

Infiltrate the NSA

To re-establish the balance between security and civil liberties, we don't just need more laws. We need more civil libertarians in the security state.

Margo Schlanger

The story of John Ashcroft and James Comey's hospital-bed heroics has by now been told many times. On March 10, 2004, President Bush's White House counsel, Alberto Gonzales, and chief of staff, Andrew Card, went to the intensive care unit of George Washington University Hospital to try to persuade the ill attorney general, Ashcroft, to sign off on continuing massive collection of Americans' Internet "metadata," a program started in October 2001. Comey, then the deputy attorney general, had refused to reauthorize the program; its most recent authorization was scheduled to expire the next day. Comey got to his boss first, and Ashcroft refused to sign. Though pushed hard by Gonzales and Card, and also by Vice President Dick Cheney and his counsel, David Addington, Comey and several of his Department of Justice (DOJ) colleagues stood their ground and declined to ratify this domestic metadata collection based on the President's bare say-so. Once leaked in 2006, this 2004 incident was the subject of much admiring press for the DOJ lawyers. It is part of what won Comey, a Republican, his current appointment by President Obama to head the FBI. But what did this incident actually accomplish? The truth is that the dramatics were entirely out of scale to the actual, limited result, which was a pause—not a stop—to the challenged data collection. Four months after Ashcroft and Comey took their stand—and at their urging—the Foreign Intelligence Surveillance Act court reinterpreted FISA to allow the very same collection program. The authority under which the collection proceeded was new, and judges gained a supervisory role over the program, but as far as the impact on civil liberties, the change was little more than symbolic. The mindset that underlay the 2004 showdown is something that I call "intelligence legalism." In political theorist Judith Shklar's classic work, legalism is defined as "the ethical attitude that holds moral conduct to be a matter of rule following" without paying enough attention to the content of the rules in question. Intelligence legalism brings that attitude into the realm of national security and surveillance. I see intelligence legalism's three crucial and simultaneous features as: imposition of substantive rules given the status of law rather than mere policy; some limited court enforcement of those rules; and empowerment of lawyers. All three were in evidence in the 2004 drama.

Yet it is not a coincidence that that incident did not catalyze a civil liberties advance. In fact, intelligence legalism, though useful, gives systematically insufficient weight to individual liberty. Its dark side is that if the courts or the Congress have not clearly recognized a particular claim to civil liberties, that claim receives not just less attention, but no consideration at all. Our system, in other words, has made legal compliance a ceiling, not a floor, for the protection of individual liberty. The question “Is it lawful?” substitutes for “Is the cost or threat to individual liberty we are proposing worth the gain to security?” The intelligence community has learned to ask: “Can we?” What it needs to learn to ask is: “Should we?”

To strengthen civil liberties, more laws may be useful, but they are not enough. What we need as well are more—and more empowered—insiders who are attuned to civil liberties.

Disclosure, Legalism, and 9/11

Thanks to the flood of information leaked by Edward Snowden, and the disclosures the government has made in response, we have an opportunity, right now, to strengthen civil liberties against the intelligence state. We have seen a moment like this only once before, in the mid-1970s—after Watergate and the exposure of both the FBI’s COINTELPRO surveillance program and massive domestic surveillance by the CIA. The intelligence scandals of the 1970s arose out of programs remarkably similar to post-9/11 mass surveillance. Under Project Shamrock and Project Minaret, the National Security Agency (NSA) for decades collected the content of most international telegraph messages originating in the United States, and listened in on the phone calls of thousands of Americans on a secret government watch list. Under the CIA and FBI’s mail-opening program, millions of international letters were tracked and hundreds of thousands were steamed open and read. In public hearings in 1975, followed by volumes of comprehensive reports, the Pike Committee in the House and, especially, the Church Committee in the Senate documented and publicized abusive intelligence agency conduct beyond the reach of Congress and the law.

