Decoding the Summer of Snowden

BY JULIAN SANCHEZ

Nearly 40 years ago, in the aftermath of the Watergate scandal, Americans got an unprecedented look behind the cloak of secrecy shielding government surveillance—and what they saw was chilling. A Senate committee headed by Sen. Frank Church uncovered a train of abuses by intelligence agencies stretching back decades, under presidents of both parties. Employing illegal break-ins, mail-opening programs, concealed bugs, bulk interception of telegrams, and telephone wiretaps, these agencies had gathered information about domestic political dissidents, journalists, labor leaders, and even members of Congress and Supreme Court justices. Perhaps most notoriously, the Church Committee revealed that J. Edgar Hoover had conducted a 10-year campaign to destroy and discredit Martin Luther King Jr., seeking to blackmail him into retirement or suicide with illegal recordings of the civil rights leader’s extramarital liaisons.

This summer, Americans got the most comprehensive look at the government’s massive surveillance machinery since the Church Committee, by way of leaked documents provided to the press by former National Security Agency (NSA) contractor Edward Snowden—as well as the government’s own grudging disclosures. As the “Summer of Snowden” stretches into autumn, Americans trying to make sense of the continuing deluge of new revelations may feel as inundated as the analysts who complain that trying to sort through the vast quantities of data flowing through that machine is like “drinking from a firehose.” Fortunately, you don’t need the NSA’s supercomputers to keep track of all the government spying. Here are the most significant programs we’ve learned about to date. Together, they reveal a surveillance machine vastly more powerful than anything Hoover could have dreamed of.

THE NSA CALL RECORDS PROGRAM

You don’t have to be a spy or terrorist to make it into the NSA’s vast databases—all it takes is placing a phone call. News reports from as early as 2006 had claimed the spy agency was indiscriminately vacuuming up

Continued on page 6
call records—but the government only acknowledged it after The Guardian published a court order leaked by Snowden demanding all of Verizon’s domestic and international phone logs. Similar orders—relying on the Patriot Act’s “business records” provision, known as Section 215—are regularly served on all major carriers, which means the government gets a record of the time, date, and duration of nearly every call an American makes, which it stores for at least five years.

Officials were quick to assure the public that the bulk collection is limited to “metadata”—information about phone calls, rather than their actual contents. But metadata can be incredibly sensitive too—revealing who has phoned a divorce lawyer, a suicide hotline, a rape crisis center, a medical specialist, an unpopular political group... or a reporter who exposes government misconduct. More sophisticated pattern analysis—mapping changes in the time, frequency, and sequence of communications—can even reveal intimate facts about people’s habits, associations, relationships, and even mental state. Cell phone records can also be used to track the owner’s location, providing a virtual map of all their movements. Officials say they don’t “currently” collect that information “under this program,” but we’ve learned that a bulk location-tracking program of some kind was piloted by NSA in 2010–2011, and the scope of location tracking under other programs remains unknown.

Access to this vast database is supposed to be strictly limited: Under rules imposed by the secret Foreign Intelligence Surveillance Court (FISC), NSA analysts are only supposed to run searches for numbers linked by “reasonable suspicion” to a foreign terror group. But those searches can pull up records of people up to three “hops” from a suspicious number. If you’ve ever called anybody who has called anybody who has called anybody who has called a suspect, your phone logs can be copied into a second database for analysis unencumbered by all those pesky restrictions.

We’ve also learned that the rules were routinely flouted: For the first three years of the call records program’s current incarnation, the FISC was misinformed about how it really worked. As a result, software tools routinely accessed the data without the required approvals: Of the 17,835 phone numbers searched by one automated alert list from 2006 to 2009, only 1,935 had been vetted for “reasonable suspicion.” Query results were also improperly shared with the CIA and FBI. Over several months in late 2008 and early 2009, the agency swore to the court that all the problems had been remedied—only to uncover a fresh batch of violations.

NSA director Keith Alexander told the FISC that the lapses were inadvertent and occurred because “there was no single person who had a complete technical understanding of the system architecture.” In a scathing response, the chief judge of the FISC concluded that the court’s “minimization procedures... have been so frequently and systematically violated that it can fairly be said that this critical element of the overall regime has never functioned effectively.”

In fact, the initial design of the system appears to have been so lax—with so few technical controls in place to ensure that the data was only used in accordance with the rules—that it seems clear little effort had been put into making that regime function effectively. We are again assured that all problems have been fixed, but the “oversight” regime fundamentally relies on the NSA to police its own activities and notify the court—eventually—when they detect something amiss.

