept. 2013.
- S. Shane, “No Morsel Too Miniscule for All-Consuming NSA,” *The New York Times*, 3 Nov. 2013.
- B. Gellman and A. Soltani, “NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say,” *The Washington Post*, 30 Oct. 2013.
- N. Perlroth and J. Markoff, “NSA May Have Penetrated Internet Cable Links,” *The New York Times*, 25 Nov. 2013.
- S. Landau, “Making Sense of Snowden: Putting the NSA Revelations in Context,” *IEEE Security & Privacy*, vol. 11, no. 4, 2013, pp. 54–63; <http://doi.ieeecomputersociety.org/10.1109/MSP.2013.90>.
- Office of the Inspector General, “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.
- D. Campbell, NSA Hearing, European Parliament, 2013, www.youtube.com/watch?v=Cu6accTBjfs&feature=youtu.be&t=2h52m25s.
- L. Cauley, “NSA Has Massive Database of Americans’ Phone Calls,” *USA Today*, 11 May 2006.
- J. Risen and E. Lichtblau, “Bush Lets US Spy on Callers without Courts,” *The New York Times*, 16 Dec. 2005.
- US Foreign Intelligence Surveillance Court, “In Re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services Inc., on Behalf of MCI Communication Services Inc. D/B/A Verizon Business Services,” Docket BR 13-80, 25 Apr. 2013.
- C. Jernigan and B. Mistree, “Gaydar: Facebook Friendships Expose Sexual Orientation,” *First Monday*, vol. 14, no. 10, 2009.
- N. Eagle, A. Pentland, and D. Lazer, “Inferring Friendship Network Structure by Using Mobile Phone Data,” *Proc. Nat’l Academy of Sciences*, vol. 106, no. 36, 2009, pp. 15274–15278.
- G. Danezis and R. Clayton, “Introducing Traffic Analysis: Attacks, Defences, and Public Policy Issues,” *Attacks, Defences, and Public Policy Issues*, CRC Press, 2007.
- P. Golle and K. Partridge, “On the Anonymity of Home/Work Location Pairs,” *Proc. 7th Int’l Conf. Pervasive Computing*, May 2009.
- S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
- J. Cole, Testimony, House of Representatives, Select Committee on Intelligence, Hearing on “Disclosure of National Security Agency Surveillance Programs,” 18 June 2013.
- B. Gellman, “NSA Broke Privacy Rules Thousands of Times per Year, Audit Says,” *The Washington Post*, 15 Aug. 2013.
- R. Clarke et al., *Liberty and Security in a Changing World: Report and Recommendations of the President’s Group on Intelligence and Communications Technologies*, 2013.
- C. Inglis, Statement, House Permanent Select Committee on Intelligence, Hearing on “How Disclosed NSA Programs Protect Americans, and Why Disclosure Aids Our Enemies,” 18 June 2013.
- S. Shane and C. Moynihan, “Drug Agents Use Vast Phone Trove, Eclipsing NSA’s,” *The New York Times*, 1 Sept. 2013.
- C. Savage, “In Test Project, NSA Tracked Cell Phone Locations,” *The New York Times*, 2 Oct. 2013.
- B. Gellman and A. Soltani, “NSA Tracking Cellphones Worldwide, Snowden Documents Show,” *The Washington Post*, 4 Dec. 2013.
- D. Van Natta Jr. and D. Butler, “How Tiny Swiss Cellphone Chips Helped Track Terror Web,” *The New York Times*, 4 Mar. 2004.
- US Foreign Intelligence Surveillance Court, “In Re Production of Tangible Things XXX,” Docket BR06-05.
- US Foreign Intelligence Surveillance Court, “In Re Production of Tangible Things XXX,” Declaration of Lieutenant General Keith B. Alexander, Docket BR08-13.
- US Foreign Intelligence Court, “In Re Production of Tangible Things from XXX,” Docket No. BR09-13, 3 Sept. 2009.
- House Permanent Select Committee on Intelligence, House of Representatives, Foreign Intelligence Surveillance Act, “House Report, No. 95-1283, pt. I,” Ninety-Fifth Congress, Second Session, 8 June 1978.
- J. Clapper, Letter to Senator Ron Wyden, 26 July 2013; www.wyden.senate.gov/download/?id=285dc9e7-195a-4467-b0fe-caa857fc4e0d.
- J. Ball and S. Ackerman, “NSA Loophole Allows Warrantless for US Citizens’ Email and Phone Calls,” *The Guardian*, 9 Aug. 2013.
- J. Watts, “NSA Accused of Spying on Brazilian Oil Company Petrobras,” *The Guardian*, 9 Sept. 2013.
- C. Helman, “Of Course the NSA Should Be Spying on Petrobras,” *Forbes*, 9 Sept. 2013.
- S. Romero, “Brazil Says It Spied on US and Others inside Its Borders,” *The New York Times*, 4 Nov. 2013.
- “Embassy Espionage: NSA’s Secret Spy Hub in Berlin,” *Der Spiegel*, 27 Oct. 2013.
- W. Diffie and S. Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption*, MIT Press, 2007.
- Department of Commerce, Bureau of Export Administration, “15 CFR Parts 734, 740, 742, 770, 772, and 774, Docket No. RIN: 0694-AC11, Revisions to Encryption Items,” 14 Jan. 2000.
- X. Wang, Y. Lisa Yin, and H. Yu, “Finding Collisions in the Full SHA-1,” *Advances in Cryptology (CRYPTO ’05)*, Springer Verlag, 2005, pp. 17–36.
- J. Kelsey, “SHA3: Past, Present, and Future,” presentation, *Workshop Cryptographic Hardware and Embedded Systems*, 2013; http://csrc.nist.gov/groups/ST/hash/sha-3/documents/kelsey_ches2013_presentation.pdf.
- “Recommendation for Random Number Generation Using Deterministic Random Bit Generators,” NIST SP 800-90, Nat’l Inst. Standards and Technology, Mar. 2007 (withdrawn in Jan. 2012 and succeeded by SP 800-90A).
- S. Landau, “Polynomials in the Nation’s Service: Using Algebra to Design the Advanced Encryption Standard,” *Am. Mathematical Monthly*, Feb. 2004, pp. 89–117.
- N. Perlroth, J. Larson, and S. Shane, “NSA Able to Foil Basic Safeguards of Privacy on the Web,” *The New York Times*, 5 Sept. 2013.
- “NIST Opens Draft Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators for Review and Comment,” supplemental *ITL Bulletin*, vol. 44, Sept. 2013.
- C. Cain Miller, “Secret Court Ruling Puts Tech Companies in Data Bind,” *The New York Times*, 13 June 2013.
- D. Drummond, “Google Statement on NSA Infiltration of Links between Data Centers,” *The Washington Post*, 30 Oct. 2013.
- C. Timberg, “Google Encrypts Data Amid Backlash against NSA Spying,” *The Washington Post*, 6 Sept. 2013.
- B. Fung, “Even after NSA Revelations, Yahoo Won’t Say If It Plans to Encrypt Data Center Traffic,” *The Washington Post*, 30 Oct. 2013.
- C. Timberg, B. Gellman, and A. Soltani, “Microsoft Moves to Boost Security,” *The Washington Post*, 27 Nov. 2013.
- J. Goetz and F. Obermaier, “Edward Snowden Enthult Namen Spahender

