In what ways does federal electronic surveillance law protect Internet communication differently from telephone communication? Should the privacy protections differ in these areas?

CHAPTER 5

NATIONAL SECURITY AND FOREIGN INTELLIGENCE

CHAPTER OUTLINE

Should the law treat investigations involving national security differently than other criminal investigations? This question has long been one that the law has struggled with. Additionally, there are times when government intelligence agencies want to gather foreign intelligence within the United States. One example is when there might be a foreign spy within the United States. Another example is when intelligence agencies just want to spy on a foreign individual who is in the United States to see what can be learned about the activities of foreign nations. These instances might not involve a criminal investigation or even an immediate national security threat — they merely involve gathering useful foreign intelligence.

The difficulty is in delineating between these activities. For example, suppose intelligence agencies are monitoring the activities of individuals with connections to a foreign terrorist organization. There will certainly be an interest in gathering foreign intelligence. National security will likely be implicated. And the case may very likely result in a criminal prosecution if evidence is obtained that the individuals are plotting a terrorist act.

The previous chapter provided an introduction to the Fourth Amendment and to electronic surveillance law, with a focus on the Electronic Communications Privacy Act (ECPA). Ordinarily, government information gathering activities would fall under the Fourth Amendment rules discussed in the previous chapter on law enforcement, and government electronic surveillance would be regulated by ECPA. However, with national security and foreign intelligence gathering, the Fourth Amendment rules are different, and ECPA often does not apply. Instead, other statutes and regulations apply.

A. THE INTELLIGENCE COMMUNITY

The United States intelligence community consists of a number of agencies that gather information about threats domestic and foreign. The three most prominent intelligence agencies are the FBI, CIA, and NSA.

Federal Bureau of Investigation (FBI). The FBI was originally created in 1908 and called the "Bureau of Investigation." It was not until 1935 when the FBI received its current name. The focus of the FBI is on domestic criminal investigations involving federal crimes. However, the FBI also has intelligence, counterintelligence, and counterterrorism functions.

Central Intelligence Agency (CIA). Before the creation of the CIA, its functions were handled by the Office of Strategic Services (OSS), which was created in 1942 by President Franklin D. Roosevelt. The OSS was eliminated at the end of World War II. President Harry Truman created the CIA with the National Security Act of 1947.

National Security Agency (NSA). Located within the Department of Defense, the NSA was created by President Truman in 1952 to engage in cryptology—deciphering encryption codes used in foreign communications. Subsequently the size and activities of the NSA have increased, and the agency is now engaged in large-scale information gathering activities.

Other Intelligence Agencies. There are many other intelligence agencies beyond the FBI, CIA, and NSA. These agencies are located within the Department of Defense, Department of Homeland Security, Department of State, and Department of the Treasury, among others. Some of these entities include the Defense Intelligence Agency (DIA), the State Department's Bureau of Intelligence and Research (INR), and the Treasury Department's Office of Terrorism and Financial Intelligence.

B. THE FOURTH AMENDMENT FRAMEWORK

Does the Fourth Amendment apply differently to national security and foreign intelligence gathering than it does for domestic criminal investigations? These questions long remained unresolved, and are still not fully resolved to this day.

In a footnote to *Katz v. United States,* 389 U.S. 347 (1967), the Court stated that perhaps a warrant might not be required in situations involving national security:

> Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not presented by this case.

Justice White, in a concurring opinion, declared:

> In joining the Court's opinion, I note the Court's acknowledgment that there are circumstance in which it is reasonable to search without a warrant. In this connection . . . the Court points out that today's decision does not reach national security cases. Wiretapping to protect the security of the Nation has been authorized by successive Presidents. The present Administration would apparently save national security cases from restrictions against wiretapping. We should not require the warrant procedure and the magistrate's judgment if the President of the United States or his chief legal officer, the Attorney General, has considered the requirements of national security and authorized electronic surveillance as reasonable.

Justices Douglas and Brennan, in another concurring opinion, took issue with Justice White:

> . . . Neither the President nor the Attorney General is a magistrate. In matters where they believe national security may be involved they are not detached, disinterested, and neutral as a court or magistrate must be. . . .
>
> There is, so far as I understand constitutional history, no distinction under the Fourth Amendment between types of crimes. Article III, § 3, gives "treason" a very narrow definition and puts restrictions on its proof. But the Fourth Amendment draws no lines between various substantive offenses. The arrests on cases of "hot pursuit" and the arrests on visible or other evidence of probable cause cut across the board and are not peculiar to any kind of crime.
>
> I would respect the present lines of distinction and not improvise because a particular crime seems particularly heinous. When the Framers took that step, as they did with treason, the worst crime of all, they made their purpose manifest.

The Supreme Court finally confronted these issues more squarely in a case decided in 1972, *United States v. United States District Court,* which has become known as the *Keith* case, named after District Court Judge Damon Keith.

