Guest Post: US Intelligence Reforms Still Allow Plenty of Suspicionless Spying on Americans

By *Margo Schlanger*
Friday, February 13, 2015 at 1:07 PM

Last week, the Obama Administration released a report and documents cataloging progress toward signals intelligence (SIGINT) reform goals set a year ago by the President in a document known as PPD-28. PPD-28 promises foreigners some of the same privacy protections given to US citizens and residents. But it turns out that those protections, even for citizens, are fairly meager, in ways that have not yet fully entered the public conversation about surveillance. US citizens and residents have been — and remain — exposed to suspicionless electronic surveillance. Implementation of PPD-28 will do little to change that.

To my mind, the surveillance I'm about to describe, which proceeds under Executive Order 12333, rather than FISA, is far more worrisome than the programs under Section 215 of the Patriot Act and Section 702 of the FISA Amendments Act that have received so much recent attention. (For example, here and here for Section 215, here and here for Section 702, and here and here for more general info.) This is content surveillance that applies to both wholly and partially domestic communications of US citizens and residents. The access and analysis rules are very, very loose. There is no judicial supervision of any kind, and Congress does almost no 12333 oversight. (See here for more on how FISA and 12333 differ).

Let's start with what we know, and then dive into how we know it.

What do we know?

- Non-selective "vacuum cleaner" SIGINT collection — mass collection of communications unlimited by particular communicants or subjects — is outside FISA's ambit, so long as the collection is either done abroad (for wire communications like those carried on landlines or cables) or involves at least one foreign communicant (for wireless communications). This kind of collection can and does include wholly and partially domestic communications of US citizens and residents.
- Once collected, analysis of these communications is also outside FISA's ambit. Instead, the use of SIGINT that was collected vacuum-cleaner-style is limited by PPD-28 to six topics: detecting and countering espionage, terrorism, weapons of mass destruction, cybersecurity threats, threats to the armed services, and transnational crime.
- This kind of entirely unlimited SIGINT collection is not favored, however: According to its new policies implementing PPD-28, when "practicable," the NSA searches for communications containing specific terms that narrow its collection to topics like "nuclear proliferation, oil sales, [and] economics." Economics!
- Again, so long as the collection is either done abroad (for wire communications) or involves at least one foreign communicant (for wireless communications), FISA does not regulate term searching based on subject matter, rather than the identity of a communicant. And because this approach uses a "discriminant," it is not deemed

"bulk" collection for purposes of PPD-28. It may thereafter be searched by the NSA for any and all foreign intelligence purposes, not just the six topics identified above.

- When the NSA uses subject matter searching — whether to acquire data or to search raw SIGINT acquired in bulk or otherwise — there is a mild tailoring requirement. Specifically, policy requires use of only selection terms that are reasonably likely to flag communications that include foreign intelligence topics (like oil sales). Policy also requires the NSA to try to develop selection techniques that "defeat, to the greatest extent practicable under the circumstances" interception of non-foreign intelligence communications. While we don't know what "practicable" means in this context, term searching is very familiar; just think of using Google or Westlaw. It seems inevitable that this approach exposes an extraordinary amount of innocent Americans' communications to the eyes of intelligence analysts.

So, when the President says that foreigners will get the same protections against surveillance as US citizens and residents, keep in mind that those protections leave a lot out.

How do we know it?

FISA has a complicated, four-part definition of "electronic surveillance," and in 2008, placed on top of that definition rules governing the Section 702, 703, and 704 programs, which address various kinds of targeted surveillance. Notably, "targeting," in the FISA context, means only the selection of objects of surveillance based on the *identity* of one or more communicant. So once you work through the statutory language, FISA does not at all regulate: (a) *non-targeted* collection of wire communications, including communications between Americans within the US, as long as the actual wire being tapped is located overseas, or (b) *non-targeted* collection of wireless communications if at least one party to the communication is located abroad. Thus, if its other constraints (wire or radio, domestic or overseas collection, etc.) are followed, FISA doesn't address strategies that select what to collect based not on the identities of communication participants, but using other techniques — say, the words used in the communication, or whether the messages are enciphered. And, again, if the other constraints are followed, FISA also does not address collect-everything "vacuum cleaner" content surveillance. In either situation, there is no "target" in FISA parlance.

The point is, so far as U.S. surveillance law is concerned, the NSA can, if it chooses, "collect [nearly] everything" — including your domestic phone calls and emails — so long as it does not select which communications to collect using the identity of a "particular, known" communicant. To be precise, it can collect communications where at least one party is abroad if it can find a non-wired way in. And it can collect even *entirely* domestic communications if it can find a wire to tap abroad — like the Transatlantic cable — that is carrying those conversations. Some have pointed out that methods exist to push domestic Internet traffic abroad to take advantage of these FISA omissions.