So what’s the security payoff from collecting such a massive archive of Americans’ sensitive data? Initially, intelligence officials tried to lump together the call records program with another recently disclosed tool known as PRISM, claiming they had together helped disrupt over 50 “terrorist events”—which was widely reported as a tally of foiled plots. Yet under pressure from skeptical legislators, they admitted that the call records database was used in only 13 of those cases, several of which involved tracking finances, not disrupting plots. Ultimately, NSA acknowledged that in only one or two of those cases did the database help identify suspects who might not have been uncovered by more traditional, targeted requests for records.

Coming on the heels of controversy over government sifting through Associated Press phone records to identify leakers, this database has obvious potential to deter anyone who would risk speaking to press about government misconduct. The current rules supposedly prevent the use of the database for leak investigations—but the rules can always be changed in secret, or ignored. Even presidents and congressmen feared J. Edgar Hoover, because you could never be sure what he might have on you. Today, we know the NSA has something on all of us.

REDEFINING “RELEVANCE”

Almost as disturbing as the construction of a vast domestic call database of dubious security value was the legal theory NSA invoked to do it. Section 215 of the USA Patriot Act allows the government to obtain any “tangible thing” that is “relevant to an authorized investigation” under a secret court order—whose recipients are gagged from revealing even the existence of the demand for records. That’s a very low standard even as traditionally understood—one that would allow the government to secretly vacuum up sensitive data about people only tenuously connected to a suspect.

Even so, Patriot Act co-author Rep. James Sensenbrenner (R-Wisc.) has insisted that the “relevance” language was meant to ensure that records obtained would have some link to specific intelligence targets. Instead, the government secretly persuaded the FISC that an entire database containing millions of people’s records, the vast majority of whom were entirely innocent, could be “relevant” to an
The court’s acceptance of this idea—and the shaky legal reasoning used to justify it—should be especially disturbing given how many government surveillance authorities depend on the “relevance” standard. It’s the same criterion used to obtain records using National Security Letters, which are issued by FBI agents without judicial approval, as well as a wide array of ordinary criminal investigative tools.

Moreover, the secret reinterpretation of “relevance” raises fundamental questions about the democratic legitimacy of effectively secret law. Briefing materials outlining the call logs program were “made available” to members of Congress who wanted to make the effort to learn about it, but it’s clear that many had no idea what they were really voting for when they renewed §215 powers in 2011. Those who did know, of course, had no reason to fear public backlash over their votes: When the true meaning of legislation is determined by secret interpretations, the people have no meaningful ability to weigh in on whether it strikes the right balance. If our political system rests on the consent of the governed, don’t the governed at least need to know what they’re supposedly consenting to?

THE FISA AMENDMENTS ACT: PRISM AND UPSTREAM

The FISA Amendments Act of 2008 was sold to the public as a minor legal “fix” to ensure that the government could pick up communications between foreigners passing through the United States, some of which might have been held to require a warrant to intercept under the original Foreign Intelligence Surveillance Act of 1979. Defending the FAA’s reauthorization late last year, Rep. Trey Gowdy (R-SC) thundered that the law “has nothing to do with Americans on American soil,” and therefore “doesn’t implicate the Bill of Rights,” because it can only be used to “target” foreigners outside the United States.

Leaked NSA documents and declassified FISC opinions, however, have made clear that the FAA has profound implications for the privacy of Americans. As I pointed out repeatedly over a year ago—though few legislators noticed—the “target” of intelligence surveillance doesn’t have to be a participant in an intercepted conversation: The government can also eavesdrop on communications that may contain information about a suspect. On that theory, NSA has been electronically sifting through vast quantities of international emails from Americans, looking for references to identifiers on their target lists.

That’s one aspect of what the NSA calls “Upstream” collection, the live filtering of huge volumes of traffic flowing over the Internet’s backbone using powerful supercomputers. Unsurprisingly, this automated search for needles in the digital haystack sometimes led to large scale “overcollection” of entirely domestic communications—with the first systemic problem reported as early as 2009.

The specter of “overcollection” again raised its head in 2011, when the FISC discovered that it had been misinformed once more, this time for “only” a few months, about the technical details of NSA’s surveillance. Here, the problem was that if a single e-mail triggered the NSA’s automatic filters while a user was downloading his inbox, the entire stream—including totally domestic messages—could be captured. As the FISC observed, even if this were a relatively rare occurrence, the massive scale of NSA interception meant the agency could be rounding up some 56,000 wholly domestic emails annually. This approach, the court drily concluded, was “deficient on statutory and constitutional grounds.”