The *Keith* case began when three founding members of a group called "the White Panthers" bombed a CIA office located in Michigan. The group was not a racist group and in fact was supportive of the Black Panthers. The White Panther agenda was to abolish money. According to the group's manifesto: "We demand total freedom for everybody! And we will not be stopped until we get it. . . . Rock

and Roll music is the spearhead of our attack because it is so effective and so much fun."[1]

When it investigated the bombing, the government wiretapped the phone calls of one of the bombers. This was done without a warrant. Recall from the previous chapter that in 1967 the Supreme Court in *United States v. Katz,* 389 U.S. 347 (1967), held that the Fourth Amendment required a warrant in order for the government to wiretap a phone call. Also recall that in 1968 Congress required special court orders for the government to engage in wiretapping when it passed Title III of the Omnibus Crime Control and Safe Streets Act (which now is the Wiretap Act portion of the Electronic Communications Privacy Act (ECPA)).

The Nixon Administration contended that because this case involved a matter of national security, he was able to conduct surveillance without a Fourth Amendment warrant or Title III court order. The Supreme Court, however, in the *Keith* decision below did not agree.

UNITED STATES V. UNITED STATES DISTRICT COURT (THE *KEITH* CASE)

407 U.S. 297 (1972)

POWELL, J. . . . The issue before us is an important one for the people of our country and their Government. It involves the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval. Successive Presidents for more than one-quarter of a century have authorized such surveillance in varying degrees, without guidance from the Congress or a definitive decision of this Court. This case brings the issue here for the first time. Its resolution is a matter of national concern, requiring sensitivity both to the Government's right to protect itself from unlawful subversion and attack and to the citizen's right to be secure in his privacy against unreasonable Government intrusion.

This case arises from a criminal proceeding in the United States District Court for the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy Government property. . . . One of the defendants, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Ann Arbor, Michigan.

Title III of the Omnibus Crime Control and Safe Streets Act, 18 U.S.C. §§ 2510-2520, authorizes the use of electronic surveillance for classes of crimes carefully specified in 18 U.S.C. § 2516. Such surveillance is subject to prior court order. Section 2518 sets forth the detailed and particularized application necessary to obtain such an order as well as carefully circumscribed conditions for its use. The Act represents a comprehensive attempt by Congress to promote more effective control of crime while protecting the privacy of individual thought and expression. Much of Title III was drawn to meet the constitutional requirements

[1] Trevor W. Morrison, *The Story of United States v. U.S. District Court (Keith): The Surveillance Power, in Presidential Power Stories* 287 (Christopher Schroeder & Curtis Bradley eds., 2008).

for electronic surveillance enunciated by this Court in *Berger v. New York,* and *Katz v. United States*.

The Government relies on § 2511(3). It argues that "in excepting national security surveillances from the Act's warrant requirement Congress recognized the President's authority to conduct such surveillances without prior judicial approval." The section thus is viewed as a recognition or affirmance of a constitutional authority in the President to conduct warrantless domestic security surveillance such as that involved in this case.

We think the language of § 2511(3), as well as the legislative history of the statute, refutes this interpretation. The relevant language is that: "Nothing contained in this chapter . . . shall limit the constitutional power of the President to take such measures as he deems necessary to protect . . ." against the dangers specified. At most, this is an implicit recognition that the President does have certain powers in the specified areas. Few would doubt this, as the section refers — among other things — to protection "against actual or potential attack or other hostile acts of a foreign power." But so far as the use of the President's electronic surveillance power is concerned, the language is essentially neutral.

Section 2511(3) certainly confers no power, as the language is wholly inappropriate for such a purpose. It merely provides that the Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them.

Our present inquiry, though important, is . . . a narrow one. It addresses a question left open by *Katz*:

> Whether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security. . . .

We begin the inquiry by noting that the President of the United States has the fundamental duty, under Art. II, § 1, of the Constitution, to "preserve, protect and defend the Constitution of the United States." Implicit in that duty is the power to protect our Government against those who would subvert or overthrow it by unlawful means. In the discharge of this duty, the President — through the Attorney General — may find it necessary to employ electronic surveillance to obtain intelligence information on the plans of those who plot unlawful acts against the Government. The use of such surveillance in internal security cases has been sanctioned more or less continuously by various Presidents and Attorneys General since July 1946.

Though the Government and respondents debate their seriousness and magnitude, threats and acts of sabotage against the Government exist in sufficient number to justify investigative powers with respect to them.[2] The covertness and complexity of potential unlawful conduct against the Government and the necessary dependency of many conspirators upon the telephone make electronic surveillance an effective investigatory instrument in certain circumstances. The

[2] The Government asserts that there were 1,562 bombing incidents in the United States from January 1, 1971, to July 1, 1971, most of which involved Government related facilities. Respondents dispute these statistics as incorporating many frivolous incidents as well as bombings against nongovernmental facilities. The precise level of this activity, however, is not relevant to the disposition of this case.

marked acceleration in technological developments and sophistication in their use have resulted in new techniques for the planning, commission, and concealment of criminal activities. It would be contrary to the public interest for Government to deny to itself the prudent and lawful employment of those very techniques which are employed against the Government and its lawabiding citizens. . . .

