Your First Amendment Rights Violated: Secret Court Found That NSA Surveillance Violated Constitution

Julian Sanchez In Politics, National Security 18 hours ago

Americans are being told that there's no need to worry about the broad surveillance programs authorized by the controversial FISA Amendments Act of 2008. Yet a report from *Wired* this weekend paints a more disturbing picture: National Security Agency surveillance enabled by the FAA was found "unreasonable under the Fourth Amendment" by the secretive Foreign Intelligence Surveillance Court "on at least one occasion."

The court also found that the government's implementation of its authority under the statute had "circumvented the spirit of the law." Despite these troubling rulings from a court notorious for its deference to intelligence agencies, Congress is so unconcerned that lawmakers don't even want to know how many citizens have been caught up in the NSA's vast and growing databases.

These revelations come by way of a letter to Sen. Ron Wyden—who will be speaking about this very government spying program at Cato this Wednesday—from the Office of the Director of National Intelligence, which approved Wyden's request for declassification of a few morsels of information about secret FISA Court rulings. In the interest of permitting some minimal public debate about the FAA, which is currently before Congress for renewal, Wyden was told he would be allowed to say the following—and **only** the following publicly:

• A recent unclassified report noted that the Foreign Intelligence Surveillance Court has repeatedly held that collection carried out pursuant to the FISA Section 702 minimization procedures used by the government is reasonable under the Fourth Amendment.

• It is also true that, on at least one occasion, the Foreign Intelligence Surveillance Court held that some collection carried out pursuant to the Section 702 minimization procedures used by the government was unreasonable under the Fourth Amendment.

• I believe that the government's implementation of Section 702 of FISA has sometimes circumvented the spirit of the law, and on at least one occasion the FISA Court has reached this same conclusion.

That first statement is almost certainly a direct reference to Sen. Dianne Feinstein's assertions in a recent report from the Senate Intelligence Committee—which noted that the Court has blessed much of the surveillance under Section 702, the part of the FAA that permits warrantless acquisition of international communications.

Given the massive volume of NSA surveillance, however, the fact that some NSA surveillance was held constitutional is much less significant, for purposes of public accountability, than the fact that some of it was *unconstitutional*. Feinstein's summary of those positive classified opinions was made public weeks ago, apparently without much trouble. Yet only now that the FAA renewal has made it through multiple committees is the public permitted to know—after much tooth-pulling from a senator, via a letter released late on a Friday afternoon—how incomplete that summary really was.

It's cause for concern any time government exceeds the bounds of the Fourth Amendment, but it should be truly worrying when it's in the context of mass-scale spying by the NSA. Based on what little we know of the NSA's programs from public reports, a single "authorization" will routinely cover hundreds or thousands of phone numbers and e-mail addresses. That means that even if there's only "one occasion" on which the NSA "circumvented the spirit of the law" or flouted the Fourth Amendment, the rights of thousands of Americans could easily have been violated.

Moving from confirmed fact to mild—but I think reasonable—speculation, there is something about the peculiar phrasing of these statements worth noticing: "collection carried out pursuant to the Section 702 minimization procedures." Minimization procedures are the rules designed to limit the retention and

dissemination of irrelevant information about innocent Americans that might get picked up during authorized surveillance. In ordinary criminal wiretaps, it makes sense to talk about "collection carried out pursuant to…minimization procedures" because, under the stricter rules governing such spying, someone is supposed to be monitoring the wiretap in real time, and ensuring that innocent conversations (like a mobster's spouse or teenage kids chatting on the house line) are not recorded.

