BALANCING PRIVACY AND SECURITY

STEVEN G. BRADBURY*

When it comes to balancing privacy and security, the Constitution does an excellent job of achieving that balance. On the one hand, national security, in its most fundamental sense—meaning protecting the United States and Americans from foreign attack—is an imperative. In a very practical sense, without effective national security, we would lose all of the other freedoms enshrined in the Constitution. Looking out for national security is undeniably a legitimate and proper function of the federal government.[1] In the war on terror, of which September 11 is a cardinal example, "signals intelligence" (sometimes called communications intelligence) is a critical element in our ability to protect the country. Discovering the hidden cells of terrorist organizations requires diligent communications intelligence, and in the realm of foreign threats to the U.S., that is precisely the mission of the National Security Agency (NSA).[2]

But there is another equally important imperative represented by the Fourth Amendment. The Fourth Amendment protects all Americans against unreasonable searches by the government.[3] This protection is among the core civil liberties that our Constitution was intended to preserve. Prior to 1967, the Supreme Court interpreted this protection to mean freedom from an unreasonable physical invasion or trespass of an individual's pri-

---

* Partner, Dechert LLP; Acting Assistant Attorney General (2005–2007) and Principal Deputy Assistant Attorney General (2004–2009), Office of Legal Counsel, U.S. Department of Justice. This essay was adapted from remarks given at the 2014 Federalist Society Annual Student Symposium at the University of Florida in Gainesville, Florida.

1. U.S. CONST. pmbl. (stating that the purpose of our government is, in part, to "provide for the common defence . . . and secure the Blessings of Liberty to ourselves and our Posterity").

2. Exec. Order No. 12,333, 46 Fed. Reg. 59,941 (Dec. 4, 1981) (establishing and delineating the NSA's roles and responsibilities).

3. U.S. CONST. amend. IV.

vate sphere, like the home or physical property.[4] Absent such a physical invasion, there was no "search" within the ambit of the Fourth Amendment. In 1967, the Court changed or clarified the standard for what is a Fourth Amendment "search" to focus instead on whether the government's action involves an encroachment on a person's "reasonable expectation of privacy" (whether involving a physical invasion or not).[5] That remains today the judicially constructed definition of a "search" under the Fourth Amendment.[6]

The fundamental principles of the Fourth Amendment mesh nicely with the needs of the national government to protect the country from foreign attack. In other words, James Madison well understood what he was doing![7] Indeed, the Constitution he helped to craft achieves just the right equilibrium. Under our Constitution, there is no necessary conflict between the needs of national security, including the mission of the National Security Agency, and the protection of the legitimate and reasonable expectations of privacy of Americans to be free from unreasonable invasion by the government. The structure of the Constitution provides a harmonious balance.

In response to political calls for greater protection of privacy, Congress may provide through legislation for additional protections over and above the baseline protections of the Constitution. There is a particular interest in legislating heightened protections in this age when technology is rapidly developing and enabling citizens to extend their lives, their personalities, and their most private thoughts out to the whole world over the Internet through digital communications.

Sometimes those statutory protections, however, can infringe on the functions and mission of our intelligence agencies in protecting the country against foreign threats, and in that event, we may see modulations in the level of statutory protec-

---

4. *See, e.g.*, Goldman v. United States, 316 U.S. 129, 134–36 (1942); Olmstead v. United States, 277 U.S. 438, 466 (1928).

5. Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

6. *See, e.g.*, United States v. Jones, 132 S. Ct. 945, 950 (2012).

7. James Madison introduced the Fourth Amendment in the House of Representatives. *See* James Madison, Speech to the House of Representatives (June 8, 1789), *in* 12 THE PAPERS OF JAMES MADISON 197, 201 (Robert A. Rutland et al. eds., 1977).

tion over time.[8] Sometimes Congress goes a little too far in ratcheting down and restricting what can be done, and other times statutory protections are modified, or modulated, to give the executive branch more leeway in responding to foreign threats. Indeed, we have seen this happen even since September 11. My view is that the current state of statutory law, as an overlay on the fundamental principles of the Fourth Amendment, has it just about right. We have reestablished a good equilibrium, and I think the activities of the National Security Agency, which I believe are fully consistent with the statutes that Congress has passed and with the Fourth Amendment, respect that balance.