But a recognition of these elementary truths does not make the employment by Government of electronic surveillance a welcome development — even when employed with restraint and under judicial supervision. There is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens. We look to the Bill of Rights to safeguard this privacy. Though physical entry of the home is the chief evil against which the wording of the Fourth Amendment is directed, its broader spirit now shields private speech from unreasonable surveillance. Our decision in *Katz* refused to lock the Fourth Amendment into instances of actual physical trespass.

. . . [N]ational security cases, moreover, often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech. . . . The danger to political dissent is acute where the Government attempts to act under so vague a concept as the power to protect "domestic security." Given the difficulty of defining the domestic security interest, the danger of abuse in acting to protect that interest becomes apparent.

The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.

As the Fourth Amendment is not absolute in its terms, our task is to examine and balance the basic values at stake in this case: the duty of Government to protect the domestic security, and the potential danger posed by unreasonable surveillance to individual privacy and free expression. If the legitimate need of Government to safeguard domestic security requires the use of electronic surveillance, the question is whether the needs of citizens for privacy and the free expression may not be better protected by requiring a warrant before such surveillance is undertaken. We must also ask whether a warrant requirement would unduly frustrate the efforts of Government to protect itself from acts of subversion and overthrow directed against it. . . .

[C]ontentions in behalf of a complete exemption from the warrant requirement, when urged on behalf of the President and the national security in its domestic implications, merit the most careful consideration. We certainly do not reject them lightly, especially at a time of worldwide ferment and when civil disorders in this country are more prevalent than in the less turbulent periods of our history. There is, no doubt, pragmatic force to the Government's position.

[W]e do not think a case has been made for the requested departure from Fourth Amendment standards. The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing

intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure.

We cannot accept the Government's argument that internal security matters are too subtle and complex for judicial evaluation. Courts regularly deal with the most difficult issues of our society. There is no reason to believe that federal judges will be insensitive to or uncomprehending of the issues involved in domestic security cases. . . . If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.

Nor do we believe prior judicial approval will fracture the secrecy essential to official intelligence gathering. The investigation of criminal activity has long involved imparting sensitive information to judicial officers who have respected the confidentialities involved. Judges may be counted upon to be especially conscious of security requirements in national security cases. Title III of the Omnibus Crime Control and Safe Streets Act already has imposed this responsibility on the judiciary in connection with such crimes as espionage, sabotage, and treason, §§ 2516(1)(a) and (c), each of which may involve domestic as well as foreign security threats. Moreover, a warrant application involves no public or adversary proceedings: it is an ex parte request before a magistrate or judge. Whatever security dangers clerical and secretarial personnel may pose can be minimized by proper administrative measures, possibly to the point of allowing the Government itself to provide the necessary clerical assistance. . . .

We emphasize, before concluding this opinion, the scope of our decision. As stated at the outset, this case involves only the domestic aspects of national security. We have not addressed and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents. . . .

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. We recognize that domestic security surveillance may involve different policy and practical considerations from the surveillance of "ordinary crime." The gathering of security intelligence is often long range and involves the interrelation of various sources and types of information. The exact targets of such surveillance may be more difficult to identify than in surveillance operations against many types of crime specified in Title III. Often, too, the emphasis of domestic intelligence gathering is on the prevention of unlawful activity or the enhancement of the Government's preparedness for some possible future crisis or emergency. Thus, the focus of domestic surveillance may be less precise than that directed against more conventional types of crime.

Given those potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth

Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection. . . .

DOUGLAS, J. concurring. While I join in the opinion of the Court, I add these words in support of it. . . .

If the Warrant Clause were held inapplicable here, then the federal intelligence machine would literally enjoy unchecked discretion. Here, federal agents wish to rummage for months on end through every conversation, no matter how intimate or personal, carried over selected telephone lines, simply to seize those few utterances which may add to their sense of the pulse of a domestic underground. . . .

That "domestic security" is said to be involved here does not draw this case outside the mainstream of Fourth Amendment law. Rather, the recurring desire of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that prohibition. For it was such excesses as the use of general warrants and the writs of assistance that led to the ratification of the Fourth Amendment. . . .

[W]e are currently in the throes of another national seizure of paranoia, resembling the hysteria which surrounded the Alien and Sedition Acts, the Palmer Raids, and the McCarthy era. Those who register dissent or who petition their governments for redress are subjected to scrutiny by grand juries, by the FBI, or even by the military. Their associates are interrogated. Their homes are bugged and their telephones are wiretapped. They are befriended by secret government informers. Their patriotism and loyalty are questioned. . . .

We have as much or more to fear from the erosion of our sense of privacy and independence by the omnipresent electronic ear of the Government as we do from the likelihood that fomenters of domestic upheaval will modify our form of governing.

NOTES & QUESTIONS

1. ***The Fourth Amendment Framework in* Keith.** The *Keith* Court draws a distinction between electronic surveillance in (1) criminal investigations, regulated under Title III (now ECPA); (2) domestic national security investigations; and (3) foreign intelligence gathering, including investigations involving "activities of foreign powers and their agents."

