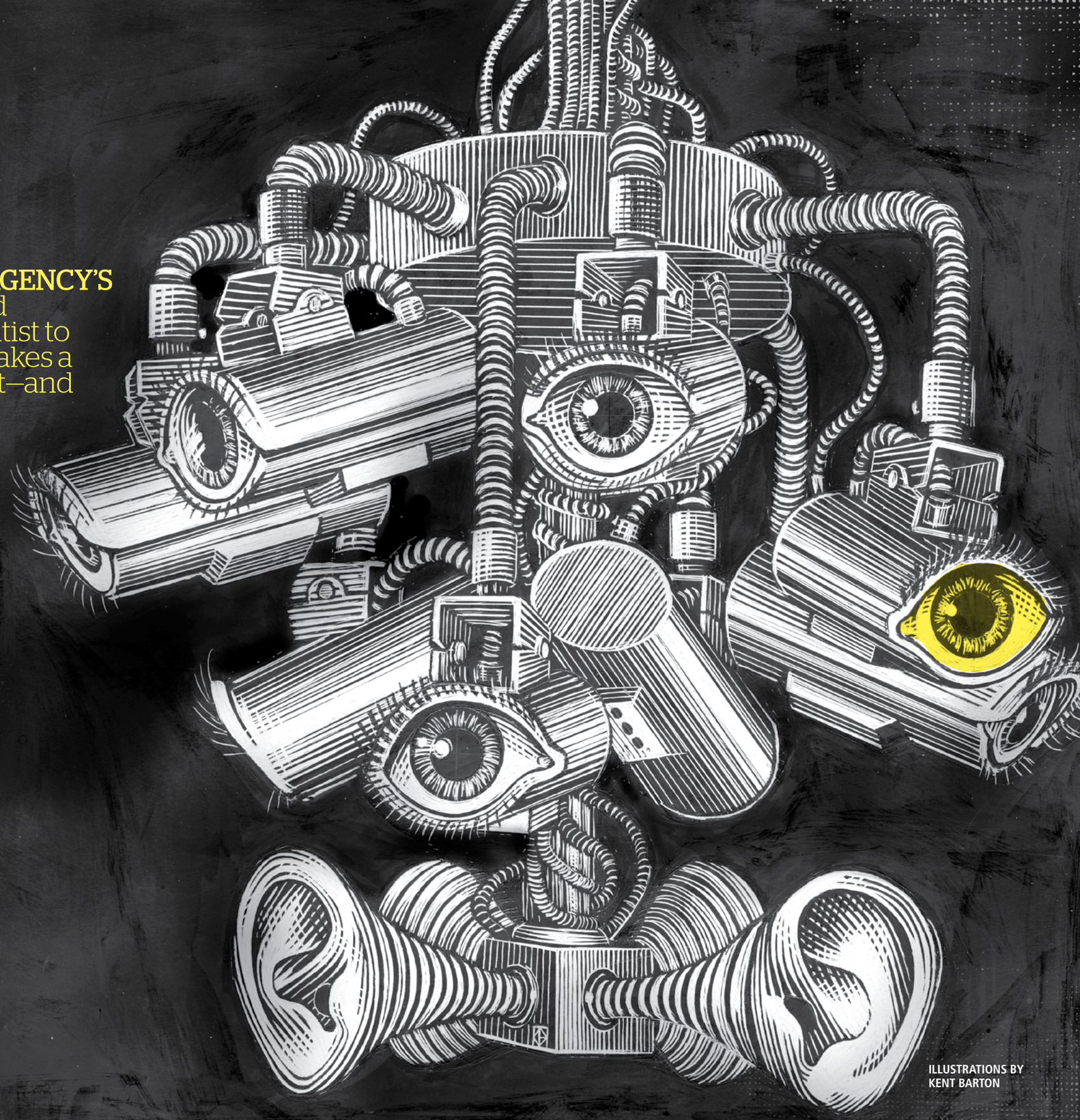
WATCHING THE WATCHERS

THE NATIONAL SECURITY AGENCY'S SURVEILLANCE isn't new and doesn't take a computer scientist to understand. **DAVID BROWN** takes a look at how the agency does it—and **WHAT NEEDS TO BE DONE.**



ILLUSTRATIONS BY KENT BARTON

ON MARCH 12, 2013, DURING AN OPEN HEARING OF THE SENATE INTELLIGENCE COMMITTEE IN WASHINGTON, D.C., Ron Wyden of Oregon asked Director of National Intelligence James R. Clapper, "Does the NSA [National Security Agency] collect any type of data at all on millions or hundreds of millions of Americans?"