A great debate is raging because of the disclosures of Edward Snowden about the National Security Agency's programs. Exposing those security programs to public debate, and, of course, to the knowledge of our enemies, results in vigorous disagreement about the importance and the dangers of these programs. I believe that the Snowden leaks have been hugely damaging to our national security. At the same time, I acknowledge that the ensuing public debate is extremely healthy. We have had great debates over the proper level of statutory civil liberties protections in the face of national security needs before; this debate is not unprecedented. But it can provide an important national "teaching moment" in terms of informing the depth of understanding of our constitutional structures by the average American. The programs of the National Security Agency that have been exposed by the Snowden leaks and by the additional declassification and release of further details by the government,[9] as well as the public debate over those programs, provide a good model for discussing and comparing the principles under the Fourth Amendment on the one hand, and some of the basic concepts that inform our concerns about balancing national security and privacy on the other.

---

8. *See generally* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757 (2014) (describing privacy protection legislation instituted since September 11).

9. *See, e.g.*, Brendan Sasso, *US declassifies details of NSA phone call surveillance program*, THE HILL (July 31, 2013, 7:15 PM), http://thehill.com/policy/technology/314771-administration-declassifies-details-of-phone-spying [http://perma.cc/PD53-VJ9J].

If you look at the two principal programs of the National Security Agency that have been disclosed,[10] they nicely illustrate some fundamental concepts under the Fourth Amendment. In addition, they inform the debate about whether Congress should go significantly further than it has gone to restrict the activities of the intelligence agencies. This debate is hugely important and historic, and largely thanks to this debate, we are living through an interesting time to be a constitutional scholar and to be a student of national security and national security law.

Let me describe the two major national security programs at issue in this debate. Because these programs aptly illustrate fundamental principles of the Fourth Amendment, I think all Americans should know more about them, especially before taking sides in the debate. The first of the two NSA programs at issue is the (by now well-known and much maligned) telephone metadata program.[11] The second program is the collection of communications content that is targeted at non-U.S. persons who are believed to be located outside the United States.[12] As that description suggests, the second program focuses on international communications.[13]

The first program, the telephone metadata collection, does not involve listening in on phone calls.[14] Indeed, it does not involve the collection of any data or information other than tables of numbers—listing which phone numbers have called what other numbers, as well as the date and time and duration of the calls.[15] This information is termed "metadata" because it includes only transactional data about communications, not any information about the substance of the communications themselves.[16] This data is collected by the telephone companies in the ordinary course of business for billing purposes and kept in their databases for a period of months. Each company has its own database of calling records for its own subscribers.

---

10. *Myth vs. Fact on FISA Collection*, U.S. HOUSE OF REPRESENTATIVES PERMANENT SELECT COMM. ON INTELLIGENCE, http://intelligence.house.gov/myth-vs-fact-fisa-collection [http://perma.cc/HN9Y-U5GG] (last visited Aug. 1, 2014).

11. *Id.*

12. *Id.*

13. *Id.*

14. *Id.*

15. *Id.*

16. *Id.*

The NSA's telephone metadata collection is authorized by an order from the Foreign Intelligence Surveillance Act ("FISA") court.[17] The FISA court has reauthorized the order every ninety days since 2006. Under this order, the NSA collects the metadata in bulk from multiple phone companies, aggregates the data together into a single database, and converts the data into a common, efficiently-searchable format. The database is kept segregated and is used only for counterterrorism investigations. Under the court's order, the NSA is permitted to access the database only when it has reasonable suspicion that a particular phone number is associated with a foreign terrorist organization, and then the NSA may only use that specific phone number to "query" the database—essentially asking the database what incoming and outgoing calls have been made to and from the suspicious phone number. The output of those queries is simply a list of those particular phone numbers that have been in contact with the suspicious number. Under the court's orders in the past, the NSA was then permitted to conduct follow-up queries two or three "hops" out from the original suspicious number, or "seed number." Earlier this year, President Obama directed the NSA to stop following the connections out to the third hop,[18] so now the NSA is limited to reviewing suspicious connections only up to two hops from the seed number.