   (1) Ordinary Criminal Investigations. Regarding ordinary criminal investigations, the *Keith* Court stated that there was no debate regarding "the necessity of obtaining a warrant in the surveillance of crimes unrelated to the national security interest."

   (2) Domestic National Security Investigations. Regarding domestic national security investigations, the focus of the *Keith* Court's opinion, its holding was that the Fourth Amendment required the issuing of a warrant in domestic security investigations. It also held that the precise requirements for issuing a requirement to investigate domestic security need not be the same as for Title III criminal surveillance.

   (3) Foreign Intelligence Gathering. Finally, the *Keith* Court stated that it did not address issues involving foreign powers and their agents.

Does this tripartite distinction seem useful as a policy matter? How does one distinguish between security surveillance (category two) and surveillance for ordinary crime (category one)?

Daniel Solove argues that such a distinction ought not to be made: "'National security' has often been abused as a justification not only for surveillance but also for maintaining the secrecy of government records as well as violating the civil liberties of citizens." He further contends that "the line between national security and regular criminal activities is very blurry, especially in an age of terrorism."[3] In his book, *Nothing to Hide,* Solove further argues:

> It is difficult to distinguish national-security matters from ordinary crime, especially when U.S. citizens are involved. National security threats *are* a form of crime. They are severe crimes. But the rules for investigating ordinary crime are designed to regulate government information gathering no matter how grave the particular crime might be. These rules aren't rigid, and they make allowances for emergencies and unusual circumstances.[4]

On the other hand, Richard Posner contends that the word "unreasonable" in the Fourth Amendment "invites a wide-ranging comparison between the benefits and costs of a search or seizure." He proposes a "sliding scale" standard where "the level of suspicion require to justify the search or seizure should fall . . . as the magnitude of the crime under investigation rises."[5] Paul Rosenzweig argues: "In this time of terror, some adjustment of the balance between liberty and security is both necessary and appropriate. . . . [T]he very text of the Fourth Amendment — with its prohibition only of 'unreasonable' searches and seizures — explicitly recognizes the need to balance the harm averted against the extent of governmental intrusion."[6]

2. ***The Church Committee Report.*** In 1976, a congressional committee led by Senator Frank Church (called the "Church Committee") engaged in an extensive investigation of government national security surveillance. It found extensive abuses, which it chronicled in its famous report known as the Church Committee Report:

   > Too many people have been spied upon by too many Government agencies and too much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power. The Government, operating primarily through

---

[3] Solove, *Surveillance Law,* 72 Geo. Wash. L. Rev. 1264, 1301-02 (2004).

[4] Daniel J. Solove, *Nothing to Hide: The False Tradeoff Between Privacy and Security* 66 (2011).

[5] Richard Posner, *Law, Pragmatism, and Democracy* 303 (2003); *see also* Akhil Reed Amar, *The Constitution and Criminal Procedure* 31 (1997) ("The core of the Fourth Amendment . . . is neither a warrant nor probable cause but reasonableness.").

[6] Paul Rosenzweig, *Civil Liberty and the Response to Terrorism,* 42 Duq. L. Rev. 663 (2004).

> secret informants, but also using other intrusive techniques such as wiretaps, microphone "bugs," surreptitious mail opening, and break-ins, has swept in vast amounts of information about the personal lives, views, and associations of American citizens. . . . Groups and individuals have been harassed and disrupted because of their political views and their lifestyles. Investigations have been based upon vague standards whose breadth made excessive collection inevitable. . . .
>
> The FBI's COINTELPRO — counterintelligence program — was designed to "disrupt" groups and "neutralize" individuals deemed to be threats to domestic security. The FBI resorted to counterintelligence tactics in part because its chief officials believed that existing law could not control the activities of certain dissident groups, and that court decisions had tied the hands of the intelligence community. Whatever opinion one holds about the policies of the targeted groups, many of the tactics employed by the FBI were indisputably degrading to a free society. . . .
>
> Since the early 1930's, intelligence agencies have frequently wiretapped and bugged American citizens without the benefit of judicial warrant. . . .
>
> There has been, in short, a clear and sustained failure by those responsible to control the intelligence community and to ensure its accountability.[7]

The Church Committee Report was influential in the creation of FISA as well as the Attorney General Guidelines.

