THE LEGALITY OF THE NATIONAL SECURITY AGENCY'S BULK DATA SURVEILLANCE PROGRAMS

JOHN YOO*

INTRODUCTION

Controversy has arisen again over the federal government's electronic surveillance efforts to gather intelligence on foreign terrorist groups. Recent disclosures, both authorized and illicit, have described two secret National Security Agency (NSA) programs. The first collects telephone "metadata" such as calling records—but not the content of phone calls—both inside and outside the United States. A second NSA program intercepts the e-mails of non-U.S. persons outside the United States.[1] Despite the claims of critics, these programs do not violate the Foreign Intelligence Surveillance Act (FISA), as recently amended by Congress, or the Fourth Amendment to the Constitution. Concerns about the proper balance between these surveillance programs and individual privacy may be appropriate, but these programs properly fall within the province of Congress and the President to set future national security policy.

Legal questions over surveillance arise from the unconventional nature of the war against al Qaeda. On September 11, 2001, the al Qaeda terrorist network launched attacks on New

---

* Emanuel S. Heller Professor of Law, University of California, Berkeley Law School; Visiting Scholar, American Enterprise Institute. I thank Steven Erkel and Lianna Bash for research assistance.

1. *See, e.g.*, NAT'L SEC. AGENCY, THE NATIONAL SECURITY AGENCY: MISSIONS, AUTHORITIES, OVERSIGHT AND PARTNERSHIPS (2013); President Barack Obama, White House Press Conference (Aug. 9, 2013), http://www.whitehouse.gov/photos-and-video/video/2013/08/09/president-obama-holds-press-conference, [http://perma.cc/0Uior8KK6xE]. An up-to-date catalogue of the declassified documents is available online, *DNI Declassifies Intelligence Community Documents Regarding Collection Under Section 702 of the Foreign Intelligence Surveillance Act*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, http://www.odni.gov/index.php/newsroom/press-releases/191-press-releases-2013/915-dni-declassifies-intelligence-community-documents-regarding-collection-under-section-702-of-the-foreign-intelligence-surveillance-act-fisa, [http://perma.cc/0d89r1gAgxj].

York City and Washington, D.C. from territory in Afghanistan substantially under its control. Under normal circumstances, American military and intelligence officers, acting pursuant to the President's Commander-in-Chief authority, would carry out electronic surveillance against a foreign enemy in wartime. Al Qaeda, however, operates through teams of covert agents who disguise their communications and movements within normal peaceful activities. American law subjects domestic criminal enterprises, which operate in similar ways, to the more elaborate system of search warrants, individualized suspicion, and judicial supervision required by the Fourth Amendment. Controversy over the legality of the NSA's programs basically centers on whether surveillance of al Qaeda should follow the wartime foreign intelligence model or the criminal justice approach.

This paper will address the legality of the NSA's programs in this light. Part I will describe the surveillance efforts against al Qaeda within a broader historical and legal context. Part II will argue that the programs, as described publicly by authoritative sources, appear to meet statutory requirements. Part III will address whether the NSA programs are constitutional along two dimensions. First, it will argue that even if some aspect of the NSA programs does not fall within Congress's authorization for foreign intelligence and counterterrorism surveillance, it would most likely rest within the President's Commander-in-Chief authority over the management of war. Second, even if the federal government has the internal authority to conduct surveillance, the Bill of Rights, through the Fourth Amendment, may still prohibit its application to citizens or non-citizens present in the territorial United States. This Article will argue, however, that the NSA programs do not violate the Fourth Amendment as currently interpreted by the federal courts.

I. HISTORICAL AND LEGAL CONTEXT

On September 11, 2001, the al Qaeda network launched four coordinated attacks aimed at critical buildings in the heart of the nation's capital and financial system. Nineteen terrorists hijacked four civilian passenger airliners and crashed them into the World Trade Center towers in New York City and the Pentagon outside Washington, D.C. Another flight, apparently

destined for the Capitol or the White House, crashed in Pennsylvania after passengers fought to seize back control of the plane. The attacks killed about 3,000 people, with many more injured, caused billions of dollars in physical damage, and caused further economic loss through disruptions in transportation, communications, and the financial markets. If a nation-state, such as the Soviet Union during the Cold War, had carried out identical strikes, there would be little doubt that the United States would be at war.

These attacks, however, differed significantly from normal attacks in conventional wars. The enemy's soldiers did not wear uniforms, did not carry arms openly, and did not operate as part of regular military units. Mohammed Atta and his eighteen agents disguised themselves as civilians for travel and training, used civilian aircraft as weapons, and launched the attacks by surprise from within U.S. borders. Al Qaeda itself cannot lay claim to the status of a nation. In 2001, it exercised no territorial sovereignty, had no population, and fielded no regular armed forces. Rather, al Qaeda takes the form of a decentralized network of extremists who wish to engineer fundamentalist political and social change in Islamic countries. Its terrorist cells operate both abroad and within the United States.

It is al Qaeda's nature as a decentralized network that stresses the normal division between military and intelligence surveillance and the warrant-based approach of the criminal justice system. The Constitution vests the President with the executive power and designates him Commander-in-Chief.[2] The Framers understood these powers to invest the executive with the duty to protect the nation from foreign attack and the right to control the conduct of military hostilities.[3] To exercise those powers effectively, the President must have the ability to engage in electronic surveillance that gathers intelligence on the enemy. Regular military intelligence need not follow standards of probable cause for a warrant or reasonableness for a

2. U.S. CONST. art. II, § 2, cl. 1.

3. *See* THE FEDERALIST NO. 70, at 423 (Alexander Hamilton) (Clinton Rossiter ed., 1961) ("Energy in the executive . . . is essential to the protection of the community against foreign attacks . . . ."); THE FEDERALIST NO. 74, at 447 (Alexander Hamilton) ("Of all the cares or concerns of government, the direction of war most peculiarly demands those qualities which distinguish the exercise of power by a single hand."); JOHN YOO, THE POWERS OF WAR AND PEACE: THE CONSTITUTION AND FOREIGN AFFAIRS AFTER 9/11 143–81 (2005).

search, just as the use of force against the enemy does not have to comply with the Fourth Amendment. During war, military signals intelligence might throw out a broad net to capture all communications within a certain area or by an enemy nation. Unlike the criminal justice system, which seeks to detain criminals, protection of national security need not rest on particularized suspicion of a specific individual.

This approach applies to national security activity that occurs within the United States as well as outside it. In 1972, the Supreme Court refused to subject surveillance for national security purposes to the Fourth Amendment warrant requirement.[4] But it has extended this protection to purely domestic terrorist groups, out of concern that the government might use its powers to suppress political liberties.[5] Lower courts, however, have found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement. In a leading 1980 case, the Fourth Circuit held that "the needs of the executive are so compelling in the area of foreign intelligence, unlike the area of domestic security, that a uniform warrant requirement would . . . unduly frustrate the President in carrying out his foreign affairs responsibilities."[6] A warrant requirement for national security searches would reduce the flexibility of the executive branch, which possesses "unparalleled expertise to make the decision whether to conduct foreign intelligence surveillance" and is "constitutionally designated as the pre-eminent authority in foreign affairs."[7] A warrant requirement would place national security decisions in the hands of the judiciary, which "is largely inexperienced in making the delicate and complex decisions that lie behind foreign intelligence surveillance."[8]

Under this framework, Presidents conducted national security surveillance using their executive authority for decades. President Nixon's abuses, however, led Congress to enact the Foreign

4. United States v. U.S. District Court, 407 U.S. 297, 321–24 (1972).

5. *Id.* at 321.