The Church Committee reports established that the intelligence community had since World War II operated outside any effective legal constraints. Consider, for example, the almost uncomprehending testimony of NSA Deputy Director Benson Buffham, facing questioning by Senator Walter Mondale, about the NSA’s warrantless surveillance of Americans’ phone calls:

Mondale: Were you concerned about its legality? Buffham: Legality? Mondale: Whether it was legal? Buffham: In what sense? Whether that would have been a legal thing to do?

Mondale: Yes. Buffham: That particular aspect didn’t enter into the discussion.

Reform took two basic approaches: disclosure—not to the public but within the executive branch and to Congress—and legalism. The most important legalistic text was FISA, enacted

in 1978. FISA protects Americans' liberty to some extent. As originally written, the act required individualized suspicion of each surveillance target, spelled out in voluminous legal papers and approved by a federal judge, to support electronic snooping on that target. Even so, FISA authorized an enormous amount of surveillance of American non-targets—after all, most communications were bound to have non-targets on one side. And once surveillance has invaded an American citizen's or resident's privacy, FISA directs the intelligence community to “minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons”—but only when such minimization is “consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.” Thus, even in its initial version, FISA categorically gave security more weight than liberty.

And then came 9/11. In the aftermath of Al Qaeda's attacks, the Bush Administration had little use for painstaking probable-cause files. Dick Cheney and his counsel, David Addington, wanted to know who was talking to whom and what they were saying—and they wanted to know fast, without involving either the judiciary or Congress. And so the President initiated three massive surveillance programs: Internet metadata collection, which beginning in 2001 tracked Americans' email communications; telephone metadata collection, which did the same for Americans' phone calls; and warrantless interception of international emails and phone calls from within the United States where one party was thought to be engaged in or preparing for international terrorism. It was the 1960s all over again.

But this time the White House's initial enthusiasm for unilateral action ran into lawyers socialized into post-Church Committee intelligence legalism. Those Bush Administration lawyers were aghast—not at the idea of collecting network information on hundreds of millions of emails and phone calls of hundreds of millions of innocent Americans, but at doing so without proper legal authority. And so they tidied up. They first persuaded the FISA court to authorize the Internet metadata program, and then the telephone metadata program. The court went back and forth on whether FISA allowed the NSA's ongoing massive foreign target content collection, too—but when the court eventually declined, the Administration persuaded Congress to amend FISA. By 2007, the FISA court and Congress had together, and mostly in secret, broadened FISA into a bulk surveillance statute. The NSA's surveillance of Americans without individualized justification was no longer a go-it-alone presidential project. The FISA court's analysis of the legality of the programs was classified; few members of Congress knew much about the programs, but in any event, their thoughts were, likewise, classified. For intelligence legalists, the necessary boxes were checked. Neither disclosure nor legalism, in other words, turned out to pose much of an obstacle to the “collect everything” ambitions of the post-9/11 security state.

Yet even when judges, acting in secret, aren't prepared to hold a surveillance program illegal, and Congress, acting in secret, isn't prepared to shut it down, that does not mean that bulk surveillance of Americans is a good idea. To decide what kind of surveillance we should all live under requires actual policy analysis: weighing the security gains against the liberty costs. Ideally, that weighing should occur in public. That's where we are now.

Snowden and Intelligence Reform

Which brings us back to Edward Snowden. Since The Guardian broke the story of the NSA's top-secret PRISM program in June 2013, dozens of reforms have been proposed for the NSA concerning the surveillance of Americans. The President appointed a blue-ribbon "Review Group on Intelligence and Communications Technologies" that offered him 46 recommendations. The independent Privacy and Civil Liberties Oversight Board, finally operational after years of Senate delays in confirming its members, issued its first two reports, with 22 recommendations between them. Advocacy organizations have weighed in, as have scholars, former government officials, journalists, and newspaper editorial boards. The President himself has responded by announcing a number of reforms and initiating a process to evaluate others. (In Congress, the so-called USA Freedom Act passed the House last May, but died in the Senate in November. Congressional proposals to end bulk collection of metadata and reform FISA courts will undoubtedly resurface.)