NSA doesn’t only listen in on the Internet backbone, however. It has also built close partnerships with major Internet companies—including Apple, Google, Microsoft, Facebook, and Yahoo—to aid in its monitoring of both “live” and stored communications via a program known as PRISM. Much remains unknown about how PRISM surveillance operates: Most of the participating companies have fervently denied giving NSA “direct access” to their servers. However, in the case of at least one platform—Microsoft’s Skype software for video chatting—the government appears to have compelled the company to make design changes that rendered a supposedly secure and encrypted service more susceptible to wiretapping.

The rules governing both types of surveillance, in theory designed to “minimize” the collection and retention of Americans’ communications, appear to have plenty of loopholes. Though the “hard selectors”—identifiers such as phone numbers or email addresses—programmed into NSA’s data vacuums are supposed to be associated with foreign targets, the agency only needs to be 51 percent confident that a particular selector is actually foreign, and when there’s no evidence either way, selectors are presumed foreign by default. Under a program called XKEYSCORE, NSA can also use “soft selectors”—general communications characteristics like language or software protocol—to zero in on a target whose address is unknown.

Once communications are seized, even if they’re domestic, they can be retained for further analysis if encrypted, or if they contain evidence of a crime unrelated to terrorism. Perhaps most disturbingly, analysts can search through NSA’s huge trove of intercepted communications for “selectors” associated with particular Americans. Initially, the rules prohibited such “backdoor searches,” but government lawyers were able to get that restriction lifted in 2011.

The blanket surveillance orders issued under the FAA resemble nothing so much as a modern version of the “general warrants”—or “writs of assistance”—that outraged the American colonists and inspired the Fourth Amendment. They may “target” information about foreigners, but they give the NSA—not neutral judges—the discretion to determine which particular “places” and digital “papers” will be searched or seized.
Gripped by the fear of terrorism, Americans have allowed the resurrection of the very practice that once sparked a revolution.

**BULLRUN: UNDERMINING ENCRYPTION AND INTERNET SECURITY**

Since its inception, breaking enemy codes and ciphers has been one of the primary missions of the NSA. In recent years, however, the agency has taken that a step further: Now it seeks to ensure that the encryption software relied on by millions of ordinary Internet users—from businesspeople engaged in sensitive professional communications to dissidents in repressive regimes—comes out of the box pre-broken.

The idea that the government should have backdoor access to encrypted communications was proposed and hotly debated in the late 1990s—and, wisely, defeated thanks to strong opposition from both privacy advocates and security experts. Having lost the public debate, NSA pressured software developers to include those backdoors secretly.

Under a program known as BULLRUN, the agency has sought, in its own words, to “insert vulnerabilities into commercial encryption systems, IT systems, networks and endpoint communications devices used by targets,” and to “covertly influence” the design of commercial software—potentially infiltrating companies when necessary—in order to “make it more tractable to advanced cryptanalytic capabilities being developed by NSA.”

Perhaps most disturbing of all, the NSA has leveraged its role as the government’s primary source of cybersecurity expertise to influence—and weaken—the public standards and specifications adopted by national and international standard-setting bodies, introducing subtle vulnerabilities. That weakens trust in those institutions, and makes the already formidable task of securing the Internet against attacks—a task that depends crucially on strong encryption—even more difficult.

“The NSA’s actions are making us all less safe,” as security and encryption expert Bruce Schneier has explained. “They’re not just spying on the bad guys, they’re deliberately weakening Internet security for everyone—including the good guys. It’s sheer folly to believe that only the NSA can exploit the vulnerabilities they create.”

**THE UNKNOWN UNKNOWNS**

In light of the government’s demonstrated willingness to expand its surveillance powers through secret court rulings and tortured legal reasoning, there’s little way of knowing what limits on NSA surveillance truly remain.

We know from FBI and NSA to state and local narcotics cops, who are then instructed to dummy up their own investigations to conceal the true source of their leads. During the debates over ratification of our Constitution, James Madison warned that “there are more instances of the abridgment of the freedom of the people by gradual and silent encroachments of those in power than by violent and sudden usurpations.”

We now know that the government has indeed been silently and gradually encroaching on the privacy of its citizens, on a scale Madison could not possibly have imagined. We don’t yet have evidence that the surveillance machine our government has constructed has been abused for political purposes in the way its far more primitive predecessor was in the 1960 and ‘70s—no surprise, since those abuses were typically only discovered years later. But if we remain complacent out of the fear of terrorism, should that day ever come, we are likely to realize only too late that there is no longer anywhere left to hide.