6. United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980) (internal quotation marks omitted).

7. *Id.* at 913–14.

8. *Id.* at 913.

Intelligence Surveillance Act (FISA) in 1978.[9] FISA replaced presidentially-ordered monitoring of national security threats with a system similar to that used by law enforcement to conduct electronic surveillance of criminal suspects, but with important differences to protect classified information. FISA requires the government to show "probable cause" that a target is "an agent of a foreign power," which includes terrorist groups.[10] A special court of federal district judges, the Foreign Intelligence Surveillance Court (FISC), examines classified information in a closed, ex parte hearing before issuing the warrant.[11]

FISA obviously strikes a compromise between the wartime and criminal approaches to information gathering. It establishes a system that bears strong resemblances to the criminal justice system, such as the requirement of an individual target, probable cause, and a warrant issued by a federal court. On the other hand, in a nod to the purposes of foreign intelligence surveillance, it does not require a showing of probable cause of criminal activity by the target, which the Fourth Amendment normally requires for a search warrant.[12] Instead, FISA only demands that the government show "probable cause" that the target is linked to a foreign power or terrorist group.

Opponents of the NSA's bulk data collection programs argue that FISA cannot authorize bulk data collection because it was structured as a protection against invasive government searches.[13] This rationale holds that FISA's "general approach" requires a degree of individualized suspicion when conducting a search.[14] This "general approach" argument rests upon FISA's requirements that electronic information be linked to a specific target, known to be a foreign power or agent thereof, and that the government show probable cause that the target is a foreign power or agent thereof.[15] Furthermore, opponents argue that the FISC was specifically created to prevent the government from

9. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. §§ 1801–1855c (2006)).

10. 50 U.S.C. § 1805(a)(2).

11. *See id.* § 1805.

12. *See, e.g.*, Illinois v. Gates, 462 U.S. 213, 217 (1983).

13. *See, e.g.*, Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 766–806 (2014).

14. *Id.* at 766–67, 782–91.

15. *Id.*

going too far in its searches, reinforcing FISA's general approach of protecting against invasive government surveillance.[16]

As explained above, FISA does not reflect a general attitude against government surveillance; rather, it creates a balance between the criminal system's restrictions on government searches and the broader acceptance of information-gathering during wartime. Although FISA does lay out a probable cause requirement, that requirement is more in line with wartime information gathering than with evidence gathering in the criminal system. And, although the FISC does check the government's ability to conduct surveillance, it only does so shrouded in complete confidentiality—reflecting the wartime, rather than criminal, system of information gathering. This blend of the criminal and wartime information gathering schemes negates the assertion that FISA broadly protects against government surveillance. Although FISA's criminal components restrict government searches, the wartime components recognize the government's need to engage in robust information gathering during times of conflict.

The Patriot Act of 2001 made important changes to FISA that bear directly on the legality of the NSA surveillance programs. Section 215 of the Patriot Act allows the government to seek an order from the FISC to require a private party to produce "tangible things," which includes "books, records, papers, documents, and other items."[17] The government can obtain the records for two purposes: either for "an investigation to obtain foreign intelligence information not concerning a United States person" or "to protect against international terrorism or clandestine intelligence activities," so long as it does not infringe on First Amendment-protected activity.[18] To obtain the order, the government must show that "there are reasonable grounds to believe" that the records are "relevant" to "an authorized investigation."[19] Information sought is presumptively relevant to an authorized investigation if the records are related to "the

16. *Id.* at 763–64.

17. USA Patriot Act of 2001, Pub. L. No. 107-56, § 215, 115 Stat. 272, 287 (codified at 50 U.S.C. § 1861 (2006)).

18. 50 U.S.C. § 1861(a)(1).

19. *Id.* § 1861(b)(2)(A).

activities of a suspected agent of a foreign power" or someone in contact with such an agent.[20]

Section 215 does not contain a revolutionary grant of authority to the government. It authorizes something akin to a grand jury subpoena for financial, communication, or travel records as part of a criminal investigation. In fact, the statute additionally defines the records as those that can be obtained by a subpoena issued by a federal court as part of a grand jury investigation.[21] Section 215 of the Patriot Act provides the authority for the NSA's collection of telephone billing records. The NSA collects the data containing the phone numbers on both ends of a call and the duration of every call made in the United States.[22] But it does not intercept the content of the call, nor does it know the identity of the subscriber.[23] It collects the information into a database of all calls in the nation, which did not exist previously because multiple telecommunications companies would delete their records.[24] The NSA purges records that are more than five years old.[25] A database allows the NSA to determine quickly the calling chain of any overseas numbers discovered to belong to al Qaeda operatives. Once the NSA tracks down the phone numbers called within the United States from a suspected al Qaeda phone number, it can then seek a warrant from the FISC to place the number under further surveillance and to collect other records, such as financial and travel information.

II. STATUTORY AUTHORITY FOR THE NSA PROGRAMS

A. Phone Call Metadata Collection

Like business records, phone call metadata falls within Section 215's definition of tangible items. Collection of such metadata relates to an authorized investigation to protect against international terrorism. Several investigations into al Qaeda plots remain open, as shown by the repeated indict-

20. *Id.* § 1861(b)(2)(A)(ii).

21. *Id.* § 1861(c)(2)(D).

22. Steven G. Bradbury, *Understanding the NSA Programs: Bulk Acquisition of Telephone Metadata Under Section 215 and Foreign-Targeted Collection Under Section 702*, LAWFARE RES. PAP. SER. Sept. 1, 2013, at 2.

23. *Id.*

24. *Id.*

25. *Id.* at 3.

ments against bomb plotters in the last five years. The examination of records also helps protect the nation against terrorist attacks. According to the NSA, only the information contained in the billing records is collected; the content of calls is not.[26] There can be no First Amendment violation if the content of the calls remains untouched. A critic might argue that the terms of the search are too broad because ninety-nine percent of the calls are unconnected to terrorism. But an intelligence search, as Judge Richard Posner has described it, "is a search for the needle in a haystack."[27] Rather than focus on foreign agents who are already known, counterterrorism agencies must search for clues among millions of potentially innocent connections, communications, and links. "The intelligence services," Posner writes, "must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented."[28] For this reason, the FISC approved the NSA program in 2006 and has continued to renew it since.[29]

Members of the al Qaeda network can be detected, with good intelligence work or luck, by examining phone and e-mail communications, as well as evidence of joint travel, shared assets, common histories or families, meetings, and so on.[30] As the time for an attack nears, "chatter" on this network will increase as operatives communicate to coordinate plans, move and position assets, and conduct reconnaissance of targets.[31] When our intelligence agents successfully locate or capture an al Qaeda member, they must be able to move quickly to follow new information to other operatives before news of the capture causes them to disappear. The NSA database is particularly

---

26. Report by the Department of Justice on the National Security Agency's Bulk Data Collection Programs Affected by USA PATRIOT Act Reauthorization 3 (Dec. 14, 2009), *available at* https://www.fas.org/irp/news/2013/07/2009_bulk.pdf, [http://perma.cc/NH79-W4R6].