Telekonfirmen," *Sueddeutsche.de*, 2 Aug. 2013; www.sueddeutsche.de/digital/internet-ueberwachung-snowden-enthueellt-namen-der-spaehen-den-telekomfirmen-1.1736791.

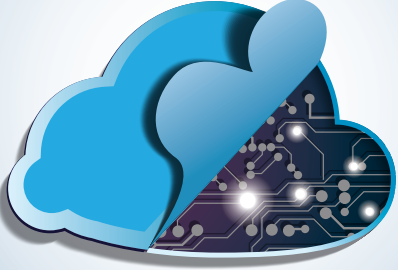
53. L. Bergman et al., "Spy Agency Data after September 11th Led FBI to Dead Ends," *The New York Times*, 17 Jan. 2006.
54. S. Shane and M. Schmidt, "FBI Did Not Tell Police in Boston of Russian Tip," *The New York Times*, 9 May 2013.
55. C.D. Leonnig, "Court's Ability to Police US Spying Program Limited," *The Washington Post*, 15 Aug. 2013.
56. K. Malkanes Hovland, "Norway Reveals It Monitored Phone Data," *Wall Street J.*, 19 Nov. 2013.
57. N. Hopkins, "UK Gathering Secret Intelligence via Covert NSA Operation," *The Guardian*, 7 June 2013.
58. J. Nye, *Soft Power: The Means to Succeed in World Politics*, Public Affairs, 2005.
59. J. Goldsmith, "We Need an Invasive NSA," *New Republic*, 10 Oct. 2013.
60. K. Hill, "Blueprints of NSA's Ridiculously Expensive Data Center in Utah Suggests It Holds Less Info than Thought," *Forbes*, 24 July 2013.

no. 1, 2014, pp. 62–64; <http://doi.ieeecomputersociety.org/10.1109/MSP.2013.161>.

Susan Landau is a senior staff privacy analyst at Google. She's also 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). Formerly a Distinguished Engineer at Sun Microsystems, Landau has been a Guggenheim Fellow and a fellow at the Radcliffe Institute for Advanced Study; she's also an ACM fellow and an AAAS fellow. Contact her at susan.landau@privacyink.org.

This Web extra accompanies the article, "Highlights from Making Sense of Snowden, Part II: What's Significant in the NSA Revelations," IEEE Security & Privacy, vol. 12,

Coming March 2014



IEEE CLOUD COMPUTING

IEEE Computer Society's newest magazine tackles the emerging technology of cloud computing. Subscribe today!

computer.org/cloudcomputing

ANYTIME, ANYWHERE ACCESS

DIGITAL MAGAZINES

Keep up on the latest tech innovations with new digital magazines from the IEEE Computer Society. At **more than 65% off regular print prices**, there has never been a better time to try one. Our industry experts will keep you informed. Digital magazines are:

- Easy to save. Easy to search.
- Email notification. Receive an alert as soon as each digital magazine is available.
- Two formats. Choose the enhanced PDF version OR the web browser-based version.
- Quick access. Download the full issue in a flash.
- Convenience. Read your digital magazine anytime, anywhere—on your laptop, iPad, or other mobile device.
- Digital archives. Subscribers can access the digital issues archive dating back to January 2007.

Interested? Go to www.computer.org/digitalmagazines to subscribe and see sample articles.