"No, sir," Clapper replied. "Not wittingly."

The beauty of absolute, impenetrable secrecy, I would argue, is that Clapper could say what he pleased. And Wyden, who had reason to suspect Clapper was speaking untruthfully, could not publicly call him on it. Wyden is bound by Senate secrecy rules.

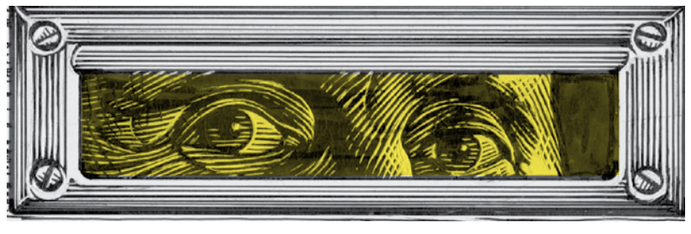
But while Clapper was testifying on Capitol Hill, what he didn't know was a whistleblower named Edward Snowden was compiling a damning portfolio of the domestic surveillance activities of the NSA. The tranche of data, later sent to *The Guardian* of London and *The Washington Post*, contained a court order directly contradicting Clapper's testimony. The Foreign Intelligence Surveillance Court, at the behest of the Federal Bureau of Investigation, ordered Verizon Business Network Services to hand over "on an ongoing, daily basis" information about every call "between the United States and abroad," and perhaps more alarmingly, "wholly within the United States, including local calls." The court issued the order under the purview of the USA PATRIOT Act, and its authorization provided for three months of persistent dragnet surveillance. The order was a renewal of a program that had been in operation for seven years. In any discussion about government surveillance and privacy rights, it is easy to get lost in the technical details of spy programs decades in the making and case law kept secret by design. The leadership of the intelligence community counts on this and uses it

as leverage against a vigorous public debate. The more bewildering a program seems to be, the more difficult it is for the public to rally against it. But the ongoing operations of the NSA are not as challenging to understand as the agency would have you believe. Equipped with some basic terminology and a broad overview of how the NSA programs interact, the public will be well prepared for one of the most pressing civil liberties discussions of our generation.

HOW DOES IT ALL WORK?

The NSA is in the signals intelligence business. "Signals" refers to any communication from any source. It might be an email or phone call, but it also might be a hacked foreign satellite, or a sophisticated bug surreptitiously placed to record conversations. When signal data is analyzed for meaning, it becomes "intelligence."

To illustrate: A target's intercepted email (signal) reveals a series of late credit card payment warnings (data). When an agent on the ground reports that the target has been feverishly participating in off-track betting, and an intercepted credit application reveals the target also is trying to buy a new sports car, the drawn conclusion (intelligence) suggests the target has a gambling problem. Generally speaking, this is what intelligence agencies do: gather information and guess.



When the NSA seeks to gather information inside the United States for foreign intelligence purposes, its activities must be authorized by a secret court established by Congress in the Foreign Intelligence Surveillance Act (FISA) of 1978. The court meets at a federal courthouse in Washington, D.C., at any given time, day or night, depending on the urgency of the request. (A FISA judge always is on call.) Generally, legal interpretations by the court are secret, and if your name has been brought before the FISA court, you will not be informed—unless the government relies on the fruits of its surveillance in prosecuting you. No opposing counsel represents the accused.

So in theory, for instance, the FBI develops a case against a suspected terrorist and presents the FISA court with an application for a wiretap. To get a warrant, the FBI needs to show it has probable cause to believe the target is a foreign power or an agent of a foreign power. The likelihood the FISA court grants surveillance request is high. Since its inception, the court has received more than 33,900 requests for warrants and denied only 11.