Such constraints as exist on this kind of collection — and concomitant retention, analysis, use, and dissemination — are based not on FISA, but on non-statutory sources implementing Executive Order 12333 and, since last year, PPD-28. The 12333 implementing procedures — Department of Defense Directive 5240.1-R and US Signals Intelligence Directive 18 (USSID 18) — make it clear that the NSA does indeed purposefully collect the content of US communications without FISA regulation.

The pertinent language in USSID 18 that governs the "processing" of bulk databases is fairly extensive:

Selection Terms 5.1. Use of Selection Terms During Processing. When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMUNICANT or the fact that the communication mentions a particular individual, the following rules apply:
a. No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a US. PERSON wherever located may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. Annual Review by the Signals Intelligence Director:

a. All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the Signals Intelligence Director or a designee.

b. The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. A copy of the results of the review will be provided to the Inspector General (IG) and the GC.

What do we learn from USSID-18? The language, like so much language in IC policy documents, is somewhat opaque. But at the very least, we learn that the NSA uses selection terms to decide what communications to acquire, and those communications can be to or from US citizens or residents. We also learn that selection terms that tag a "significant number" of US communications are required to be a little bit tailored: there should be "reason to believe" they will obtain foreign intelligence; and, to the extent practicable, they should be designed to *not* obtain communications that are of no foreign intelligence interest.

What is covered by "foreign intelligence?" In case there was any doubt about how broad that authority is, we learn a bit more from training slides the NSA released over a year ago, which refer (on slide 48) to "collecting based upon SUBJECT MATTER (e.g. nuclear proliferation, oil sales, economics)."

As might be expected, both vacuum-cleaner and term-searching techniques pull in massive amounts of raw data. The same training slides (on slide 69) explain: "[R]aw SIGINT databases contain completely innocent U.S. person communications and non-foreign intelligence information as well as FI [foreign intelligence]." As a result, NSA personnel are not free to trawl those databases willy nilly. Rather, "to protect the privacy rights of US citizens, the Justice Department has determined search of these databases are a collection/targeting activity." (Slide 70.) This means searches of already-collected raw data are required to follow the USSID-18 tailoring rules. It bears reemphasizing that those tailoring rules are pretty loose. They require merely that searches of already-collected raw SIGINT be reasonably likely to retrieve foreign intelligence, and that such searches be designed to the extent practicable not to retrieve other communications.

PPD-28 adds the smallest bit of extra protection. It limits what it describes as "bulk" collection to six specified purposes (detecting and countering espionage, terrorism, weapons of mass destruction, cybersecurity threats, threats to the armed services, and transnational crime). These are considerably narrower than "foreign intelligence.

But the narrower purpose rules of PPD-28 don't cover collection that uses term searching, no matter how wide-open these terms are, or how much data is acquired under them. Quite the contrary; such collection is excluded by definition. PPD-28 states: "References to signals intelligence collected in 'bulk' mean the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired*without the use of discriminants* (e.g., specific identifiers, selection terms, etc.)." (Emphasis added).

Moreover, the Directive specifically states that its limits on "bulk" collection "do not apply to signals intelligence data that is temporarily acquired to facilitate targeted collection." This carve-out is revealing: there would be no reason for it unless the NSA does, in fact, "temporarily acquire" data and then subject it to various searches that facilitate "targeted" collection for purposes not authorized for bulk collection. (Note that PPD-28 does not define "targeted;" I infer that "targeted" here covers use of topical selection terms as well as communicant targeting, but I may be incorrect in this inference.)

And finally, the NSA procedures released last week, which now govern SIGINT procedures for non-US persons, constrain the agency the tiniest bit more, stating a preference for collecting data on specific subjects instead of collecting everything:

> Whenever practicable, collection will occur through the use of one or more SELECTION TERMS in order to focus the collection on specific foreign intelligence targets (e.g., a specific, known international terrorist or terrorist group) or specific foreign intelligence topics (e.g., the proliferation of weapons of mass destruction by a foreign power or its agents).

Note, though, that notwithstanding the parenthetical examples, subject matter searching can be for any foreign intelligence topic (oil sales, economics, etc.), not just counterterrorism or counterproliferation.

So, all of this together adds up to the list I started off with, and to extraordinarily broad access by the NSA to your domestic communications. Lots of unanswered questions remain: what about FBI and CIA? How much unfiltered content communication data does the IC

actually collect? How much does it retain? And so on. We'd need much more transparency to answer those questions and dozens more that deserve answers.

Tags: Congressional Oversight, FISA, FISC, Foreign Surveillance, Fourth Amendment,Guest Post, Metadata, NSA Reform, Privacy, Section 215, Section 702, Surveillance

---

ABOUT THE AUTHOR

Margo Schlanger Margo Schlanger is the Henry M. Butzel Professor of Law at the University of Michigan, where she also heads the Civil Rights Litigation Clearinghouse. She served as the Officer for Civil Rights and Civil Liberties at the Department of Homeland Security in 2010 and 2011. Follow her on Twitter (@mjschlanger).