THE NSA, THE METADATA PROGRAM, AND THE FISC

*GEOFFREY R. STONE**

In the fall of 2013, after Edward Snowden's leaks of classified information, President Obama appointed me to serve on a five-person Review Group charged with evaluating the National Security Agency's (NSA) foreign intelligence surveillance programs. This was an extraordinary experience, and I thought I would reflect a bit on that experience this afternoon.

In our first meeting in the situation room, President Obama told us that he wanted the Review Group to serve as an independent body that would advise him about how best to strike an appropriate balance between protecting national security and preserving civil liberties. He made it very clear that he wanted us to be rigorous, tough-minded, and honest in every way.

We were a diverse group in terms of our professional backgrounds, experiences, and ways of thinking about these issues. There was Michael Morell, who had spent his career with the Central Intelligence Agency (CIA), including two stints as acting director; Richard Clarke, a veteran of the State and Defense Departments in four presidential administrations and an expert in cybersecurity; Peter Swire, a professor at Georgia Tech who had served in both the Clinton and Obama administrations as an expert on issues of privacy and information technology; and Cass Sunstein, one of our nation's most distinguished legal scholars who had just finished a stint in the Office of Management and Budget during the Obama administration. And then there was me, a constitutional law professor at the University of Chicago and a self-professed civil libertarian. It was quite clear, given the makeup of the Review Group, that we would agree on nothing. As Susan Rice later commented to us, we were "five highly egotistical, high-testosterone guys" who were being "thrown in a room together, with nobody in charge, and expected to solve a set of intractable problems."

But as we spent five months together, working three or four days each week in a secure facility in our nation's capital, we came to trust, respect, and learn from one other so much that, to our amazement, we eventually produced a 300-page report including

* Edward H. Levi Distinguished Service Professor of Law, The University of Chicago.

forty-six *unanimous* recommendations.[1] None of us would have imagined that that was possible when we began.

Before turning to specific recommendations, I should offer two general observations. The first concerns the NSA. From the very outset, I approached my responsibilities as a member of the Review Group with great skepticism about the NSA. I assumed that the most problematic surveillance programs that Edward Snowden had brought to light were the result of an NSA run amok. I could not have been more wrong. In the end, I came away with a view of the NSA that I found quite surprising.

Not only did I find that the NSA had helped to thwart numerous terrorist plots against the United States and its allies in the years since 9/11, I also found that it was an organization that operated with a high degree of integrity and a deep commitment to the rule of law. The Review Group found no evidence that the NSA had knowingly or intentionally engaged in unlawful or unauthorized activity. To the contrary, it worked hard to ensure that it operated within the bounds of its authority.

This is not to say that the NSA should have had all of the authorities it was given. As I discuss in more detail below, the Review Group found that many of the programs undertaken by the NSA, such as the Section 215 Metadata Program, were highly problematic. But the responsibility for directing the NSA to carry out those programs rested not with the NSA itself, but with the Executive Branch, the Congress, and the Foreign Intelligence Surveillance Court (FISC), which expressly authorized those programs.

To be clear, I am not saying that we should trust the NSA. We should not. The NSA, like the Federal Bureau of Investigation (FBI), the CIA, and similar agencies of government, necessarily has broad powers of surveillance and investigation. There is always the risk that such agencies will abuse those powers to the detriment of the nation. The NSA should therefore be subject to constant and rigorous review and oversight. The work it does, although important to the safety of our nation, poses great dangers to core American values. Careful and ongoing oversight of the NSA and its programs is therefore imperative.

My second general observation concerns the issue of oversight. As a member of the Review Group, I had a rare opportunity to ob-

1. *See* RICHARD A. CLARKE, MICHAEL J. MORELL, GEOFFREY R. STONE, CASS R. SUNSTEIN & PETER SWIRE, THE NSA REPORT: LIBERTY AND SECURITY IN A CHANGING WORLD: THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (2014).

serve and evaluate the various mechanisms our government uses to oversee the activities of our nation's intelligence agencies. At the structural level, I was surprised by the variety and range of oversight mechanisms in place. The NSA's activities, for example, are overseen by the NSA's Inspector General, the Director of National Intelligence, the FISC, the Department of Justice, the Privacy and Civil Liberties Oversight Board, and the Senate and House Intelligence Committees. Cumulatively, we found that these oversight mechanisms worked reasonably well when it came to ensuring that the NSA properly implemented the authorities it had been given.