3. ***National Security vs. Civil Liberties.*** Eric Posner and Adrian Vermeule argue that the legislature and judiciary should defer to the executive in times of emergency and that it is justified to curtail civil liberties when national security is threatened:

> 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. . . .
>
> During emergencies, when new threats appear, the balance shifts; government should and will reduce civil liberties in order to enhance security in those domains where the two must be traded off. . . .
>
> In emergencies . . . judges are at sea, even more so than are executive officials. The novelty of the threats and of the necessary responses makes judicial routines and evolved legal rules seem inapposite, even obstructive. There is a premium on the executive's capacities for swift, vigorous, and secretive action.[8]

4. ***The Fourth Amendment and Foreign Intelligence Surveillance.*** *Keith* did not address how the Fourth Amendment would govern foreign intelligence surveillance (category three). Circuit courts examining the issue have concluded that at a minimum, no warrant is required by the Fourth Amendment for foreign intelligence surveillance. In *United States v. Butenko*, 494 F.2d 593 (3d Cir. 1974) (en banc), the court justified this conclusion by reasoning that "foreign intelligence gathering is a clandestine and highly unstructured activity, and the need for electronic surveillance often cannot be anticipated in advance." Reaching a similar conclusion in *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980), the court reasoned: "[T]he 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, following *Keith,* 'unduly frustrate' the President in carrying out his foreign affairs responsibilities."

[7] *Intelligence Activities and the Rights of Americans* (Vol. 2), Final Report of the Select Committee to Study Government Operations with Respect to Intelligence Activities 5, 10, 15 (Apr. 26, 1976).

[8] Eric A. Posner & Adrian Vermeule, *Terror in the Balance: Security, Liberty, and the Courts* 4, 5, 18 (2006). For another defense of the curtailment of civil liberties for national security, see Richard A. Posner, *Not a Suicide Pact: The Constitution in a Time of National Emergency* (2006).

C. FOREIGN INTELLIGENCE GATHERING

1. THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

In the *Keith* case, the Court explicitly refused to address whether the Fourth Amendment would require a warrant for surveillance of agents of foreign powers.

The Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, codified at 50 U.S.C. §§ 1801–1811, establishes standards and procedures for use of electronic surveillance to collect "foreign intelligence" within the United States. § 1804(a)(7)(B). FISA creates a different regime than ECPA, the legal regime that governs electronic surveillance for law enforcement purposes. The regime created by FISA is designed primarily for intelligence gathering agencies to regulate how they gain general intelligence about foreign powers and agents of foreign powers within the borders of the United States. In contrast, the regime of ECPA is designed for domestic law enforcement to govern the gathering of information for criminal investigations involving people in United States.

Applicability of FISA. When does FISA govern rather than ECPA? FISA generally applies when foreign intelligence gathering is "a significant purpose" of the investigation. 50 U.S.C. § 1804(a)(7)(B) and § 1823(a)(7)(B). The language of "a significant purpose" comes from the USA PATRIOT Act of 2001. Prior to the USA PATRIOT Act, FISA as interpreted by the courts required that the collection of foreign intelligence be the primary purpose for surveillance. After the USA PATRIOT Act, foreign intelligence gathering need no longer be the primary purpose. A further expansion of the FISA occurred in 2008 with amendments to that law, which we discuss below.

The Foreign Intelligence Surveillance Court (FISC). Requests for FISA orders are reviewed by a special court of federal district court judges. The USA PATRIOT Act increased the number of judges on the FISC from 7 to 11. 50 U.S.C. § 1803(a). The proceedings are ex parte, with the Department of Justice (DOJ) making the applications to the court on behalf of the CIA and other agencies. The Court meets in secret, and its proceedings are generally not revealed to the public or to the targets of the surveillance.

In 2007, the FISC declined an ACLU request to access its documents relating to alleged unauthorized surveillance. *In re Motion for Release of Court Records*,

526 F. Supp. 2d (2007). This case was an exception to the usual procedure of *ex parte* only hearings before the FISC. The court found that it had jurisdiction to entertain motions for release of its documents, and then denied the request. It stated:

> The FISC is a unique court. Its entire docket relates to the collection of foreign intelligence by the federal government. The applications submitted to it by the government are classified, as are the overwhelming majority of the FISC's orders. Court sessions are held behind closed doors in a secure facility, and every proceeding in its history prior to this one has been ex parte, with the government the only party. . . . Other courts operate primarily in public with secrecy the exception; the FISC operates primarily in secret, with public access the exception.

Perhaps most importantly, the court noted that "the proper functioning of the FISA process would be adversely affected if submitting sensitive information to the FISC could subject the Executive Branch's classification to a heightened form of judicial review."

Court Orders. The legal test for surveillance under FISA is not whether probable cause exists that the party to be monitored is involved in criminal activity. Rather, the court must find probable cause that the party to be monitored is a "foreign power" or "an agent of a foreign power." § 1801. Therefore, unlike ECPA or the Fourth Amendment, FISA surveillance is not tied to any required showing of a connection to criminal activity. However, if the monitored party is a "United States person" (a citizen or permanent resident alien), the government must establish probable cause that the party's activities "may" or "are about to" involve a criminal violation. § 1801(b)(2)(A).

Surveillance Without Court Orders. In certain circumstances, FISA authorizes surveillance without having to first obtain a court order. § 1802. In particular, the surveillance must be "solely directed at" obtaining intelligence exclusively from "foreign powers." § 1802(a). There must be "no substantial likelihood that the surveillance will acquire the contents of any communications to which a United States person is a party." § 1802(a)(1)(B). Electronic surveillance without a court order requires the authorization of the President, through the Attorney General, in writing under oath. § 1802(a)(1).

