‘We Kill People Based on Metadata’

David Cole

Supporters of the National Security Agency inevitably defend its sweeping collection of phone and Internet records on the ground that it is only collecting so-called “metadata”—who you call, when you call, how long you talk. Since this does not include the actual content of the communications, the threat to privacy is said to be negligible. That argument is profoundly misleading.

Of course knowing the content of a call can be crucial to establishing a particular threat. But metadata alone can provide an extremely detailed picture of a person’s most intimate associations and interests, and it’s actually much easier as a technological matter to search huge amounts of metadata than to listen to millions of phone calls. As NSA General Counsel Stewart Baker has said, “metadata absolutely tells you everything about somebody’s life. If you have enough metadata, you don’t really need content.” When I quoted Baker at a recent debate at Johns Hopkins University, my opponent, General Michael Hayden, former director of the NSA and the CIA, called Baker’s comment “absolutely correct,” and raised him one, asserting, “We kill people based on metadata.”

It is precisely this power to collect our metadata that has prompted one of Congress’s most bipartisan initiatives in recent years. On May 7, the House Judiciary Committee voted 32-0 to adopt an amended form of the USA Freedom Act, a bill to rein in NSA spying on Americans, initially proposed by Democratic Senator Patrick Leahy and Republican Congressman James Sensenbrenner. On May 8, the House Intelligence Committee, which has until now opposed any real reform of the NSA, also unanimously approved the same bill. And the Obama administration has welcomed the development.

For some, no doubt, the very fact that this bill has attracted such broad bipartisan
approval will be grounds for suspicion. After all, this is the same Congress that repeatedly reauthorized the 2001 USA Patriot Act, a law that was also proposed by Sensenbrenner and on which the bulk collection of metadata was said to rest—even if many members of Congress were not aware of how the NSA was using (or abusing) it. And this is the same administration that retained the NSA’s data collection program, inherited from its predecessor, as long as it was a secret, and only called for reform when the American people learned from the disclosures of NSA contractor Edward Snowden that the government was routinely collecting phone and Internet records on all of us. So, one might well ask, if Congress and the White House, Republicans and Democrats, liberals and conservatives, all now agree on reform, how meaningful can the reform be?

This is a reasonable question. This compromise bill addresses only one part of the NSA’s surveillance activities, and does not do nearly enough to address the many other privacy-invasive practices that we now know the NSA has undertaken. But it’s nonetheless an important first step, and would introduce several crucial reforms affecting all Americans.

First, and most importantly, it would significantly limit the collection of phone metadata and other “business records.” Until now, the NSA and the Foreign Intelligence Surveillance Court have aggressively interpreted a USA Patriot Act provision that authorized collection of business records “relevant” to a counterterrorism investigation. The NSA convinced the court that because it might be useful in the future to search through anyone’s calling history to see if that person had been in contact with a suspected terrorist, the agency should be able to collect everyone’s records and store them for five years.

The NSA has said it only searched its vast database of our calling records when it had reasonable suspicion that a phone number was connected to terrorism. But it did not have to demonstrate the basis for this suspicion to a judge. Moreover, it was authorized to collect data on all callers one, two, or three steps removed from the suspect number—an authority that can quickly generate more than one million phone numbers of innocent Americans from a single suspect source number. The fact that you may have called someone (say, your aunt) who in turn called someone (say, the Pizza Hut delivery guy) who was in turn once called by a suspected terrorist says nothing about whether you’ve engaged in wrongdoing. But it will land you in the NSA’s database of suspected terrorist contacts.

Under the USA Freedom Act, the NSA would be prohibited from collecting phone and Internet data en masse. Instead, such records would remain with the telephone and Internet companies, and the NSA would only be authorized to approach those companies on an individual, case-by-case basis, and only when it could first satisfy the Foreign Intelligence Surveillance Court that there is reasonable suspicion that a particular person, entity, or account is linked to an
reasonable suspicion that a particular person, entity, or account is linked to an international terrorist or a representative of a foreign government or political organization. This is much closer to the specific kind of suspicion that the Fourth Amendment generally requires for intrusions on privacy. At that point, the court could order phone companies to produce phone calling records of all numbers that communicated with the suspect number (the first “hop”), as well as all numbers with which those numbers in turn communicated (the second “hop”).

Further restrictions are necessary. Through these authorized searches the NSA would still be able to collect large amounts of metadata on persons whose only “sin” was that they called or were called by someone who called or was called by a suspected terrorist or foreign agent. At a minimum, “back-end” limits on how the NSA searches its storehouse of phone numbers are still needed. But the bill would at least end the practice of collecting everyone’s calling records.

Second, the new House bill imposes similar limits on other USA Patriot Act provisions that were susceptible to being used, or had been used, to authorize collection of data in bulk. These include a provision empowering the government to obtain information by “national security letters,” a kind of administrative subpoena issued without judicial oversight, and “pen registers,” which intercept Internet and phone trafficking data. All of these powers would now be limited by the same requirement that the government seek case-by-case warrants based on suspicion about a particular person or group. The point is to end bulk collection of data across the board, and return the agency to the more targeted searches and inquiries that US laws have historically deemed reasonable.