27. Richard A. Posner, *A New Surveillance Act*, WALL ST. J., Feb. 15, 2006, at A16, *available at* http://online.wsj.com/news/articles/SB113996743590074183, [http://perma.cc/0KHARXyijnr]. *See generally* Richard A. Posner, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 (2005).

28. Posner, *A New Surveillance Act*, *supra* note 27.

29. Bradbury, *supra* note 22, at 2.

30. *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 47, 361–98 (2004) [hereinafter 9/11 COMMISSION REPORT]; *id.* at 227 n.68 (noting that the United Arab Emirates was able to track Marwan al Shehhi, one of the future 9/11 hijackers, when he contacted his family).

31. *See id.* at 263–65.

important because it will point the way to al Qaeda agents within the United States, where they are closest to their targets and able to inflict the most harm on civilians.

The September 11 hijackers themselves provide an example of the way that the NSA could use business record information to locate an al Qaeda cell. Links suggested by commercially available data might have turned up ties between every single one of the al Qaeda plotters and Khalid al Mihdhar and Nawar al Hazmi, the two hijackers known to the CIA to have been in the country in the summer of 2001.[32] Mihdhar and Hazmi had rented apartments in their own names and were listed in the San Diego phone book.[33] Both Mohammad Atta, the leader of the September 11 al Qaeda cell, and Marwan al-Shehi, who piloted one of the planes into the World Trade Center, had lived there with them.[34] Hijacker Majed Moqed used the same frequent flier number as Mihdhar; five hijackers used the same phone number as Atta when booking their flights; the remaining hijackers shared addresses or phone numbers with one of those hijackers, Ahmed Alghamdi, who was in the United States in violation of his visa at the time.[35]

Our intelligence agents, in fact, had strong leads that could conceivably have led them to all of the hijackers before 9/11.[36] CIA agents had identified Mihdhar as a likely al Qaeda operative because he was spotted at a meeting in Kuala Lumpur and mentioned in Middle East intercepts as part of an al Qaeda "cadre."[37] Hazmi too was known as likely to be al Qaeda.[38] But in neither case was there enough evidence for a criminal arrest because they had not violated any American laws. If our intelligence services had been able to track immediately their cell phone calls and e-mail, it is possible that enough of the hijacking team could have been rounded up to avert 9/11.[39] Our task is much more difficult today, because we might not have even

---

32. Heather MacDonald, *What We Don't Know* Can *Hurt Us*, CITY JOURNAL, Spring 2004, http://www.city-journal.org/html/14_2_what_we_dont_know.html, [http://perma.cc/0p9HZgCszyo].

33. *Id.*

34. *Id.*

35. *Id.*

36. *Id.*

37. 9/11 COMMISSION REPORT, *supra* note 30, at 158, 181.

38. *See id.* at 158–59, 181–82.

39. *Id.* at 272.

this slender information in hand when the next al Qaeda plot moves toward execution.

As the United States fought the Afghanistan and Iraq wars, and as it has continued to pursue al Qaeda groups in the Middle East and Africa, it has captured al Qaeda laptops, cell phones, financial documents, and other instruments of modern high-tech life. This has given intelligence officers information on dozens or hundreds of e-mail addresses, telephone numbers, bank and credit account numbers, and residential and office addresses used by al Qaeda networks.[40] To exploit this, U.S. intelligence services must follow those leads as fast as possible, before the network of al Qaeda operatives can migrate to a new leader. An e-mail lead can disappear as quickly as it takes someone to open a new e-mail account.

FISA and the law enforcement mentality it embodies create several problems. FISA requires "probable cause" to believe that someone is an agent of a foreign power before one can get a warrant to collect phone calls and e-mails.[41] An al Qaeda leader could have a cell phone with 100 numbers in its memory, ten of which are in the United States and thus require a warrant. Would a FISA judge have found probable cause to think the users of those ten numbers are al Qaeda too? Probably not. Would our intelligence agencies even immediately know who was using those numbers at the time of the captured al Qaeda leader's calls? The same question can be asked of his e-mail, as it will not be immediately obvious which addresses in his inbox are held by U.S. residents.

In our world of rapidly shifting e-mail addresses, multiple cell phone numbers, and internet communications, FISA imposes slow and cumbersome procedures on our intelligence and law enforcement officers.[42] These laborious checks are based on the

---

40. *See, e.g.*, *id.* at 382.

41. 50 U.S.C. § 1805(a)(2) (2006).

42. *See* Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 825 (1989), reasoning that:

> FISA also must keep pace with the continuing explosion in communications technologies available both to law enforcement agencies and potential surveillance targets. FISA was drafted to take account of experience and technology developed between 1968 and 1978, but the decade since its passage has witnessed substantial technological changes that could require amendments to FISA in order to extend its privacy

assumption that we remain within the criminal justice system, which looks backward at crimes in order to conduct prosecutions, rather than within the national security system, which looks forward in order to prevent attacks on the American people.[43] FISA requires a lengthy review process, in which special FBI and DOJ lawyers prepare an extensive package of facts and law to present to the FISC.[44] The Attorney General must personally sign the application, and another high-ranking national security officer, such as the President's National Security Advisor or the Director of the FBI, must certify that the information sought is for foreign intelligence.[45] Only a quickly searchable database of numbers will allow the government to take advantage of captured al Qaeda numbers abroad, before the cells within the United States break their contacts.

A critic, however, might argue that billions of innocent calling records are not "relevant" to a terrorism investigation.[46] Even if terrorist communications take place over the phone, that cannot justify the collection of all phone call records in the United States, the vast majority of which have nothing to do with the grounds for the search. The FISC rejected this argument because, to be useful, a database has to be broad enough to find terrorist calls. "Because known and unknown international terrorist operatives are using telephone communications, and because it is necessary to obtain the bulk collection of a telephone company's metadata to determine those connections between known and unknown international terrorist operatives as part of authorized investigations," the Court observed, "the production of the information sought meets the standard for relevance under Section 215."[47] Aggregating calling records

---

protections and to facilitate legitimate government interests that might otherwise be frustrated.

43. *See* JOHN YOO, WAR BY OTHER MEANS: AN INSIDER'S ACCOUNT OF THE WAR ON TERROR 71–74, 79–80 (2006) (noting that an artificial "Wall" in place for decades between information gathered for intelligence and information gathered for law enforcement purposes hindered the government's ability to piece together intelligence which could have stopped the 9/11 attacks).

44. *See* 50 U.S.C. § 1804 (2006).

45. *Id.* § 1804(a).

46. *See, e.g.*, Klayman v. Obama, 957 F. Supp. 2d 1, 41 (D.D.C. 2013) (holding that the potential impact that bulk metadata collection could have on the plaintiff's privacy rights likely outweighed the government's interest in terrorism prevention).

47. *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things From [Redacted] at 18, BR 13-109 (FISA Ct.

into a database, the court found, was necessary to find the terrorist communications and the links between terrorists.[48] It may not even be possible to detect the links unless such a database is created. If a database is not comprehensive, in other words, then the government will only be able to glimpse incomplete patterns of terrorist activity, if it can glimpse any at all.

Relevance is a slippery concept, but it cannot require that every piece of information obtained by subpoena must contain information related to guilt. Even when grand juries subpoena the business records or communications of a criminal suspect, it is likely that the large majority of the items will not have any relationship to the crime. Nonetheless, a grand jury may subpoena all of a suspect's financial records to find those that pertain to a criminal conspiracy. A different way to view the NSA's telephone calling record program is that the "relevant" tangible "thing" is the database itself, rather than any individual calling record.