Video Surveillance. Unlike ECPA, FISA explicitly regulates video surveillance. In order to have court approval for video surveillance, the FISA requires the government to submit, among other things, "a detailed description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance," § 1804(a)(6); "a certification . . . that such information cannot reasonably be obtained by normal investigative techniques," § 1804(a)(7); and "a statement of the period of time for which the electronic surveillance is required to be maintained," § 1804(a)(10). Video surveillance orders can last for 90 days.

The FISA Amendments Act. In 2008, Congress enacted significant amendments to FISA. The FISA Amendments Act (FAA) was passed in response to the revelation in 2005 that since 9/11 the National Security Agency (NSA) was engaging in an extensive program of warrantless wiretapping of international phone calls. Subsequently, several lawsuits were brought against the telecommunications companies that participated in the surveillance for violating FISA and ECPA. One of the most controversial aspects of the FAA was a grant of retroactive immunity to these companies. The NSA surveillance program and the ensuing litigation will be discussed later in this chapter.

In its other aspects, the FAA both expanded the government's surveillance abilities and added new privacy protections. The FAA explicitly permits collection of information from U.S. telecommunications facilities where it is not possible in advance to know whether a communication is purely international (that is, all parties to it are located outside of the United States) or whether the communication involves a foreign power or its agents. David Kris explains, "With the advent of web-based communication and other developments, the government cannot always determine — consistently, reliably, and in real time — the location of parties to an e-mail message."[9] It is also possible to collect information and then examine it (through data mining) to look for links with a foreign power or its agents. The perceived need, Kris states, was for a kind of "vacuum-cleaner" capacity that would enable the government to sift through large amounts of information without meeting FISA's traditional warrant requirements.

FAA amends FISA to permit "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." § 702(a). The person targeted must be a non-U.S. person, or certain more restrictive measures apply. §§ 703–04. The critical substantive requirements are that the "target" of the surveillance be someone overseas and that a "significant purpose" of the surveillance be to acquire "foreign intelligence information," which is broadly defined.

The collection of this information must be carried out in accordance with certain "targeting procedures" to ensure that the collection is directed at persons located outside the United States. § 702(c)(1)(A). The acquisition must also involve new minimization procedures, which the Attorney General is to adopt. § 702(e). The Justice Department and the Director of National Intelligence must certify in advance of the surveillance activity that targeting and minimization procedures meet the statutory standards and that "a significant purpose" of the surveillance is to acquire foreign intelligence information. § 702(g)(2). The FAA also states that the government may not engage in a kind of "reverse-targeting" — the government cannot target "a person reasonably believed to be outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." § 702(b)(2).

The FISC is to review certifications and the targeting and minimization procedures adopted. If a certification does not "contain all the required elements" or the procedures "are not consistent with the requirements" of the FAA or the

---

[9] David Kris, *A Guide to the New FISA Bill, Part I*, Balkanization (June 21, 2008), at http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-i.html. Kris is co-author of the leading treatise, J. Douglas Wilson & David Kris, *National Security Investigations and Prosecutions* (2007).

Fourth Amendment to the U.S. Constitution, the FISC is to issue an order directing the government to correct any deficiencies. § 702(i)(3).

As for its expansion of privacy protections, the FAA requires that the FISC approve surveillance of a U.S. citizen abroad based on a showing that includes a finding that the person is "an agent of a foreign power, or an officer or employee of a foreign power." Previously, FISA did not regulate surveillance of targets, whether U.S. citizens or not, when located outside the United States. The FAA also contains new mechanisms for congressional oversight and crafts new audit functions for the Inspector Generals of the Department Justice.

GLOBAL RELIEF FOUNDATION, INC. V. O'NEIL

207 F. Supp. 779 (N.D. Ill. 2002)

. . . [A]gents of the FBI arrived at the corporate headquarters of Global Relief [a U.S.-based Islamic humanitarian relief organization] and the home of its executive director on December 14, 2001 and seized a considerable amount of material they felt was relevant to their investigation of Global Relief's activities. As the defendants have conceded in their briefs, no warrant had been obtained before the FBI arrived either at Global Relief's headquarters or the executive director's residence. Nevertheless, FISA includes a provision which states that, when the Attorney General declares that "an emergency situation exists with respect to the execution of a search to obtain foreign intelligence information" prior to the Foreign Intelligence Surveillance Court acting on the application, a warrantless search is authorized. 50 U.S.C. § 1824(e)(1)(B)(i). When such an emergency situation arises, the government must submit a warrant application to the Foreign Intelligence Surveillance Court within 72 hours of the warrantless search for approval. *See* 50 U.S.C. § 1824(e). In this case, the failure of the FBI agents to present a FISA warrant on December 14 was caused by the Assistant Attorney General's declaration that an emergency situation existed with respect to the targeted documents and material. The defendants did submit a warrant application to the Foreign Intelligence Surveillance Court on December 15, as required by 50 U.S.C. § 1824(e). We have reviewed the warrant that issued and the submissions to the Foreign Intelligence Surveillance Court in support of that warrant.