In practice, the secrecy surrounding the NSA's and FBI's intelligence-gathering has prevented the public from understanding what information these agencies collect and how they use that information. The NSA's mass call-tracking program, of which Verizon is a part, is concerned primarily with "metadata." Metadata consists of, at a minimum, whom you call, the date and time of your call, and the duration of your conversation. Rules for obtaining a business records order under USA PATRIOT Act Section 215, which is what the phone metadata program operates under, are less than stringent, says Kel McClanahan, executive director of the public interest law firm National Security Counselors. There is no "probable cause" standard. "The FBI agent only has to show he has a reasonable suspicion that the search will turn up something relevant to an investigation," McClanahan points out. Accordingly, the court can order Internet and telecommunications companies to turn over vast troves of records and user activity.

Because the court order to Verizon stated, "No person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things through this order," it stands to reason that every company issued such demands is similarly gagged. (Days after Glenn Greenwald of *The Guardian* broke the story, it came to light that AT&T and Sprint Nextel are also required to hand over call records, and credit card companies similarly hand over records of their customers' transactions.)

Meanwhile, the FISA Amendments Act of 2008 allows for domestic surveillance of U.S. citizens, provided one end of the correspondence (which can include emails, Skype calls and other electronic communications) is a foreigner abroad relevant to an investigation. The government also is allowed to conduct surveillance about its targets. One end of the communication still needs to be foreign, but the government can collect such communications as long as its FISA Amendments Act certifications last, which is one year with the option to renew. The upshot is if you have friends who live outside the 50 states, your emails can be monitored without a judge seeing a scrap of justification.

Based on a leaked document signed by Attorney General Eric Holder, "minimization" procedures are in place for data the NSA inadvertently collects, though loopholes are legion. Analysts are to destroy "communications of or concerning a United States person" at the "earliest practicable point" provided the data is unrelated to the investigation underway, contains no foreign intelligence information and does not contain evidence of a crime.

(Inadvertently collected attorney-client communications where the client is under active indictment are to be segregated and logged with the Department of Justice, so no such data may be used in any criminal prosecution. This directive does not apply, however, to attorney-client intercepts when prosecutions are contemplated or completed, nor does it apply to military commission prosecutions.)

There is an alarming exception to the minimization policy when it comes to encrypted data. "In the context of a cryptanalytic effort," the leaked document states, "maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis." Meaning if you don't want anyone to read your email, the NSA wants to read it that much more and can store the information forever, or until it can break the encryption.

The constitutionality of such a rule is questionable. It's as if a policeman who knocks on the wrong door and finds it to be locked could stay at the house as long as it takes to pick the lock and then may walk in and take a look around.

Another unsettling aspect of NSA surveillance is how far its tendrils are authorized to reach. Provided that the NSA has legally targeted a terrorist suspect under the rules set by the FISA Court, analysts are authorized to perform two collection "hops." This means not only can the agency collect and analyze the initial target's email, phone calls and correspondence but it also can do the same for everyone in the target's address book and everyone in those people's address books. The metadata program goes one hop further.

The Associated Press did the math on a triple-hop: "If the average person called 40 unique people, three-hop analysis would allow the government to mine the records of 2.5 million Americans when investigating one suspected terrorist." In other words the boundaries of the NSA are farther-reaching than imagined. And remember, encrypted files and messages can be stored forever.

At least one customer of Verizon Business Network Services has taken action against the government. On June 11, 2013, the ACLU filed a lawsuit before the U.S. District Court in the Southern District of New York over the "dragnet acquisition" of its telephone records. The legal complaint states, "The practice is akin to snatching every American's address book—with annotations detailing whom we spoke to, when we talked, for how long and from where. It gives the government a comprehensive record of our associations and public movements, revealing a wealth of detail about our familial, political, professional, religious and intimate associations."

The defendants listed in the ACLU's complaint include Keith Alexander, the director of the NSA; Robert Mueller, former director of the FBI; Charles Hagel, the Secretary of Defense; Eric Holder, the Attorney General; and James Clapper. The goal of the suit is to have the court find the mass call tracking unlawful and in violation of the First and Fourth Amendments, to have the program permanently shut down, and to have related databases purged of collected records.