Of course, the NSA program differs from a subpoena to a financial institution for the records of a known criminal suspect. The amount of data collected by the NSA program is many orders of magnitude greater, and hence the percentage of directly involved communications much smaller. Also, unlike a regular subpoena, it is important to have as large a searchable database as possible because the breadth will bring into the sharpest contrast the possible patterns of terrorist activity. On the other hand, the magnitude of harm that the government seeks to prevent exceeds by several orders that of regular crime. The magnitude of the harm should be taken into account in judging relevance as well as the unprecedented difficulties of locating al Qaeda operatives disguised within the United States.

B. Electronic Communications Data Collection

The NSA's second surveillance program, which targets internet communications involving foreigners, poses different legal challenges. But a careful review shows that it does not violate statutory or constitutional law, although the program's facts remain somewhat unclear. According to reports, in addi-

---

Aug. 29, 2013), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf, [http://perma.cc/Y3YZ-YMBY].

48. *Id.*

tion to the collection of telephone call metadata, the NSA also intercepts electronic communications—presumably e-mails—by foreigners outside the United States.[49] Apparently, this program also depends on the collection and storage of vast amounts of data, gained either by request from internet service providers (ISPs) or from the internet backbone networks themselves.[50] According to its own public description of the program in August 2013, the NSA generates "identifiers" of non-U.S. persons outside the country whom it believes "possess, communicate, or are likely to receive foreign intelligence information authorized for collection under an approved certification."[51] The government uses these "identifiers," which take the form of e-mail addresses and phone numbers, to acquire selected communications.[52]

The NSA's program falls precisely within FISA as currently written. Congress specifically amended the statute, at first temporarily in 2007 and then permanently in 2008, to authorize this exact program.[53] It most recently renewed this authority, codified in section 702 of FISA, in 2012.[54] Section 702 allows the government to target for surveillance a non-U.S. person reasonably believed to be outside the United States for up to one year. Congress specifically limited the reach of the statute in four ways. Surveillance may not:

1. Intentionally target anyone known to be inside the United States
2. Seek to reverse target a person believed to be in the United States through their contacts with individuals outside the United States
3. Intentionally target any U.S. person

---

49. NAT'L SEC. AGENCY, *supra* note 1, at 4.

50. *Id.*

51. *Id.*

52. *Id.*

53. *See* Protect America Act of 2007, Pub. L. No. 110-55, § 1, 121 Stat. 552, 552; FISA Amendments Act of 2008, Pub. L. No. 110-261, § 101, 122 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a).

54. FISA Amendments Act of 2012, Pub. L. No. 112-238, § 2, 122 Stat. 2474, 2474 (codified at 50 U.S.C. § 1881a).

4. Intentionally collect any communication where the sender and all receivers are known to be in the United States.[55]

These exclusions leave only one category of communications that the government may collect: the communications of non-U.S. persons believed to be outside the United States. It does not allow the surveillance of wholly domestic communications or those by U.S. persons anywhere in the world. Notice the important omission: the statute is not concerned with where the communications take place, only the locations of the persons engaged in communicating.

Congress's authorization of collection based only on the location of the sender and receiver is important because of the nature of internet communications. When a person sends an e-mail, the internet breaks the message up into packets, sends them through the most efficient network routes possible, and then reassembles them into the message at a point of reception. Depending on network efficiencies, the electronic communications of two people—even if they are in adjacent towns—might traverse any country where network backbones are located, such as the United States. Section 702 simply recognizes that a different set of surveillance authorities should not be triggered simply because part of a message between non-U.S. persons passes through the United States. For example, if a suspected terrorist in Pakistan were to send an e-mail to an address of a person believed to be located in Afghanistan, the NSA could intercept the e-mail even if part or all of the message itself moved through communication networks located in the United States.

With internet communications, however, the government may not easily know the physical location or citizenship of the senders or receivers. An e-mail address, such as yoo@law.berkeley.edu, does not obviously contain geographical location data. Berkeley might refer to a city in California, Australia, Canada, or the United Kingdom, or to the University of California at Berkeley. ISP-based e-mails, such as Gmail, Yahoo, or Hotmail, provide even less hint of a location. The government could look at metadata contained within the e-mail messages themselves, or perhaps at the MAC addresses, which are unique to each computer, to attempt to determine location. But because

55. 50 U.S.C. § 1881a(b).

of this lack of precision, it is inevitable that some unauthorized communications will be collected. As a result, Section 702 requires the FISC to approve the procedures used to develop targets and to minimize the collection of any communications by U.S. persons.[56] If the government seeks to intentionally collect the e-mails of U.S. persons or non-U.S. persons located in the United States, it must still obtain a FISC court order.[57]

This second NSA surveillance program fits cleanly within statutory authorization because Congress amended FISA precisely to permit the program. To be sure, there have been disagreements between the FISC and the NSA over how to implement the program in a manner consistent with Section 702. Examination of the FISC opinions made public, however, indicate that these contests involve minimization procedures where the NSA has intercepted a relatively small number of domestic communications or e-mails by U.S. persons. In October 2011, for example, the FISC criticized an NSA technique of collecting e-mails from "upstream" sources—that is, from the internet backbone itself rather than from ISPs—because it swept in several thousand domestic e-mails out of tens of millions of foreign e-mails.[58] The FISC's opinion did not terminate the program but instead led the NSA to modify its minimization procedures so as to avoid collection of the domestic e-mails.[59] One month later, the FISC approved the new minimization procedures, and the collection program continued.[60] These declassified FISC opinions make clear that judicial resistance to the NSA's program comes not from the legal authority for the electronic surveillance, but from second order concerns over implementation. Concerns about the legality of the program do not arise under FISA or other statutes, but under the Constitution.

---

56. *Id.* § 1881a(g).

57. *Id.* § 1804.

58. FISA Ct. Memorandum Opinion and Order of Oct. 3, 2011, *available at* http://www.odni.gov/files/documents/October%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf, [http://perma.cc/NKM2-RMVH].

59. *Id.*

60. FISA Ct. Memorandum Opinion and Order of Nov. 30, 2011, *available at* http://www.odni.gov/files/documents/November%202011%20Bates%20Opinion%20and%20Order%20Part%201.pdf, [http://perma.cc/7X8J-VQJX].

III. CONSTITUTIONALITY OF THE NSA PROGRAMS

A. Metadata Collection and Third-Party Doctrine

Even if Congress and the President have sufficient statutory authority to carry out the NSA programs, they may still violate the Constitution. A government decision may satisfy the structural provisions of the Constitution—such as the separation of powers and federalism—yet still run afoul of the Bill of Rights. This part measures the two NSA programs against the primary individual right at stake: the Fourth Amendment's protection against unreasonable searches and seizures. It concludes that both the telephone metadata and the foreign e-mail collection programs, as currently described by the Obama administration, do not violate the Fourth Amendment.