Third, the bill would establish a panel of legal experts, appointed by the presiding judges of the Foreign Intelligence Surveillance Court, who would participate in proceedings before the court when it addresses “a novel or significant interpretation of law,” and in any other proceedings at the court’s discretion. They would appear as amicus curiae, or “friends of the court,” but their purpose would be to add an independent assessment of the legal issues involved, ensuring that the court is not hearing only from the government. Such a panel would increase the likelihood that difficult legal issues get a full and fair consideration, and would likely shore up the public legitimacy of the secret court, which as of now is dismissed by many, rightly or wrongly, as a “rubber stamp.”

Finally, the bill contains a number of measures designed to increase transparency and oversight. It would require the attorney general to request the declassification of opinions of the FISA court, permit private Internet and telephone companies to report semiannually on the volume of records they were required to produce, and require the Inspectors General of the Justice Department and the Intelligence Community to report on the numbers of records requested and the effectiveness of the program. Had Verizon been permitted to report, for example, that it was
of the program. Had Verizon been permitted to report, for example, that it was being compelled to turn over hundreds of millions of phone records on its customers to the NSA, and had the Inspector General informed us that the program had stopped not a single terrorist act, it is likely that bulk collection would have been cut short long ago.

Even with all these reforms, however, the USA Freedom Act only skims the surface. It does not address, for example, the NSA’s guerilla-like tactics of inserting vulnerabilities into computer software and drivers, to be exploited later to surreptitiously intercept private communications. It also focuses exclusively on reining in the NSA’s direct spying on Americans. As Snowden’s disclosures have shown, the NSA collects far more private information on foreigners—including the content as well as the metadata of e-mails, online chats, social media, and phone calls—than on US citizens.

The FISA Amendments Act of 2008 permits the NSA to intercept the content of communications when it can demonstrate nothing more than reason to believe that its targets are foreign nationals living abroad, and that the information might relate to “foreign intelligence.” “Foreign intelligence” is in turn defined to include any information that might inform our foreign affairs, which is no restriction at all. Under this authority, the NSA established the PRISM program, which collects both content and metadata from e-mail, Internet, and phone communications by millions of users worldwide. It is probably under this authority that, according to The Washington Post, the NSA is recording “every single” phone call from a particular, unnamed country. Documents leaked by Snowden demonstrate that the NSA also collects, again by the millions and billions, foreign nationals’ e-mail contact lists, cell phone location data, and texts. This is the very definition of dragnet surveillance.

Congress is far less motivated to do anything about the NSA’s abuse of the rights of foreign nationals. They are “them,” not “us.” They don’t vote. But they have human rights, too; the right to privacy, recognized in the International Covenant on Civil and Political Rights, which the US has signed and ratified, does not limit protections to Americans. Snowden’s revelations have justifiably led to protests from many of our closest allies; they don’t want their privacy invaded by the NSA any more than we do, and they have more to complain about than we do, as they have suffered far greater intrusions.

In the Internet era, it is increasingly common that everyone’s communications cross national boundaries. That makes all of us vulnerable, for when the government collects data in bulk from people it believes are foreign nationals, it is almost certain to sweep up lots of communications in which Americans are involved. The initial version of the USA Freedom Act accordingly sought to limit the NSA’s ability to conduct so-called “back door” searches of content collected
from foreigners for communications with Americans citizens. But that provision was stripped in committee, leaving the back door wide open.

Defense hawks will argue that even these reforms go too far, and that we may be risking our security by tying the NSA’s hands. But as the Privacy and Civil Liberties Oversight Board found, there is little evidence that the metadata program has made us safer. Moreover, if we want to preserve the liberties that define us as a democratic society, we have to learn to live with risk. It is the insistence on preemptively eliminating all terrorist threats—an unattainable goal—that led the NSA to collect so much information so expansively in the first place.

The fact that the USA Freedom Act has achieved such wide-ranging support may be less an indication of its compromises than of a fundamental shift in American views. In July 2013, following the Snowden revelations, the Pew Research Center reported that for the first time since it started asking the question in 2004, more Americans expressed concern that counter-terrorism measures were infringing their civil liberties than worried that the government was not doing enough to keep them safe.

Congress is responsive to such shifts in popular opinion. The question now is whether that new attitude can be translated into more systemic reform, or whether enactment of this bill will placate enough people that the demand for further reform fizzles. If the Senate can pass or even strengthen the USA Freedom Act, as Senator Leahy has said he intends to do, it will be a significant achievement for civil liberties. But the biggest mistake any of us could make would be to conclude that this bill solves the problem.

May 10, 2014, 10:12 a.m.
How Many Have We Killed?
David Cole

The NSA vs. Free Speech
Kenneth Roth

What the NSA Knows
James Bamford