We conclude that the FISA application established probable cause to believe that Global Relief and the executive director were agents of a foreign power, as that term is defined for FISA purposes, at the time the search was conducted and the application was granted. . . . Given the sensitive nature of the information upon which we have relied in making this determination and the Attorney General's sworn assertion that disclosure of the underlying information would harm national security, it would be improper for us to elaborate further on this subject.

This Court has concluded that disclosure of the information we have reviewed could substantially undermine ongoing investigations required to apprehend the conspirators behind the September 11 murders and undermine the ability of law enforcement agencies to reduce the possibility of terrorist crimes in the future. Furthermore, this Court is persuaded that the search and seizure made by the FBI on December 14 were authorized by FISA. Accordingly, we decline plaintiff's request that we declare the search invalid and order the immediate return of all items seized.

NOTES & QUESTIONS

1. ***Probable Cause.*** Searches under the Wiretap Act require a "super warrant," including a showing of probable cause that an individual has committed or is about to commit an enumerated offense. 18 U.S.C. § 2518(3). What is the required showing of probable cause for a FISA search? FISA requires a judicial finding, as the *O'Neill* case indicates, that probable cause exists to believe that the target is an agent of a foreign power. It also states that no U.S. person can be considered an agent of a foreign power based solely on First Amendment activities.
2. ***Defendants' Rights?*** In *Global Relief Foundation*, the court finds that disclosure of the information that it reviewed in deciding on the validity of the search was not to be revealed to the defendant because it "could substantially undermine ongoing investigations required to apprehend the conspirators behind the September 11 murders and undermine the ability of law enforcement agencies to reduce the possibility of terrorist crimes in the future." However, FISA requires that defendants receive notice about "any information obtained or derived from an electronic surveillance of that aggrieved person" pursuant to FISA when the government seeks to use information at trial or other official proceedings. 50 U.S.C. § 1806(c).
3. ***The Three* Keith *Categories.*** Recall the *Keith* Court's distinction between electronic surveillance in (1) criminal investigations; (2) domestic security investigations; and (3) investigations involving "activities of foreign powers and their agents." Today, ECPA regulates electronic surveillance in criminal investigations (category one above). The Foreign Intelligence Surveillance Act (FISA), as enacted in 1978, regulates electronic and other kinds of surveillance in cases involving foreign powers and their agents (category three).

   What then of the *Keith* category of "domestic security investigations" (category two)? Recall that the defendants in the underlying criminal proceeding were charged with a conspiracy to destroy government property. One of the defendants, for example, was charged with "the dynamite bombing" of a CIA office in Michigan. *Keith* makes it clear that it would be consistent with the Fourth Amendment for Congress to create different statutory requirements for issuing warrants for surveillance in cases involving domestic security. But Congress has not enacted such rules, and, as a consequence, law enforcement is required to carry out surveillance of criminal activities similar to those in *Keith* under the requirements of Title III and other parts of ECPA.
4. ***The Lone Wolf Amendment.*** The *Keith* categories and related rules remain unaltered by the "lone wolf" amendment to FISA in 2004. That year, Congress amended FISA to include any non-U.S. person who "engages in international terrorism or activities in preparation therefor" in the definition of "agent of a foreign power." The change means that the "lone wolf" terrorist need not be tied to a foreign power, but must be a non-U.S. person engaged in or plotting

"international terrorism." FISA defines "international terrorism" as involving, among other things, activities that "[o]ccur totally outside the U.S., or transcend national boundaries in terms of the means by which they accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum." 50 U.S.C. § 1801(c). As an illustration of the coverage of the "Lone Wolf" amendment, it would not cover Timothy McVeigh, the Oklahoma City bomber.

5. ***A New Agency for Domestic Intelligence?*** Francesca Bignami notes that in European countries, one governmental agency typically gathers intelligence on threats abroad posed by foreign governments, and another agency "is charged with gathering intelligence at home, on activities sponsored by foreign powers (counter-intelligence) as well as on home-grown security threats."[10] Both of these agencies are generally overseen not by judiciary, but by legislative and executive branches. Both intelligence agencies generally carry out surveillance under a more permissive set of legal rules than the domestic police. In contrast, in the United States, the FBI is charged with both domestic intelligence investigations and criminal investigations of violations of federal law.

Judge Richard Posner has emerged as the leading critic of the assignment of this double function to the FBI. He contends that the combination of criminal investigation and domestic intelligence at the FBI has not been successful: "If the incompatibility between the law enforcement and intelligence cultures is conceded, then it follows that an agency 100 percent dedicated to domestic intelligence would be likely to do a better job than the FBI, which is at most 20 percent intelligence and thus at least 80 percent criminal investigation and in consequence dominated by the criminal investigations."[11] Posner calls for creation of a "pure" domestic intelligence agency, one without any law enforcement responsibilities and located outside of the FBI. For Posner, the new U.S. Security Intelligence Surveillance can be modeled on the United Kingdom's MI5 or the Canadian Security Intelligence Service. What should the rules be for such a domestic intelligence agency concerning telecommunications surveillance? Should the FISA rules be applied to it?