CLASSIFIED INFORMATION

In 2005, *The New York Times* revealed a set of NSA surveillance programs that, though considered shocking at the time, have since been institutionalized. The content intercepted by the programs is code-named RAGTIME and includes foreign-to-foreign counterterrorism data, intercepted signals from foreign governments and counterproliferation data. The most salient aspect of the program is called RAGTIME-P, which concerns domestic spying. (The P stands for PATRIOT Act.) The bulk metadata provided to the NSA by Verizon presumably would fall under RAGTIME-P.

Because of the files Edward Snowden provided, we now know the most well-known ongoing operation of the NSA is called PRISM. Its purpose is classified, but Snowden's files offer a pretty good idea of how it works and what it does.

PRISM is a data mining operation designed to access foreign communications stored on U.S. servers, even when one side of the conversation terminates in the United States. Prominent members of the U.S. technology industry provide NSA analysts with access to a stealthy domain of real-time digital information, which spans many elements of the average person's Internet activity—email, chats, Facebook messages and profile information, instant messages, video, Skype and other voice-based communications, and photographs (and valuable metadata contained within). Known members of the program include Google, Microsoft and Yahoo, a trio that originate 98 percent of all PRISM "product." To be clear PRISM is neither a database nor a secret surveillance club companies may join. PRISM is the front end of a sophisticated array of databases, protocols, agreements and legal coercions.

How are those databases filled and where are those agreements forged? Based on the recent revelations, the FISA Court authorized the broad framework of PRISM. To collect data, the FBI Data Intercept Technology Unit installs "government equipment on private company property to retrieve matching information from a participating company," according to a *Washington Post* analysis of one leaked document. These companies receive a list of material needing to be collected, and that material is mirrored onto the government systems and passed to the NSA.

Six Things That Must Change Today

SINCE THE SNOWDEN REVELATIONS, there has been a surge of interest in reforming the legal framework of the surveillance state. The ACLU's lawsuit has attracted support from everyone from the National Rifle Association to Rep. Jim Sensenbrenner, the author of the USA PATRIOT Act. In the meantime, if the rights of Americans are to be preserved, here are six things that must change today.

1. The Foreign Intelligence Surveillance Court must be reformed. Advocates must be allowed to challenge the government's assertions before the approval of broad surveillance programs. This is particularly necessary when the programs are not obviously authorized by law or rely upon novel interpretations of law. These challenges should be public so Americans understand what the court interprets the surveillance laws to allow.

2. The U.S. government should be required to inform Americans who have had their data intercepted and provide redress.

3. Section 702 of the Foreign Intelligence Surveillance Act needs to be rewritten. As Senator Ron Wyden stated, loopholes allow spy agencies to "conduct warrantless searches for the phone calls or emails of law-abiding Americans." And as Bush administration officials admitted in pushing for passage of the law, it was designed specifically to allow the government to acquire Americans' international communications.

4. Section 215 of the USA PATRIOT Act should be modified to prohibit bulk collection. Indiscriminate or dragnet surveillance is unlawful and unnecessary and should be ended.

5. Independent security specialists should audit the surveillance procedures of NSA analysts and administrators. The NSA has admitted that by simply ignoring protocol, analysts can spy on innocent Americans abroad. More shocking, these constitutional breaches are known largely because of self-reporting; the agency wouldn't have known about them if not for personal confessions.

6. Congress should investigate agency heads and officials who gave false or misleading testimony in support of these surveillance programs. The same people who presided over the most egregious breaches of privacy in American history have been placed in charge of fixing things. The problems with this logic are self-evident. Rather than trust them to fix the problem, Congress should investigate those who gave false or misleading testimony in defense of these surveillance programs.

Stand with us! Take action on this and other critical civil liberties issues at **aclu.org/action**.

Strictly speaking, PRISM targets must be foreigners abroad, and a warrant is not necessary—and not just in cases where catastrophe is imminent. This is problematic, to put it mildly, as surveillance targeted at foreign persons inevitably sweeps in domestic communications. Not talking to a terrorist and thus unconcerned? You should be concerned. The foreign half of the surveillance under the FISA Amendments Act need not be the actual person of interest to U.S. authorities.