We were less impressed, though, with oversight of a different sort. Once the government, whether the Executive Branch, the Congress, or the FISC, authorized the intelligence agencies to undertake certain types of surveillance, there was insufficient attention to whether the programs instituted under those authorities could or should be refined and improved over time. This sort of retrospective oversight—constantly evaluating and re-evaluating programs to ensure that they are properly designed to respect fundamental interests in individual privacy and civil liberties—is absolutely essential. The issue here is not whether the intelligence agencies are violating the rules, but whether the rules themselves should constantly be re-examined.

This is so, because with experience over time it is often possible to identify ways in which programs can be refined and narrowed in order to strike a better balance between the interests of national security and individual liberty. That, indeed, was the central theme of the Review Group's recommendations. What we found, in program after program, was that significant refinements could and should be made that would better protect personal privacy and individual freedom without unduly interfering with the capacity of these programs to keep our nation safe. That an extraordinary and ad hoc institution like the Review Group was necessary to bring these recommendations to light suggested, quite strongly, that existing oversight mechanisms were not performing this function adequately.

Let me turn now to two of the Review Group's specific recommendations. The report contains forty-six recommendations, but that understates the number of issues addressed. Many of our recommendations had multiple subparts, so there were about 200 recommendations in all. The recommendations addressed a broad range of issues, but I will focus, for illustrative purposes, on two areas: the collection of telephone metadata and the role of the FISC.

Before 1978, when the government engaged in foreign intelligence surveillance, whether in the United States or abroad, it was subject only to the discretion of the President as commander in chief. There were no legislative restrictions, and there was no judicial involvement or oversight of anything the President did in the name of foreign intelligence surveillance. In the 1970s, grave abuses by the FBI, the CIA, the NSA, and Army Intelligence under the auspices of J. Edgar Hoover, Lyndon Johnson, and Richard Nixon came to light. For various, though mostly political, reasons, they had engaged in surveillance of American citizens that was understood to be inappropriate—and in some instances illegal—and often highly invasive of privacy beyond the scope of any agency's authority.[2]

Congress decided to do something to rein this in, ultimately resulting in the Foreign Intelligence Surveillance Act of 1978.[3] That legislation did many things, but most importantly, it brought various elements of foreign intelligence surveillance under the rule of law through the creation of the FISC, which for the first time empowered judges to oversee foreign intelligence surveillance that took place inside the United States.

Ordinary federal courts do not have security clearances, and a great deal of foreign intelligence information is classified. Therefore, you could not have an ordinary federal judge deciding whether the executive branch could undertake a foreign intelligence wiretap. The FISC enabled judges to play their traditional role in overseeing what the executive branch did in the classified realm. The court was authorized to deal with foreign intelligence surveillance that took place inside the United States. What the President did outside the United States was regarded as beyond the scope of even Congress's business at that time.

From the late 1970s until 9/11, that process worked reasonably well. There was a wake-up call after 9/11, though, and public support grew for granting the intelligence agencies much greater capacity in order to prevent such attacks in the future. Congress made a number of modifications to the Foreign Intelligence Surveillance Act in the wake of 9/11 to strengthen the agencies' ability to ferret out information about possible terrorist plots.

2. *See* GEOFFREY R. STONE, PERILOUS TIMES: FREE SPEECH IN WARTIME FROM THE SEDITION ACT OF 1798 TO THE WAR ON TERRORISM 496–97 (2004).

3. 50 U.S.C. §§ 1801–1885.

One of the provisions of the new legislation was Section 215 of the Foreign Intelligence Surveillance Act,[4] which authorized the agencies to go to the FISC to obtain an order based on reasonable and articulable suspicion that a suspect was engaged in international terrorist activity.