The NSA's first program, which collects metadata on domestic phone calls, poses the fewest constitutional difficulties. Under existing judicial doctrine, individuals have Fourth Amendment rights in the content of communications, but not in their addressing information.[61] Privacy does not extend to the writing on the outside of envelopes deposited in the mail because the sender has voluntarily revealed the addresses to the post office for delivery.[62] An identical principle applies to telecommunications. In *Smith v. Maryland*, the Supreme Court found calling information, such as the phone number dialed, beyond Fourth Amendment protection because the consumer had voluntarily turned over the information to a third party—namely, the phone company—for connection and billing purposes.[63] Under the rubric of *Katz v. United States*, no one can have an expectation of privacy in records that they have handed over to someone else.[64]

In recent cases, however, the Court has turned a skeptical eye toward new search technologies. In *Kyllo v. United States*,[65] for example, the Court held that thermal imaging of homes

---

61. *See* Smith v. Maryland, 442 U.S. 735, 744–45 (1979); United States v. Miller, 425 U.S. 435, 443 (1976).

62. *See, e.g.*, Katz v. United States, 389 U.S. 347, 351 (1967) (holding that "[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection").

63. *Smith*, 442 U.S. at 744–45.

64. *Katz*, 389 U.S. at 351.

65. 533 U.S. 27 (2001).

qualified as a search under the Fourth Amendment, even though the police used the imaging device from a public street.[66] In *United States v. Jones*,[67] the Court found that the Fourth Amendment required a warrant for the installation of a global positioning service tracker on a car.[68] These cases turn on the means by which the government conducts a search in a place protected by the Fourth Amendment. In *Kyllo*, the Court believed that thermal imaging verged on a physical search of a home,[69] while *Jones* involved physical intrusion into a private car.[70] Neither holding calls into doubt the loss of Fourth Amendment rights when an individual voluntarily hands over information to a third party. In other words, the information sought by the NSA programs would require a warrant to be searched if it remained within the home or personal computing devices. As a result, the Constitution does not require a warrant for a pen register because no electronic interception or surveillance of the content of the calls has occurred.

Meanwhile, the data collected is potentially of enormous use in frustrating al Qaeda plots. If U.S. agents are pointed to members of an al Qaeda sleeper cell by a domestic phone number found in a captured al Qaeda leader's cell phone, call pattern analysis would allow the NSA quickly to determine the extent of the network and its activities. The NSA, for example, could track the sleeper cell as it periodically changed phone numbers. This could give a quick, initial, database-generated glimpse of the possible size and activity level of the cell in an environment where time is of the essence. A critic might respond that there is a difference between a pen register that captures the phone numbers called by a single person and a database that captures all of the phone numbers called by everyone in the United States. The Supreme Court, however, has never held that obtaining billing records would somehow violate privacy merely because of a large number of such records.

Another Article in this Issue of the *Journal* challenges the constitutionality of the NSA's bulk collection program. In her article, Professor Laura Donohue calls into question the applicability of

66. *Id.* at 41.
67. 132 S. Ct. 945 (2012).
68. *Id.* at 949.
69. *Kyllo*, 533 U.S. at 34–35.
70. *Jones*, 132 S. Ct. at 948.

Smith v. Maryland to the NSA's bulk metadata collection.[71] She argues that the telephone metadata system "is an entirely different situation" from that in *Smith*. In distinguishing *Smith* from the NSA's metadata program, Professor Donohue argues that, unlike the police placing a pen register on a single caller whom the police suspect of criminal behavior, "[t]he NSA is engaging in bulk collection absent any reasonable suspicion that the individuals, whose telephone information is being collected, are engaged in *any* wrongdoing. To the contrary, almost all of the information obtained will bear no relationship whatsoever to criminal activity."[72] In addition to questioning the applicability of *Smith*, Professor Donohue illustrates the recent tensions that have emerged between the Fourth Amendment and the government's ever-increasing use of new technologies. Under the trespass doctrine, Professor Donohue argues that the NSA's metadata collection "amounts to a general warrant—the elimination of which was the aim of the Fourth Amendment."[73] Therefore, as Professor Donohue concludes, the collection of bulk metadata is "a digital trespass on individuals' private spheres."[74]

There are several flaws with Professor Donohue's analysis. Most notably, the *Smith* Court held that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[75] It makes no difference—notwithstanding Professor Donohue's argument—whether the government collects a single suspect's metadata, as in *Smith*, or thousands of callers' metadata, the vast majority of whom are not suspected of any wrongdoing. The point remains the same: individuals lose their expectation of privacy the moment they voluntarily reveal information to third parties. To use the words of Judge Eagan: "[W]here one individual does not have a Fourth Amendment interest, grouping together a large number of similarly-situated individuals cannot result in a Fourth Amendment interest springing into existence *ex nihilo*."[76]

Moreover, though Professor Donohue is correct that tensions have emerged between the Fourth Amendment and the gov-

71. Donohue, *supra* note 13, at 865–71.
72. *Id*. at 869.
73. *Id*. at 765.
74. *Id.*
75. Smith v. Maryland, 442 U.S. 735, 743–44 (1979).
76. *In re* Application of the Federal Bureau of Investigation, *supra* note 47, at 9.

ernment's use of technology, she nevertheless misapplies the trespass doctrine to the NSA's metadata collection. Unlike *Jones*, *Kyllo*, or *Jardines*, the government collection of individuals' metadata does not amount to a trespass or infringe onto their private digital sphere. Indeed, as the Court has emphasized in *Katz* and *Smith*, a digital trespass will not occur when one voluntarily turns his or her information over to third parties to see.

B. The Territorial Reach of the Fourth Amendment

A different Fourth Amendment issue applies to the second NSA program, which intercepts e-mails between foreigners abroad. As the Supreme Court has observed, the Fourth Amendment does not provide rights outside the United States except to citizens or those with sufficient connections to the nation, such as permanent resident aliens. In *United States v. Verdugo-Urquidez*,[77] the Court held that a non-U.S. person could not claim any constitutional rights to bar his capture outside the United States.[78] A critic might respond that the Bill of Rights limits the powers of the government regardless of the citizenship of the individual involved. Tellingly, the Court rejected this argument because it would render impossible the conduct of war against foreign enemies.[79] If all foreigners held Fourth Amendment rights, the Court reasoned, the U.S would be unable to use force against them in wartime without a warrant or a determination of constitutional reasonableness after the fact.[80] Such a rule, the Court reasoned, had never prevailed in American history.[81] So long as the second NSA program collects foreign e-mails between non-U.S. persons, the Fourth Amendment is not implicated.[82]

There is one critical fact about the e-mail intercept program, however, that might trigger the Fourth Amendment. Passage of e-mail packets through switches or network backbones located within the territorial United States might create enough of a nexus with the United States to garner constitutional protections. A court might analogize the legal status of e-mails to an

77. 494 U.S. 259 (1990).
78. *Id.* at 261.
79. *Id.* at 273–74.
80. *See id.*
81. *Id.* at 266–67.
82. *See id.* at 274–75.

air flight that takes off from Canada and lands in Mexico—while the plane flies over the United States, it falls subject to the jurisdiction of the United States.

There are several reasons, however, that this analogy fails. First, packets are not the message themselves, but are pieces of them that are broken apart and reassembled. The message itself is not in a completed form except when it is first written and when it is later reassembled. At those points in time, when the message is actually a unified whole, it is located outside the United States.

Second, finding that any packet that traverses the United States triggers the Bill of Rights would effectively extend constitutional status to all e-mail communications in the world. This is because much of the internet backbone is located in the United States, making the United States central to the operation of the internet and the crossroads for much of the world's digital communication traffic. But if everyone in the world has a constitutional right, then the Constitution has lost its meaning as a framework of government for a single community: "We the People" of the United States.[83] This is a result that the Court in *Verdugo-Urquidez* expressly sought to avoid.