Neither PRISM nor the NSA is the only game in town. Internet surveillance is a global operation, and thanks to significant partnerships, U.S. allies also contribute to the data bank. The United States, United Kingdom, Canada, Australia and New Zealand—known collectively as the "five eyes"—signed the 1946 UK-USA agreement to share intelligence. The GCHQ, the British equivalent of the NSA, has partnered with British telecommunications companies to plant interception devices on transatlantic fiber-optic cables. Like the U.S. members of PRISM, the companies are legally compelled to participate and gagged from revealing their participation. Data acquired from the British operation is shared with the NSA. The United States has paid GCHQ at least $150 million to help mitigate the costs of tapping the data conduits.

The NSA has denied using signals intelligence partnerships with foreign governments as a way to bypass FISA and spy on American citizens, though the Snowden documents have revealed that the United States provides raw data to Israel regarding American citizens.

Israel isn't the only unexpected beneficiary of NSA data. To help build criminal cases against Americans, the U.S. Drug Enforcement Administration (DEA) mines billions of telephone records from AT&T and also receives tips derived from NSA surveillance and wiretapping. To cover these tracks, DEA agents are trained to "reverse engineer" their cases, creating a false investigative trail that conceals the use of surreptitious surveillance tactics.

According to ACLU Deputy Legal Director Jameel Jaffer, "When law enforcement agents and prosecutors conceal the role of intelligence surveillance in criminal investigations, they violate the constitutional rights of the accused and insulate controversial intelligence programs from judicial review."

The NSA builds many tools to help automate the refinement of raw signals data. Of the NSA systems revealed so far, one of the most powerful is called XKEYSCORE. Its job is to sort the collected data, apply tags and pipe the improved information to various databases. Analysts may then use XKEYSCORE to enter meaningful selector search queries of collected data, similar to the way Google works.

Storing and processing the entirety of the world's communications takes substantial computing power. In 2010, *The Washington Post* reported that the NSA intercepts and stores 1.7 billion phone calls and electronic messages every day. In addition to its massive headquarters at Fort Meade, Maryland, the agency has constructed several facilities around the world to accommodate the inconceivable amount of information being collected. Signals intelligence from the Middle East is processed at a new $1 billion facility at Fort Gordon, Georgia. Asian intelligence is analyzed at a newly expanded facility in Hawaii. (Edward Snowden is the facility's most famous alumnus.) Major sites also exist in Texas and Colorado, and a new million-square-foot data center in Utah has reached a kind of "Area 51" status in the eyes of civil libertarians.

THE WATCHDOG NEEDS A WATCHDOG

Contrary to the testimony of National Intelligence Director James Clapper, not only was the NSA collecting data on hundreds of millions of Americans, it was doing so "wittingly." (Can someone "unwittingly" stumble into the Foreign Intelligence Surveillance Court and walk away with permission to siphon data concerning hundreds of millions of Americans?) As the ACLU has long argued, whether Clapper spoke untruthfully or dissembled tradecraft vernacular with subatomic precision, the whole affair punctures any argument that Congress can effectively oversee the national security state.

To wit, on July 24, 2013, the House of Representatives voted down an amendment from Rep. Justin Amash of Michigan that would have ended the NSA's bulk collection of phone records. Before the roll call Rep. Amash said, "Opponents of this amendment will use the same tactic that every government throughout history has used to justify its violation of rights: fear." His prediction was validated when Rep. Mike Rogers of Michigan declared that passing the amendment "takes us back to September 10." Rep. Michele Bachmann of Minnesota said only "those who are engaged in Islamic jihad" have benefited from recent revelations of the mass surveillance of American citizens. Leadership in the House, as well as the White House, lobbied relentlessly against the bill, and it failed 217-205.

> "I, SITTING AT MY DESK, CERTAINLY **HAD THE AUTHORITIES TO WIRETAP ANYONE,** FROM YOU, OR YOUR ACCOUNTANT, TO A FEDERAL JUDGE, TO **EVEN THE PRESIDENT** IF I HAD A PERSONAL EMAIL."
> —*Edward Snowden*

Until Congress adequately reins in and oversees the activities of the NSA, it falls to watchdog groups, whistleblowers and organizations such as the ACLU to take up the cause. At the very least, though, Congress should press for NSA reforms with regard to internal oversight.