The purpose of this metadata program is to enable FBI investigators to discover new phone numbers—numbers the FBI was not aware of before—that may be associated with a terrorist cell operating inside the United States. Of course, phone numbers within the U.S. that may be in communication with known foreign terrorist organizations outside the U.S. are among the most important numbers to identify for national security purposes. If the NSA discovers such a number from this program, the NSA will "tip" the number to the FBI for follow-up investigation. If the FBI investigates the person or persons associated with the new number and discovers further suspicious information, at a certain point in the investigation, the FBI may develop sufficient

17. *See* 50 U.S.C. § 1861 (2012).

18. *See* Press Release, The White House, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [http://perma.cc/38MX-ARH2].

probable cause of terrorist-related activity to obtain a wiretap warrant or a search warrant from a federal judge, including potentially from a FISA court judge.[19] The further investigation may lead to evidence that could support an arrest.

That is the way that counterterrorism investigations, just like other law enforcement investigations, generally develop. One discovery may lead to probable cause for a wiretap and eventually for an arrest. The "search" standard of the Fourth Amendment is flexible and enables law enforcement organizations or intelligence agencies to put together the building blocks of an investigation that may lead to probable cause for an eventual arrest.

In applying the Fourth Amendment's concept of a "search," there is a logical and critical difference between transactional records—or metadata—and the content of communications. The Supreme Court has held that a customer of a telephone company does not have a reasonable expectation of privacy in the sort of calling records involved in the NSA's metadata collection,[20] which are transactional records generated by the companies for their own business purposes in the course of providing services.[21] They are similar in this respect to the records generated by a bank when a check is cashed, or the records generated by a merchant when a customer charges a purchase to a credit card.[22] These are all business records of transactions and are not private records that the customer controls or in which the customer maintains a reasonable expectation of privacy.[23] In the case of telephone metadata, that is principally because the records are generated for and used by the phone companies in the course of operating their businesses, and they do not reveal the content of any customer's private communication.[24]

Similarly, government agencies, including both law enforcement departments and regulatory agencies conducting regulatory investigations, act consistently with the demands of

---

19. *See* 50 U.S.C. § 1805 (2012).

20. *See* Smith v. Maryland, 442 U.S. 735, 742–44 (1979).

21. Myth vs. Fact on FISA Collection, *supra* note 10.

22. *See* United States v. Miller, 425 U.S. 435, 437 (1976) (finding no reasonable expectation of privacy in bank records under the Fourth Amendment).

23. *Smith*, 442 U.S. at 742–44.

24. Myth vs. Fact on FISA Collection, *supra* note 10.

the Fourth Amendment when they obtain business records that are relevant to an authorized investigation through the use of subpoenas, often without any court involvement.[25] This standard of "relevance" is the same standard that regulatory agencies rely on to obtain business records with administrative subpoenas or civil investigatory demands,[26] which are not approved by any court.[27] The standard is no different from that used by grand juries to subpoena documents and other records that the grand jury believes may be relevant to whether a crime has or has not been committed.[28] Grand jury subpoenas also do not require court approval. The important difference for the NSA is that its authority comes from the Foreign Intelligence Surveillance Act (FISA), and under FISA, the NSA is required to get court approval in the form of a court order authorizing the collection of the business records, and that is what the NSA does to collect the telephone metadata.

Some have argued that the NSA must or should obtain a search warrant supported by probable cause before obtaining such metadata business records.[29] The Fourth Amendment, however, does not require a search warrant in these circumstances,[30] and a probable cause requirement would be wholly unworkable for this type of program. The point of the metadata collection is to discover the initial building blocks of information to support a follow-up investigation that may eventually lead to the development of probable cause. The probable cause sufficient to support a wiretap or search warrant often only comes from following up on an ini-

---

25. *Id.*

26. Graham Hughes, *Administrative Subpoenas and the Grand Jury: Converging Streams of Criminal and Civil Compulsory Process*, 47 VAND. L. REV. 573, 587 (1994) (civil investigation demands "almost exactly mirror[] the standards for challenging a grand jury subpoena" as does obtaining an administrative subpoena).