Third, non-U.S. persons communicating outside the U.S. could not possibly have an expectation of privacy under the Fourth Amendment. To be sure, they might think their messages are private because of the difficulty of intercepting internet communications. But they could not think they had any expectation of privacy cognizable under the U.S. Constitution when they were not located within the United States and had no other connections to the nation. Non-U.S. persons outside the territorial U.S. do not have enough connections with the U.S. to benefit from its laws and constitutional protections.

C. The Applicability of the Fourth Amendment to Searches Implicating National Security

Even if constitutional privacy interests were thought to extend to telephone metadata or to foreign e-mails, the Fourth Amendment's warrant requirement still would not apply be-

83. *See* JULIAN KU & JOHN YOO, TAMING GLOBALIZATION: INTERNATIONAL LAW, THE U.S. CONSTITUTION, AND THE NEW WORLD ORDER 47–50 (2012) (explaining the relationship of the Constitution's guiding principle of popular sovereignty with national security and foreign affairs).

cause the NSA searches seek to prevent military attacks, not garden-variety criminal activity.[84] As observed earlier, every lower court to examine the question has found that when the government conducts a search of a foreign power or its agents, it need not meet the requirements that apply to criminal law enforcement. Though, admittedly, the Supreme Court has never ruled on the question, it has suggested in dicta that roadblocks and dragnets to stop a terrorist bombing in an American city would not need to meet the warrant requirement's demand for individualized suspicion.[85]

This approach is fully consistent with the Supreme Court's recent Fourth Amendment cases. Not all searches require a warrant. Rather, as the Court found in a 1995 case upholding random drug testing of high school athletes, "[a]s the text of the Fourth Amendment indicates, the ultimate measure of the constitutionality of a governmental search is 'reasonableness.'"[86] When a passenger enters an airport, government employees search his belongings and subject him to an x-ray—undoubtedly a search—without a warrant. When travelers enter the country, customs and immigration officials can search their baggage and sometimes their persons without a warrant.[87] Of course, when law enforcement undertakes a search to discover evidence of criminal wrongdoing, reasonableness generally requires a judicial warrant. But when the government's conduct is not focused on law enforcement, a warrant is unnecessary. A warrantless search can be constitutional, the Court has said, "'when special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable.'"[88]

A search must be "reasonable" under the circumstances. What does "reasonable" mean? The Court has upheld warrantless searches to reduce deaths on the nation's highways, to

---

84. This conclusion is supported by the Supreme Court's recent "special needs" cases, which allow reasonable, warrantless searches for government needs that go beyond regular law enforcement. *See* Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995) (random drug-testing of student athletes); Mich. Dep't of State Police v. Sitz, 496 U.S. 444, 447 (1990) (stopping drunk drivers); United States v. Martinez-Fuerte, 428 U.S. 543, 545 (1976) (border control checkpoints).

85. City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

86. *Vernonia*, 515 U.S. at 652.

87. *See, e.g.*, United States v. Montoya de Hernandez, 473 U.S. 531, 538 (1985).

88. *Vernonia*, 515 U.S. at 653 (quoting Griffin v. Wisconsin, 483 U.S. 868, 873 (1987)).

maintain safety among railway workers, and to ensure that government officials were not using drugs.[89] In these cases, the "'importance of the governmental interests'" outweighed the "'nature and quality of the intrusion on the individual's Fourth Amendment interests.'"[90] It is hard to imagine that any of these situations are more important than protecting the nation from a direct foreign attack in wartime. "It is obvious and unarguable," the Supreme Court has observed several times, "that no governmental interest is more compelling than the security of the Nation."[91] It is the duty of the President to respond to attacks on the territory and people of the United States, and Congress confirmed the President's authority to use force after September 11. The extraordinary circumstances of war require that the government seek specific information relevant to possible attacks on Americans, sometimes in situations where obtaining a warrant is not practical.[92]

Before the September 11 attacks, the Supreme Court observed that the Fourth Amendment's warrant requirement would probably not apply to the special circumstances created by a potential terrorist attack. "[T]he Fourth Amendment would almost certainly permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route."[93] To be sure, this case, *City of Indianapolis v. Edmond*, challenged the constitutionality of a highway checkpoint program that searched cars for illegal drugs rather than for terrorists. And in *Edmond*, the Court found that the checkpoints vio-

---

89. *See, e.g.*, Pennsylvania v. Labron, 518 U.S. 938, 940 (1996) (per curiam) (automobile searches); *Vernonia*, 515 U.S. at 664–65 (drug testing of athletes); *Sitz*, 496 U.S. at 447 (drunk driver checkpoints); Skinner v. Ry. Labor Executives' Ass'n, 489 U.S. 602, 634 (1989) (drug testing railroad personnel); Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 666 (1989) (drug testing federal customs officers); United States v. Place, 462 U.S. 696, 698 (1983) (baggage search); Terry v. Ohio, 392 U.S. 1, 30–31 (1968) (temporary stop and search).

90. *See* Tennessee v. Garner, 471 U.S. 1, 8 (1985) (quoting *Place*, 462 U.S. at 703).

91. Haig v. Agee, 453 U.S. 280, 307 (1981).

92. The courts have observed that even the use of deadly force is reasonable under the Fourth Amendment if used in self-defense or to protect others. Here, the right to self-defense is not that of an individual, but that of the nation and of its citizens. *Cf. In re* Neagle, 135 U.S. 1, 69 (1890); The Prize Cases, 67 U.S. (2 Black) 635, 673–74 (1862). If the government's heightened interest in self-defense justifies the use of deadly force, then it certainly would also justify warrantless searches.

93. City of Indianapolis v. Edmond, 531 U.S. 32, 44 (2000).

lated the Fourth Amendment protection against search and seizure because the police were searching for drugs for the purpose of "crime control" and "the ordinary enterprise of investigating crimes." [94] But the Court still observed that some warrantless searches were acceptable in the emergency situation of a possible terrorist attack, in which the "need for such measures to ensure public safety can be particularly acute."[95] If the Supreme Court has found that searches for border and airport control present special needs that do not call for a warrant, a court would be hard pressed to deny that searches to find foreign terrorists bent on attacking the United States fall within the same category.

If national security searches do not require a warrant, it might be asked why FISA is even necessary. FISA offers the executive branch a deal. If a President complies with the process of obtaining a FISA warrant, courts will likely agree that the search was reasonable and will admit its fruits as evidence in a criminal case. FISA does not create the power to authorize national security searches. Rather, it describes a safe harbor that deems searches obtained with a warrant reasonable under the Fourth Amendment. If a President proceeds with a search under his own authority rather than under FISA or under ordinary criminal procedure, he takes his chances. A court might refuse to admit evidence in any future proceeding that had been obtained without a warrant, or even allow the target to sue the government for damages.[96] Then again, it might not.

FISA ultimately cannot limit the President's powers to protect national security through surveillance if those powers stem from his unique Article II responsibilities. Intercepting enemy communications has long been part of waging war; indeed, it is critical to the successful use of force.[97] The U.S. military cannot at-

---

94. *Id.*

95. *Id.* at 47–48.

96. *Cf.* AKHIL REED AMAR, THE CONSTITUTION AND CRIMINAL PROCEDURE: FIRST PRINCIPLES 1–45 (1997).