When I suggested this to Tim Shorrock, author of *Spies for Hire: The Secret World of Intelligence Outsourcing* (Simon & Schuster, 2008), he noted that meaningful reform is difficult because of the agency's overreliance on defense contractors. "The central institutional failure of the NSA was not keeping the capabilities to analyze signals intelligence in-house," Shorrock says. "Likewise Congress failed to provide proper leadership of and oversight over NSA's procurement process when this analysis was outsourced."

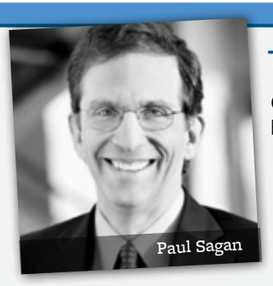
Shorrock points out that not only the technology but also the entire process of signals intelligence was privatized. The cozy multibillion-dollar relationship between the intelligence community and defense contractors has created an obfuscation factory that is nearly impenetrable to outsiders tasked with providing oversight and wholly resistant to reform.

Meanwhile outside security specialists should closely audit the agency and its industry cohorts. In an interview with Glenn Greenwald, Edward Snowden said, "I, sitting at my desk, certainly had the authorities to wiretap anyone, from you, or your accountant, to a federal judge, to even the president if I had a personal email." If this is true—and NSA whistleblower William Binney confirmed it in an interview with *USA Today*, and the ACLU has long made that argument—whatever the effectiveness of the legal framework driving NSA activities, the system depends on the trustworthiness of the analyst or administrator.

This can be said for every such career. Soldiers can commit war crimes if they choose, and police officers can use lethal force in lieu of writing a speeding ticket. They rightfully suffer terrible consequences, but the damage remains. The NSA's tools and programs are extraordinarily powerful. That without raising red flags an analyst can plug in anyone's email address and begin reading their messages calls into question the agency's internal security procedures. The NSA is placing a tremendous amount of trust in polygraph examinations and security clearance questionnaires if those are the final arbiters of an employee's reliability.

The documents Edward Snowden and other whistleblowers provided led Robert S. Litt, general counsel for the Office of the Director of National Intelligence, to declare in a speech on July 19, 2013, "These disclosures threaten to cause long-lasting and irreversible harm to our ability to identify and respond to the many threats facing our nation." But the now-revealed actions of the intelligence community also cause great harm to our national identity and lead me to ask a more troubling question: If a low-ranking contractor could find out about the once unimaginable dragnet surveillance of hundreds of millions of American citizens, what other secrets are the powerful figures at the National Security Agency hiding? That this question needs to be asked suggests the American public is overdue for an answer.

In June a spokesperson for the NSA told *The Guardian*, "The continued publication of these allegations about highly classified issues—and other information taken out of context—makes it impossible to conduct a reasonable discussion on the merits of these programs." But if not for the continued publication of the "allegations," we'd have no acknowledgement, let alone discussion, of these programs at all. ■


Paul Sagan

Tapping Technology

CIVIL ACTIVISM has been the norm for Paul Sagan since the '70s. "I was a journalist at the time, and it all started with protecting free speech," he says. "I was living near Chicago and a neo-Nazi group wanted to march in Skokie, a nearby suburb with a large Jewish population. As disgusting as their message was, the ACLU was the group willing to defend their First Amendment right to free speech. They have been one of the most steadfast defenders of civil rights—even with unpopular issues."

He became a member of the ACLU around the same time, and when his career path subsequently shifted from journalism to Internet technology, Sagan found himself in another industry particularly connected to the ACLU's work. "The government has gathered massive amounts of data on all of us for often unclear reasons," Sagan says. "The ACLU has taken on the challenge of making sure there is a watchdog and Constitutional limits."

As a resident of the Boston area, Sagan's local ACLU affiliate is naturally interested in privacy issues. "The Boston area is known for tech innovation and the ACLU of Massachusetts is trying to help make sure technology is used appropriately to provide greater security for all of us, not less," he says. "But the ACLU is using the courts to protect us from unreasonable encroachments on our liberties by the government. It's a constant battle, but one worth supporting."