If the agencies made such a showing, the FISC could then issue an order that authorized them to go to banks, credit card companies, telephone companies, internet companies, etc., and serve the equivalent of a subpoena demanding records about the individual in question.

In 2006, as technology changed, the NSA came to the FISC and proposed a new program to gather telephone metadata from huge numbers of phone calls that took place in the United States—and to hold that data for five years. That metadata consists of phone numbers: every phone number covered by the order, every number called by every phone number covered by the order, and every number that calls every phone number covered by the order. It doesn't include names, it doesn't include geographical locations, and it doesn't include content, but it includes huge amounts of numbers, typically covering tens if not hundreds of millions of Americans each year.

The intelligence agencies wanted this information because they now had the technological capability to manage a database of that magnitude. The FISC, the Senate and House intelligence committees, and the Department of Justice approved the program.[5] It enabled the NSA, when it had reasonable and articulable suspicion that a particular telephone number—almost invariably a number outside the United States—was associated with a person suspected of terrorist activity, to query the database. That is, an NSA analyst could type in the phone number of the suspected terrorist and the database would return information about the numbers with which the suspect's number was in contact.

The idea was to connect the dots. Although the program collected massive amounts of data, it was designed not to reveal that

4. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act") of 2001, Pub. L. 107-56, § 215, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861(a)(1) (2006 & Supp. V 2011)).

5. *See In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from [Telecommunications Providers] Relating to [Redacted version], Order No. BR-05 (FISA Ct. May 24, 2006). The government explained the rationale for the program in FEDERATION OF AMERICAN SCIENTISTS, BULK COLLECTION OF TELEPHONY META-DATA UNDER SECTION 215 OF THE USA PATRIOT ACT 35 (Aug. 9, 2013).

data to the NSA indiscriminately. When the analysts queried a suspected number, the information they received reflected only the numbers associated with other suspected terrorists that the queried number had been in contact with. The goal, in other words, was to determine whether a suspected terrorist outside the United States was speaking, directly or indirectly, to a suspected terrorist inside the United States.[6]

In 2012, the most recent year for which full data was available, the NSA queried the database for 288 numbers. Those 288 numbers yielded twelve tips.

That is, in twelve instances based on those 288 queries, agents discovered that the suspected terrorists outside the United States were communicating, directly or indirectly, with numbers associated with terrorist suspects in the United States.

In those twelve instances, the NSA turned the information over to the FBI for further investigation.

None of the twelve tips in 2012 produced information that was useful in preventing a planned terrorist attack. In fact, in the seven years during which the program had existed up to that point, there had not been a single instance in which the metadata program had led directly to the prevention of a terrorist attack. Many other programs employed by the NSA have had very productive results, but not this one.[7]

Defenders of the program argued, not unreasonably, that the fact that the program had yet to turn up information that prevented a terrorist attack did not represent a failure. An effort to prevent attacks on the scale of 9/11—including possible nuclear, chemical, or biological attacks—might yield meaningful information only once in a decade. Failing to prevent such an attack, though, would be catastrophic. Thus, the program was analogous to a fire alarm in one's home. It might save your life only once a decade, but that doesn't mean you toss it out or don't replace the batteries.

After evaluating the program, we concluded that, although it was not as draconian as the public had been led to believe, it was not sufficiently limited to protect the legitimate privacy interests of Americans. With that in mind, we made three fundamental recommendations with regard to the program:

First, the government itself should not hold the database. As historical experience teaches, one of the grave dangers of aggres-

6. *See* CLARKE ET AL., *supra* note 1, at 48–55.