97. In the 1907 Hague Regulations, one of the first treaties on the laws of war, the leading military powers agreed that "the employment of measures necessary for obtaining information about the enemy and the country [is] considered permissible." Laws and Customs of War on Land (Hague IV) art. 24, Oct. 18, 1907, 36 Stat. 2277. Interception of electronic communications is known as SIGINT, or signals intelligence, as opposed to HUMINT, or human intelligence. Writers on the laws of war have recognized that interception of an enemy's communications is a legitimate

tack or defend to good effect unless it knows where to aim. America has a long history of conducting intelligence operations to obtain information on the enemy. General Washington used spies extensively during the Revolutionary War and as President established a secret fund for spying that existed until the creation of the CIA.[98] President Lincoln personally hired spies during the Civil War, a practice the Supreme Court upheld.[99] In both World Wars I and II, Presidents ordered the interception of electronic communications leaving the United States.[100] Some of America's greatest wartime intelligence successes have involved signals intelligence (SIGINT), most notably the breaking of Japanese diplomatic and naval codes during World War II, which allowed the U.S. Navy to anticipate the attack on Midway Island.[101] SIGINT is even more important in this war than in those of the last century. Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them.[102] The primary way to stop those attacks is to find and stop al Qaeda operatives who have infiltrated the United States. The best way to find them is to intercept their electronic communications entering or leaving the country.

The need for executive authority over electronic intelligence gathering becomes apparent when we consider the facts of the war against al Qaeda. In the hours and days after September 11, members of the government thought that al Qaeda would try to crash other airliners or use a weapon of mass destruction in a major east coast city, probably Washington, D.C. Combat air patrols began flying above New York and Washington. Suppose a plane was hijacked and would not respond to air traffic controllers. It would be reasonable for U.S. antiterrorism personnel to intercept any radio or cell phone calls to

---

tool of war. According to one recognized authority, nations at war can gather intelligence using air and ground reconnaissance and observation, "interception of enemy messages, wireless and other," capture of documents, and interrogation of prisoners. MORRIS GREENSPAN, THE MODERN LAW OF LAND WARFARE 326 (1959).

98. Halperin v. CIA, 629 F.2d 144, 157–59 (D.C. Cir. 1980).

99. Totten v. United States, 92 U.S. 105, 106 (1876).

100. Exec. Order No. 2604 (Apr. 28, 1917) (World War I order); Exec. Order No. 8985, 6 Fed. Reg. 6625 (Dec. 23, 1941) (World War II order).

101. CHRISTOPHER ANDREW, FOR THE PRESIDENT'S EYES ONLY 124–25 (1995).

102. Gordon Corera, *Al-Qaeda Chief Zawahiri urges 'lone-wolf' attacks on US*, BBC, Sept. 13, 2013, *available at* www.bbc.co.uk/news/world-middle-east-24083314, [http://perma.cc/48KT-S8KV].

or from the airliner, to discover the hijackers' intentions, what was happening on the plane, and ultimately whether it would be necessary for the fighters to shoot down the plane. Under the civil libertarian approach to privacy, the government could not monitor the suspected hijackers' phone or radio calls unless they received a judicial warrant first—the calls, after all, are electronic communications within the United States. A warrant would be hard to obtain because it is unlikely that the government would then know the identities of all the hijackers, who might be U.S. citizens or permanent resident aliens. But because the United States is in a state of war, the military can intercept the communications of the plane to see if it poses a threat, and target the enemy if necessary, without a judicial warrant because the purpose is not arrest and trial, but to prevent an attack. This comports far better with the principle of reasonableness that guides the Fourth Amendment.

As Commander-in-Chief, the President has the constitutional power and the responsibility to wage war in response to a direct attack against the United States.[103] In the Civil War, President Lincoln undertook several actions—raising an army, withdrawing money from the treasury, launching a blockade—on his own authority in response to the Confederate attack on Fort Sumter, moves that Congress and the Supreme Court later approved.[104] During World War II, the Supreme Court similarly recognized that once war began, the President's authority as Commander-in-Chief and Chief Executive gave him the tools necessary to wage war effectively.[105] In the wake of the September 11 attacks, Congress agreed that "the President has authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States," which recognizes the

---

103. *See* ERIC A. POSNER & ADRIAN VERMEULE, TERROR IN THE BALANCE: SECURITY, LIBERTY, AND THE COURTS 4 (2007) ("The essential feature of the emergency is that national security is threatened; because the executive is the only organ of government with the resources, power, and flexibility to respond to threats to national security, it is natural, inevitable, and desirable for power to flow to this branch of government. Congress rationally acquiesces; courts rationally defer.").

104. *See* The Prize Cases, 67 U.S. (2 Black) 635, 670 (1862). For a more detailed discussion, see JOHN YOO, CRISIS AND COMMAND: THE HISTORY OF EXECUTIVE POWER FROM GEORGE WASHINGTON TO GEORGE W. BUSH 208–12 (2009).

105. The President has the power "to direct the performance of those functions which may constitutionally be performed by the military arm of the nation in time of war" and to issue military commands using the powers to conduct war "to repel and defeat the enemy." *Ex parte Quirin*, 317 U.S. 1, 28 (1942).

President's authority to use force to respond to al Qaeda, and any powers necessary and proper to that end.[106]

Even legal scholars who argue against this historical practice concede that once the United States has been attacked, the President can respond immediately with force. The ability to collect intelligence is intrinsic to the use of military force. It is inconceivable that the Constitution would vest in the President the powers of Commander-in-Chief and Chief Executive and give him the responsibility to protect the nation from attack, but then disable him from gathering intelligence on how to use the military most effectively to defeat the enemy. Every evidence of the Framers' understanding of the Constitution is that the government would have every ability to meet a foreign danger. As James Madison wrote in *The Federalist*, "[s]ecurity against foreign danger is one of the primitive objects of civil society."[107] Therefore, the "powers requisite for attaining it must be effectually confided to the federal councils."[108] After World War II, the Supreme Court declared that a "grant of war power includes all that is necessary and proper for carrying these powers into execution."[109] Covert operations and electronic surveillance are clearly part of this authority.

During the writing of the Constitution, some Framers believed that the President alone should manage intelligence because only he could keep secrets.[110] Several Supreme Court cases have recognized that the President's role as Commander-in-Chief and the primary organ of the nation in its foreign relations must include the power to collect intelligence.[111] These authorities agree that responsibility for intelligence gathering

106. Authorization for the Use of Military Force, Pub. L. 107-40, 115 Stat. 224 (2001).

107. THE FEDERALIST NO. 41, at 256 (James Madison) (Clinton Rossiter ed., 1961).

108. *Id.*

109. Johnson v. Eisentrager, 339 U.S. 763, 788 (1950).

110. THE FEDERALIST NO. 64, at 392–93 (John Jay).

111. *See, e.g.*, Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948); United States v. Curtiss-Wright Export Corp., 299 U.S. 304, 320 (1936). In a post-Civil War case, recently re-affirmed, the Court ruled that President Lincoln had the constitutional authority to engage in espionage. The President "was undoubtedly authorized during the war, as commander-in-chief . . . to employ secret agents to enter the rebel lines and obtain information respecting the strength, resources, and movements of the enemy." Totten v. United States, 92 U.S. 105, 106 (1876). On Totten's continuing vitality, see Tenet v. Doe, 544 U.S. 1, 8–11 (2005).

rests with the President because the structure of the office allows for unified, secret, and speedy action.

