How the NSA's Surveillance Procedures Threaten Americans' Privacy

Newly released documents confirm what critics have long suspected—that the National Security Agency, a component of the Defense Department, is engaged in unconstitutional surveillance of Americans' communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans' international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans' privacy are weak and riddled with exceptions.

The FISA Amendment Act, signed into law by President Bush in 2008, expanded the government's authority to monitor Americans' electronic communications. Critics of the law feared the NSA would use the law to conduct broad surveillance of Americans' international communications and, in the process, capture an unknown quantity of purely domestic communications. Government officials contended that the law authorized surveillance of foreign nationals outside the United States—not of Americans—and that it included robust safeguards to protect Americans' privacy. Last year, in a successful effort to derail a constitutional challenge to the law, the Obama administration made these same claims to the U.S. Supreme Court.

Now *The Guardian* has published two previously secret documents that show how the FISA Amendments Act is being implemented. One document sets out the government's "targeting procedures"—the procedures it uses to determine whether it has the authority to acquire communications in the first place. The other sets out the government's "minimization procedures"—the procedures that govern the retention, analysis, and dissemination of the communications it acquires. Both documents—the "Procedures"—have apparently been endorsed by the Foreign Intelligence Surveillance Court, which oversees government surveillance in some national security cases.

The Procedures are complex, but at least some of their flaws are clear.

1. **The Procedures permit the NSA to monitor Americans' international communications in the course of surveillance targeted at foreigners abroad.**

The NSA "is not listening to Americans' phone calls or monitoring their emails," the Chairman of the House Intelligence Committee recently said, and many other government officials, including the president himself, have made similar assurances. But these statements are not true. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans' communications with those foreign targets. Indeed, in advocating for the Act, government officials made clear that these "one-end-domestic" communications were the ones of most interest to them. The Procedures contemplate not only that the NSA will acquire Americans' international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans' communications that contain "foreign intelligence information" or evidence of a crime can be retained forever, and even communications that don't can be retained for as long as five years. Despite government officials' claims to the contrary, the NSA is building a growing database of Americans' international telephone calls and emails.

2. **The Procedures allow the surveillance of Americans by failing to ensure that the NSA's surveillance targets are in fact foreigners outside the United States.**

The Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the U.S. government sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts the government's premise, the Procedures fail to ensure that the NSA's surveillance targets are *in fact* foreigners outside the United States. This is because the Procedures permit the NSA to *presume* that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

3. **The Procedures permit the government to conduct surveillance that has no real connection to the government's foreign intelligence interests.**

One of the fundamental problems with the Act is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who aren't even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the Act allows the government to conduct surveillance only if one of its purposes is to gather "foreign intelligence information." That term, though, is defined very broadly to include not only information about terrorism but

also information about intelligence activities, the national defense, and even "the foreign affairs of the United States." The Procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner's address book. In other words, the NSA seems to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA's surveillance.

4. The Procedures permit the NSA to collect international communications, including Americans' international communications, in bulk.

On its face, the Act permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the Act made clear that this was one of its principal purposes, and unsurprisingly, the Procedures give effect to that design. While they require the government to identify a "target" outside the country, once the target has been identified the Procedures permit the NSA to sweep up the communications of any foreigner who may be communicating "about" the target. The Procedures contemplate that the NSA will do this by "employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas," by "target[ing] Internet links that terminate in a foreign country," or by identifying "the country code of the telephone number." However the NSA does it, the result is the same: millions of communications may be swept up, Americans' international communications among them.

5. The Procedures allow the NSA to retain even purely domestic communications.

Given the permissive standards the NSA uses to determine whether prospective surveillance targets are foreigners abroad, errors are inevitable. Some of the communications the NSA collects under the Act, then, will be purely domestic. (Notably, a 2009 *New York Times* article discusses an episode in which the NSA used the Act to engage in "significant and systemic" overcollection of such domestic communications.) The Act should require the NSA to purge these communications from its databases, but it does not. The Procedures allow the government to keep and analyze even purely domestic communications if they contain significant foreign intelligence information, evidence of a crime, or encrypted information. Again, foreign intelligence information is defined exceedingly broadly. The result is that the NSA is steadily building a database of Americans' purely domestic calls and emails.

6. The Procedures allow the government to collect and retain communications protected by the attorney–client privilege.

The Procedures expressly contemplate that the NSA will collect attorney–client communications. In general, these communications receive no special protection—they can be acquired, retained, and disseminated like any other. Thus, if the NSA acquires the communications of lawyers representing individuals who have been charged before the military commissions at Guantanamo, nothing in the Procedures would seem to prohibit the NSA from sharing the communications with military prosecutors. The Procedures include a more restrictive rule for communications between attorneys and their clients who have been criminally indicted in the United States—the NSA may not share these communications with prosecutors. Even those communications, however, may be retained to the extent that they include foreign intelligence information.

7. The Procedures contemplate that the NSA will maintain "knowledge databases" containing sensitive information about Americans.

To determine whether a target is a foreigner abroad, the Procedures contemplate that the NSA will consult various NSA databases containing information collected by it and other agencies through signals intelligence, human intelligence, law enforcement, and other means. These databases—referred to as "NSA content repositories" and "knowledge databases"—apparently house internet data, including metadata that reveals online activities, as well as telephone numbers and email addresses that the agency has reason to believe are being used by U.S. persons. The Procedures' reference to "Home Location Registers," which receive updates whenever a phone "moves into a new service area," suggests that the NSA also collects some form of location information about millions of Americans' cellphones. The Procedures do not say what limits apply to these databases or what safeguards, if any, are in place to protect Americans' constitutional rights.

8. The Procedures allow the NSA to retain encrypted communications indefinitely.

The Procedures permit the NSA to retain, forever, all communications—even purely domestic ones—that are encrypted. The use of encryption to protect data is a routine and sometimes legally required practice by financial organizations, health care providers, and real-time communications services (like Skype and Apple's FaceTime). Accordingly, the Procedures permit the NSA to retain huge volumes of Americans' most sensitive information.