27. *See id.* at 589.

28. *See* United States v. R. Enterprises, Inc., 498 U.S. 292, 297 (1991) (holding grand jury subpoenas do not require probable cause).

29. *See, e.g.*, Randy Barnett, *Why the NSA Data Seizures Are Unconstitutional*, 38 HARV. J.L. & PUB. POL'Y 3 (2015).

30. *See* Smith v. Maryland, 442 U.S. 735 (1979) (holding that there is no reasonable expectation of privacy in metadata); Orin Kerr, *Metadata, the NSA, and the Fourth Amendment: A Constitutional Analysis of Collecting and Querying Call Records Databases*, VOLOKH CONSPIRACY (July 17, 2014, 3:54 AM), http://www.volokh.com/2013/07/17/metadata-the-nsa-and-the-fourth-amendment-a-constitutional-analysis-of-collecting-and-querying-call-records-databases/ [http://perma.cc/5FGR-JFML].

tial "tip" generated by the review of transactional records, and that is precisely how this program is intended to contribute to counterterrorism investigations.

Responding to public opposition to the NSA's telephone metadata program, Congress is currently considering legislation that would prohibit the collection of bulk metadata under FISA. In my view, such a restriction is a bad idea. Under this legislation, the NSA would be unable to collect data from multiple companies where necessary to assemble a single, efficiently searchable database.[31] This restriction would also mean that the NSA would be prevented from collecting and storing data in bulk where doing so is the only way to preserve important business records that may be useful for a counterterrorism investigation.[32] Without the ability for U.S. intelligence agencies to acquire the data in bulk under FISA, these important business records would only exist for as long as the private companies happen to retain the data for their own business purposes or as required by regulatory agencies for reasons unrelated to national security.[33] For example, telephone companies typically retain their metadata calling records for only 18 months, as specified by the Federal Communications Commission for purposes of resolving customer billing disputes.[34] Under its metadata program, on the other hand, the NSA was storing the data for five years, so that it could conduct more extensive historical analyses of calling connections involving suspected terrorist numbers—historical analyses that can often provide very important new leads for FBI investigations.

The second NSA program revealed by Snowden is the so-called "section 702" program. Unlike the metadata program, this second program does involve content collection, but this collection is focused on international communications. The 702 collection is conducted under an amendment to the Foreign Intelligence Surveillance Act that Congress passed in 2008. The program, as it exists today, is the successor of sorts to the war-

---

31. Dan Roberts, *The USA Freedom Act: a look at the key points of the draft bill*, THE GUARDIAN, Oct. 10, 2013, http://www.theguardian.com/world/2013/oct/10/the-usa-freedom-act-a-look-at-the-key-points-of-the-draft-bill [http://perma.cc/P8XT-F9Z6].

32. *Id.*

33. USA Freedom Act, H.R. 3361, 113th Cong. (2014).

34. *See* 47 C.F.R. § 42.6 (2014).

rantless surveillance program that President Bush initiated after September 11. Collections under the 702 program are "searches" under the Fourth Amendment because they do involve content. And these searches even involve reviewing private communications of Americans who may be party to an international call or email with someone outside the U.S. who is the target of the surveillance.

The critical point for Fourth Amendment purposes, however, is that this surveillance is focused on foreign intelligence and on international communications. The 702 program is designed to target the international communications of "non-U.S. persons"—meaning neither U.S. citizens nor lawful permanent U.S. residents—who are reasonably believed to be located outside the U.S. when the surveillance occurs.[35] These foreigners—and their international communications—are "searched" under the 702 program within the meaning of the Fourth Amendment, but the courts of appeals have been consistent in holding that such foreign intelligence searches targeted at foreign threats to the U.S., rather than domestic U.S. security threats, do not require a traditional search warrant under the Fourth Amendment in order to justify the search as "reasonable."[36] In other words, a foreign intelligence search targeted at non-U.S. security threats, even one conducted on telephone lines or email connections inside the United States, may be "reasonable" in satisfaction of the Fourth Amendment without the need to obtain a court-approved search warrant supported by a traditional probable cause determination.