Presidents have long ordered electronic surveillance without any judicial or congressional participation. More than a year before the Pearl Harbor attacks, but with war clearly looming with the Axis powers, President Franklin Roosevelt authorized the FBI to intercept any communications, whether wholly inside the country or abroad, of persons "suspected of subversive activities against the Government of the United States, including suspected spies."[112] FDR was concerned that "fifth columns" could wreak havoc with the war effort. "It is too late to do anything about it after sabotage, assassinations and 'fifth column' activities are completed," FDR wrote in his order.[113] FDR ordered the surveillance even though a federal law at the time prohibited electronic surveillance without a warrant.[114] Presidents continued to monitor the communications of national security threats on their own authority, even in peacetime.[115] If Presidents in times of peace could order surveillance of spies and terrorists, executive authority is only the greater now, as hostilities continue against al Qaeda. This is not a view that Justice Departments have held only under Presidents George W. Bush or Barack Obama. The Clinton Justice Department held a similar view of the executive branch's authority to conduct surveillance outside the FISA framework.[116]

Courts have never opposed a President's authority to engage in warrantless electronic surveillance to protect national securi-

---

112. United States v. U.S. District Court, 444 F.2d 651, 669–70 (6th Cir. 1971).

113. *Id*.

114. *See* Nardone v. United States, 302 U.S. 379, 382 (1937) (interpreting section 605 of Federal Communications Act of 1934 to prohibit interception of telephone calls).

115. *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation of the H. Permanent Select Comm. on Intelligence*, 95th Cong., 14 (1978) (statement of Griffin Bell, Att'y General of the United States).

116. Most notably, Clinton Deputy Attorney General Jamie Gorelick testified before Congress that the Justice Department could carry out physical searches for foreign intelligence purposes, even though FISA at the time did not provide for them. *See Amending the Foreign Intelligence Surveillance Act: Hearing Before the H. Permanent Select Comm. on Intelligence*, 103d Cong. 54, 56 (1994) (statement of Jamie Gorelick, Deputy Att'y General of the United States). Clinton's OLC even issued a legal opinion that the President could order the sharing of electronic surveillance gathered through criminal wiretaps between the Justice Department and intelligence agencies, even though this was prohibited by statute. *See* Title III Electronic Surveillance Material and the Intelligence Community, 24 Op. O.L.C. 261, 269–70 (2000).

ty. When the Supreme Court first considered this question in 1972, it held that the Fourth Amendment required a judicial warrant if a President wanted to conduct surveillance of a purely domestic group, but it refused to address surveillance of foreign threats to national security.[117] In the years since, every federal appeals court to address the question, including the FISA Appeals Court, has "held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information."[118] The FISA Appeals Court did not even feel that it was worth much discussion. It took the President's power to do so "for granted," and observed that "FISA could not encroach on the President's constitutional power."[119]

Congress also implicitly authorized the President to carry out electronic surveillance to prevent further attacks on the United States. Congress's September 18, 2001 Authorization to Use Military Force is sweeping; it has no limitation on time or place—its only limitation is that the President is to pursue al Qaeda.[120] Although the President did not need, as a constitutional matter, Congress's permission to pursue and attack al Qaeda after the attacks on New York City and the Pentagon, its passage shows that the President and Congress fully agreed that military action would be appropriate. Congress's approval of the killing and capture of al Qaeda members obviously must include the tools to locate them in the first place.

A choice between FISA or his constitutional authority gives the President the discretion to use the best method to protect the United States, whether through the military or by relying on law enforcement. It also means warrantless surveillance will not be introduced into the criminal justice system; the judiciary is only needed to enforce this legal distinction. Presidents could alleviate concern about the NSA programs by publicly declaring that no evidence generated by them will be used in a criminal case. Although FISA cannot supersede the President's constitutional authority, it can provide a more stable system for the domestic collection of foreign intelligence, such as the NSA's collection of phone call metadata and foreign e-mails.

---

117. United States v. U.S. District Court, 407 U.S. 297, 321–22 (1972).

118. *See, e.g.*, *In re* Sealed Case, 310 F.3d 717, 742 (FISA Ct. Rev. 2002).

119. *Id.*

120. Authorization for the Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).

IV. CONCLUSIONS

The real problem with FISA, and even the Patriot Act, as they existed before the 2008 Amendments, is that they remained rooted in a law enforcement approach to electronic surveillance. They tied the government's counterterrorism efforts to individualized suspicion. Searches and wiretaps had to target a specific individual already believed to be involved in harmful activity. But detecting al Qaeda members who have no previous criminal record in the United States, and who are undeterred by the possibility of criminal sanctions, requires the use of more sweeping methods.

To prevent attacks successfully, the government has to devote surveillance resources where there is a reasonable chance that terrorists will appear or communicate, even if their specific identities remain unknown. What if the government knew that there was a fifty percent chance that terrorists would use a certain communications pipeline, such as e-mail provided by a popular Pakistani ISP, but that most of the communications on that channel would not be linked to terrorism? An approach based on individualized suspicion would prevent computers from searching through that channel for the keywords or names that might suggest terrorist communications because there are no specific al Qaeda suspects and thus no probable cause. Searching for terrorists depends on playing the probabilities rather than individualized suspicion, just as roadblocks or airport screenings do. The private owner of any website has detailed access to information about the individuals who visit the site that he can exploit for his own commercial purposes, such as selling lists of names to spammers or gathering market data on individuals or groups. Is the government's effort to find violent terrorists a less legitimate use of such data?

Individualized suspicion dictates the focus of law enforcement, but war demands that our armed forces defend the country with a broader perspective. Armies do not meet a "probable cause" requirement when they attack a position, fire on enemy troops, or intercept enemy communications. The purpose of the criminal justice system is to hold a specific person responsible for a discrete crime that has already happened. But focusing on individualized suspicion does not make sense when the purpose of intelligence is to take action, such as killing or captur-

ing members of an enemy group, to prevent future harm to the nation from a foreign threat.

FISA should be regarded as a safe harbor that allows the fruits of an authorized search to be used for prosecution. Using FISA sacrifices speed and breadth of information in favor of individualized suspicion, but it provides a path for using evidence in a civilian criminal prosecution. If the President chooses to rely on his constitutional authority alone to conduct warrantless searches, then he should generally use the information only for military purposes. The primary objective of the NSA program is to "detect and prevent" possible al Qaeda attacks on the United States, whether another attack like September 11; a bomb in apartment buildings, bridges, or transportation hubs such as airports; or a nuclear, biological, or chemical attack. These are not hypotheticals; they are all al Qaeda plots, some of which U.S. intelligence and law enforcement agencies have already stopped. A President will want to use information gathered by the NSA to deploy military, intelligence, and law enforcement personnel to stop the next attack. The price to pay for speed, however, is foregoing any future criminal prosecution. If the President wants to use the NSA to engage in warrantless searches, he cannot use its fruits in an ordinary criminal prosecution.

Al Qaeda has launched a variety of efforts to attack the United States, and it intends to continue them. The primary way to stop those attacks is to find and stop al Qaeda operatives, and the best way to find them is to intercept their electronic communications. Properly understood, the Constitution does not subject the government to unreasonable burdens in carrying out its highest duty of protecting the nation from attack.