As they should, many reform proposals would change the rules that govern surveillance. For example, Congress should insist on tighter rules governing collection, and should require individual rather than group justifications for data acquisition, analysis, and use. Whatever steps are chosen can then be enforced by the courts, inspectors general, agency lawyers, and compliance staffs.

At the same time, there is an additional opportunity to strengthen individual liberty and privacy with interventions that are less legalistic. Several recent proposals attempt to build offices within the executive branch—with full access to highly classified information—that can advocate for civil liberties interests that are broader than those recognized by the courts or Congress:

- The President announced in August 2013 that the NSA would "put in place a full-time civil liberties and privacy officer." The new NSA civil liberties and privacy officer, Rebecca Richards, began work in January 2014.
- The President's Review Group recommended "the creation of a privacy and civil liberties policy official located both in the National Security Council Staff and the Office of Management and Budget." Several White House staffers are now assigned to this role.
- A reform proposal endorsed (at least in weak form) by nearly everyone is to adjust FISA proceedings by introducing a public advocate. The President's Review Group

recommended the creation of a “Public Interest Advocate to represent privacy and civil liberties interests” in the FISA court, allowing the court to invite participation, but also allowing the advocate to “intervene on her own initiative.” Similarly, the President called on Congress “to authorize the establishment of a panel of advocates from outside government to provide an independent voice in significant cases before the Foreign Intelligence Surveillance Court.” Both the House and Senate versions of the USA Freedom Act would have provided for an advocate, although details differed.

What ties these initiatives together is that they all propose to police the intelligence community by amplifying civil liberties advocacy inside institutions hidden from the public eye. In most activities of government, outside scrutiny and accountability can promote good policy. In the secret world of the intelligence community, however, these methods are largely unavailable—there’s simply too much the public doesn’t, and can’t, know. Therefore, the proposals listed rely on the designation of in-house officials to prioritize privacy and civil liberties—values that otherwise lack advocates within the intelligence community’s governance structure.

Can such an approach actually work? Skeptics, who are many, say no. But I say maybe it can. Institutional design is important; civil liberties offices need deliberate and careful arrangements to safeguard their influence and commitment. The ideas here are no panacea, but they can play a useful role in filling the civil liberties gap that intelligence legalism creates. Here are ways to make them work.

NSA Office of Civil Liberties and Privacy

The NSA has a new Office of Civil Liberties and Privacy, which has the difficult assignment of decreasing the civil liberties impact of NSA operations. The new office’s procedures and role are still evolving. Its current staff allocation is just its director, Richards, and six others—probably too small for staff to be at every table where their perspective would be useful. Richards, who ran privacy compliance at the Department of Homeland Security (DHS), is respected by civil liberties advocates, but that hardly guarantees her success. This office faces twin dangers: impotence on the one hand, and capture or assimilation on the other.

Begin with impotence: Any internal governmental office whose mission is to constrain its agency (I have in my academic work given such shops the generic title “Offices of Goodness”) runs the risk of losing influence and being ignored, whether by being excluded from internal processes or by having its attempted contributions rebuffed.

There is already a large compliance staff at NSA, hundreds of people who are charged with ensuring the agency abides by the constraints imposed by statute and executive and court order. If the NSA’s civil liberties office is going to add anything distinctive, it will need to go beyond intelligence legalism. For example, the Supreme Court so far has not held that

metadata surveillance violates the Constitution's requirement that the government undertake only reasonable searches. Yet it is obvious that even if bulk metadata collection is legal, it still imposes major costs to Americans' privacy. To advocate against bulk metadata surveillance because of those costs—arguing, perhaps, that the gain to security is too small to justify continuation of the program—instead of limiting the discussion to the letter of the law is to shift from a compliance framework to a policy framework, adding protection of interests on top of the existing respect for clearly established rights.

There are organizational risks involved in such a move. A compliance framework provides significant legitimation for the office's activities. Intelligence legalism is powerful, and it dictates that government agencies must obey the rules. If the new office pushes for more liberty-protective policy, it will lack that legitimation. And so it will be especially vulnerable to being bureaucratically frozen out—disinvited to meetings, kept off distribution lists, or invited but ignored.