But that's not how FISA surveillance normally works. As a rare public ruling by the FISA Court explains, the standard procedure for FISA surveillance is that "large amounts of information are collected by automatic recording to be minimized after the fact." The court elaborated: "Virtually all information seized, whether by electronic surveillance or physical search, is **minimized hours, days, or weeks after collection**." (Emphasis mine.) In other words, minimization is something that normally happens *after* collection: First you intercept, then you toss out the irrelevant stuff. Intelligence officials have suggested the same in recent testimony before Congress: Communications aren't "minimized" until they're reviewed by human analysts—and given the incredible volume of NSA collection, it's unlikely that more than a small fraction of what's intercepted ever is seen by human eyes. Yet in the statements above, we have two intriguing implications: First, that "collection" and "minimization" are in some sense happening contemporaneously (otherwise how could "collection" be "pursuant to" minimization rules?) and second, that these procedures are somehow fairly intimately connected to the question of "reasonableness" under the Fourth Amendment.

To make sense of this, we need to turn to the Defense Department's somewhat counter intuitive definition of "collection" for intelligence purposes. As the Department's procedures manual explains:

Information shall be considered as "collected" only when it has been received for use by an employee of a DoD intelligence component in the course of his official duties…. Data acquired by electronic means is "collected" only when it has been processed into intelligible form.

This dovetails with a great deal of what we know about recent NSA surveillance, in which enormous quantities of communications are stored in a vast database

codenamed Pinwale for later analysis. Under the FAA, the Court doesn't review in advance whether there's probable cause to justify surveillance of any particular individual, as is normally the case with search warrants. Rather, the Court simply verifies that the NSA is employing "targeting procedures" designed to pick up communications with at least one foreign participant. By that limited standard, an algorithm designed to record every call and e-mail between the United States and Pakistan (or England) would qualify, which hardly sounds stringent enough to pass Fourth Amendment muster even under the looser rules that apply to foreign intelligence.

The language of these statements, however, would be consistent with the clever "solution" former NSA employees and whistleblowers like Bill Binney have long been telling us the agency has adopted. Referring to a massive data storage facility being constructed by NSA in Utah, Binney writes:

"The sheer size of that capacity indicates that the NSA is not filtering personal electronic communications such as email before storage but is, in fact, storing all that they are collecting. The capacity of NSA's planned infrastructure far exceeds the capacity necessary for the storage of discreet, targeted communications or even for the storage of the routing information from all electronic communications. The capacity of NSA's planned infrastructure is consistent, as a mathematical matter, with seizing both the routing information and the contents o all electronic communications."

Binney argues that when NSA officials have denied they are engaged in broad and indiscriminate "interception" of Americans' communications, they are using that term "in a very narrow way," analogous to the technical definition of "collection" above, not counting an e-mail or call as "intercepted" until it has been reviewed by human eyes. On this theory, the entire burden of satisfying the Fourth Amendment's requirement of "reasonableness" is borne by the "minimization procedures" governing the use of the massive Pinwale database. On this theory, the constitutional "search" does not occur when all these billions of calls and emails are actually intercepted (in the ordinary sense) and recorded by the NSA, but only when the database is queried.

This is a huge departure from what has traditionally been understood to be constitutionally permitted. We do not normally allow the government to

indiscriminately make copies of everyone's private correspondence, so long as they promise not to read it without a warrant: The copying *itself* is supposed to require a warrant, except in extraordinary circumstances. It appears almost certain that a very different rule is in effect now, at least for the NSA.

It cannot be overemphasized how dangerous such a change would be. Traditionally, a citizen's right to private communication was either respected or violated at the time it occurred: Your rights would be violated in real time, or not at all, and even in the lawless era of J. Edgar Hoover, only so many citizens could be spied on at once. Under this new regime, the threat to our rights is perpetual. Even if this administration and the next are scrupulous about respecting civil liberties, even if every man and woman currently employed by the NSA is noble and pure of heart, the conversation you have today may well be there for the use or misuse of whoever holds power in ten years, or fifteen, or twenty. Will the incumbent president in 2032 resist the temptation to hunt for dirt in online chats from his opponent's college years—showing greater restraint than so many past presidents? One must hope so—but better to design the rules of a free society so that such leaps of faith aren't required.