In fact, consistent with the conclusion that no warrant is required, this entire category of foreign-targeted international communications intelligence gathering was originally intended by Congress to be completely excluded from FISA when the statute was enacted in 1978. FISA was originally designed so that such surveillance would not require any approval from the FISA court at all. Indeed, prior to enactment of FISA, such foreign intelligence surveillance occurred under the Ar-

35. *See* 50 U.S.C. § 1802 (2012).

36. *See* United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075–76 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987).

ticle II constitutional authority of the President without any court involvement.

Over time, however, in the decades following the enactment of FISA, communications technology changed, and, as a result, the surveillance of most international communications came to require a FISA order, even though Congress had not intended that result. The executive branch tolerated the requirement to go through the motions of obtaining FISA court approval for each individual surveillance operation right up until September 11. But with the attacks of September 11 and the fear of further imminent attacks on the U.S. homeland, the impediments created by the cumbersome FISA process[37] became a serious problem. The President's and the intelligence community's attention was trained on detecting potential follow-on terrorist plots through broader and more nimble surveillance of the international communications of identified terrorist suspects than would be feasible under traditional FISA procedures as they existed at that time.[38] It was for that reason that President Bush authorized the NSA to initiate the extraordinary "warrantless" surveillance program.

Eventually, at the end of 2005, *The New York Times* reported on the existence of this warrantless surveillance program, and that disclosure precipitated controversy and a heated public and political debate, including on Capitol Hill. What was the ultimate outcome of this debate? President Bush was not impeached for circumventing FISA (as Al Gore had urged[39]), and no one who carried out his orders was prosecuted. Instead, Congress effectively approved and ratified the President's surveillance pro-

---

37. Richard Henry Seamon & William Dylan Gardner, *The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement*, 28 HARV. J.L. & PUB POL'Y 319, 376–77 (2005).

38. *See* PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 3–4 (2014), http://www.pclob.gov/All%20Documents/Report%20on%20the%20Section%20702%20Program/PCLOB-Section-702-Report-PRE-RELEASE.pdf [http://perma.cc/GF3B-W7PR] [hereinafter 702 Report].

39. Teddy Davis, *Gore Says Bush Wiretapping Could Be Impeachable Offense*, ABC NEWS (Jan. 16, 2006), http://abcnews.go.com/US/story?id=1511599 [http://perma.cc/5XDX-ANKW].

gram.[40] Congress and the executive branch ultimately came together and enacted new legislation reforming or modulating the FISA procedures to permit the executive branch to continue implementing a broad and nimble program of foreign-targeted intelligence surveillance of international communications coming into or going out of the U.S.[41] Section 702 of FISA is the current embodiment of that policy.[42]

The five-member, Senate-confirmed Privacy and Civil Liberties Oversight Board recently completed a review of the current section 702 program and unanimously concluded that the program is constitutional and is fully consistent with the requirements of the statute enacted by Congress.[43]

The story of the 702 program provides powerful validation of the Constitution's brilliant balance of the twin imperatives of preserving individual privacy and protecting national security. It is a story of decisive presidential action in the face of an extreme foreign threat to the United States followed by healthy public debate and legislative action by Congress to modify the FISA law in fundamental respects so as to accommodate and enable the type of foreign intelligence surveillance the executive branch deemed critical for national defense.

I believe the Constitution bequeathed to us by the Founders encourages and permits the two political branches to come together in this fashion to craft a reasonable and workable framework for protecting the nation from external threats while staying true to our Fourth Amendment principles. I also strongly believe that history will judge the 702 story as a compelling example of how our constitutional structure enables us to meet the greatest national challenges while preserving and protecting the most fundamental liberties we cherish and whose preservation and fulfillment are the true purposes of our federal government.

---

40. Eric Lichtblau, *Deal Reached in Congress to Rewrite Rules on Wiretapping*, N.Y. TIMES, June 20, 2008, http://www.nytimes.com/2008/06/20/washington/20fisacnd.html?_r=0 [http://perma.cc/8DY-VLUP].

41. *Id.*

42. *See* 702 Report, *supra* note 38, at 19–20.

43. *Id.* at 15.