7. *See id.* at 56–57.

sive surveillance is that some misguided public official—whether a J. Edgar Hoover or a Richard Nixon—will use this extraordinary pool of data to do harm. To learn information, for example, about free speech, about political associations, about political enemies. Although the metadata consists only of phone numbers, if you look at the pattern of a person's calls over an extended period of time, you can learn an awful lot that can be put to nefarious use. Therefore, we recommended that the information should remain in the hands of the telephone service providers, who already have it for billing purposes. But the government itself should not hold the data.[8] Recognizing that it might prove difficult to implement the program efficiently if the data remains in the possession of individual telephone service providers, we recommended that, if that proves to be the case, "the government might authorize a specially designated private organization to collect and store the bulk telephony meta-data."[9]

Second, we recommended that the NSA should not be able to query the database without a court order. Human nature being what it is, the people engaged in the enterprise of finding bad guys are likely to err on the side of suspicion where a neutral or detached observer might not. That's why we ordinarily require search warrants issued by neutral and detached judges in criminal investigations. We therefore recommended that the NSA should not be allowed to query the database on the basis of its own analysts' judgment. The FISC should have to determine independently in each instance whether the standard of reasonable and articulable suspicion is met. This requirement would also reduce substantially the risk of unlawful access to the database.

Third, we recommended that the data should not be held for more than two years. We concluded that five years is unnecessary. The data gets stale, its value depreciates, and the risks of misuse increase as the information accumulates.[10]

These recommendations, I'm pleased to say, were all incorporated into the USA Freedom Act, which was adopted by Congress and signed into law by President Obama on June 2, 2015.[11]

---

8. *See id.* at 67–71 (Recommendation 5).

9. *See id.* at 71.

10. *See id.* at 70 n.118.

11. *See* Pub. L. No. 114-23, 129 Stat. 268 (2015); Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html [https://perma.cc/8397-7KQY].

Interestingly, the media have recently reported that the NSA has now recommended that the Section 215 metadata program should be abandoned.[12] This is not surprising. The program is very expensive and it has not yielded any significant results. Indeed, the NSA had a similar program for emails, but it voluntarily abandoned that program before the Snowden disclosures for these reasons. It might well have done the same as far back as 2014 with the telephone metadata program, but once Snowden leaked the existence of the program, I suspect that the NSA could not terminate the program because it would have been seen, mistakenly, as a "victory" for Edward Snowden.

A second issue worth noting involves the operations of the FISC. The FISC was initially designed primarily to issue search warrants and to limit the ability of Presidents to authorize foreign intelligence surveillance in the United States without judicial oversight. What became evident over time, though, was that at least on some occasions the FISC would have to decide not only whether the government could show probable cause or reasonable suspicion for a particular investigation but whether and how certain novel methods of surveillance were governed by the law. Sometimes these involved complex questions of statutory or constitutional interpretation. This was illustrated, for example, by the FISC's decision to permit the Section 215 metadata program.[13]

The Review Group's judgment was that when such issues arise, the FISC judges should hear arguments not only from the government, but also from advocates on the other side, just as would any other court. We therefore recommended the creation of a privacy and civil liberties advocate to represent the other side when these sorts of complex legal and constitutional issues arise.[14] The FISC judges objected to this recommendation. They argued that they were responsible jurists who could sort through the legal issues on their own. President Obama compromised on this. He adopted the recommendation that there should be a privacy and civil liberties advocate, but he concluded that this advocate should be authorized to participate in the proceedings of the FISC only if the judges of

12. *See* Dustin Volz & Warren P. Strobel, *NSA Recommends Dropping Phone-Surveillance Program*, WALL ST. J. (Apr. 24, 2019).

13. *See In re* Application of the Federal Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Telecommunications Providers] Relating to [Redacted version], Order No. BR-05 (FISA Ct. May 24, 2006); CLARKE ET AL., *supra* note 1, at 48.

14. *See* CLARKE ET AL., *supra* note 1, at 146–153 (Recommendation 28).

that court invited such participation. This recommendation, too, was enacted into law in the USA Freedom Act.[15]

Of course, not everything the Review Group recommended was enacted into law. But perhaps the most important lesson of this experience is that regular outside reviews conducted by independent experts charged with the task of rigorously evaluating existing programs and making recommendations designed to improve them are essential both to our national security and to the protection of our individual liberties. This should be a model for the future.

15. *See* 129 Stat. 268 (2015).