UNITED STATES V. ISA

923 F.2d 1300 (8th Cir. 1991)

[The FBI obtained an order pursuant to FISA to bug the home of Zein Hassan Isa and his wife, Maria Matias. The FBI suspected Isa, a naturalized U.S. citizen, of being an agent of the Palestine Liberation Organization (PLO). One evening, the FBI's recording tapes of the bugged home captured Zein and Maria's murder of their 16-year-old daughter, Tina. Zein and Maria became angry at Tina's general rebelliousness and her defiance of their order not to date a particular young man. On the tape, Zein said to Tina: "Here, listen, my dear daughter, do you know that this is the last day? Tonight, you're going to die!" Tina responded in disbelief: "Huh?" Maria held Tina down while Zein stabbed her six times in the chest. While Tina screamed, Zein said: "Quiet, little one! Die my daughter, die!" The FBI turned the tapes over to the State of Missouri, where the Isas resided, where they were used to convict the Isas of murder. The Isas were sentenced to death.[12] Zein Isa argued that the recording should be suppressed because it captured events that had no relevance to the FBI's foreign intelligence gathering.]

[10] Francesca Bignami, *European versus American Liberty*, 48 B.C. L. Rev. 609, 621 (2007).

[11] Richard A. Posner, *Uncertain Shield* 101-02 (2006).

GIBSON, J. . . . [A]ppellant argues that his fourth amendment rights were violated because the government failed to comply with the minimization procedures defined in 50 U.S.C. § 1801(h). Specifically, he contends that the tapes turned over to the State of Missouri record a "private domestic matter," which is not relevant material under the Foreign Intelligence Surveillance Act and must therefore be destroyed. In support of this argument, he cites isolated sentences regarding required minimization procedures from the legislative history of the Foreign Intelligence Surveillance Act:

> Minimization procedures might also include restrictions on the use of surveillance to times when foreign intelligence information is likely to be obtained, ... [Furthermore, a target's] communications which are clearly not relevant to his clandestine intelligence activities should be destroyed. S. Rep. No. 95-701, 95th Cong., 2d Sess. 4.

Notwithstanding the minimization procedures required by [FISA], the Act specifically authorizes the retention of information that is "evidence of a crime," 50 U.S.C. § 1801(h)(3), and provides procedures for the retention and dissemination of such information. 50 U.S.C. § 1806(b)-(f). There is no requirement that the "crime" be related to foreign intelligence. . . .

Thus, we conclude that the tapes are "evidence of crime" and that the district court correctly denied appellant's motion to suppress. 50 U.S.C. § 1801(h)(3).

NOTES & QUESTIONS

1. ***Use of Information Obtained Through FISA Orders.*** As the *Isa* court notes, information obtained via FISA can be used in criminal trials. However, the standard to obtain a FISA order does not require probable cause. Is it appropriate to allow the use of evidence that would ordinarily required a warrant with probable cause to obtain? On the other hand, the FISA order in *Isa* was properly obtained, and the agents unexpectedly obtained evidence of a murder. If the order is obtained properly in good faith, and evidence of a crime is unexpectedly gathered, why should it be excluded from use in a criminal prosecution?
2. ***Minimization Procedures and Information Screening "Walls."*** As illustrated by *Isa,* FISA allows the use of information properly obtained under FISA to be used in a criminal prosecution. What prevents the government from using the often more lax standards of FISA to gather evidence in a criminal investigation?

[12] The Eighth Circuit opinion contains a very meager account of the facts on this case. The facts contained in this book are taken from *Terror and Death at Home Are Caught in F.B.I. Tape,* N.Y. Times, Oct. 28, 1991, at A14.

The standards of FISA are often much less stringent than those of ECPA. Government officials would merely need to say that they are conducting "intelligence gathering" and obtain a FISA order rather than an order under ECPA — and then, if they uncover evidence of a crime, they could use it to prosecute. FISA has some built-in protections against this. For example, it requires that "the purpose" of the surveillance be foreign intelligence gathering. This language was interpreted by courts as the "primary" purpose.

FISA requires that procedures be implemented to minimize the collection, retention, and dissemination of information about U.S. persons. § 1801(h)(1). Minimization procedures are designed to prevent the broad power of "foreign intelligence gathering" from being used for routine criminal investigations. In a number of instances, however, there are overlaps between foreign intelligence gathering and criminal investigations.

One common minimization procedure is what is known as an "information screening wall." With the "wall," an official not involved in the criminal investigation must review the raw materials gathered by FISA surveillance and only pass on information that might be relevant evidence. The wall is designed to prevent criminal justice personnel from initiating or directing the FISA surveillance. The wall does not prevent the sharing of information; rather, it prevents criminal prosecutors from becoming involved in the front end of the investigation rather than on the back end.

How should terrorism investigations, which involve both intelligence gathering and the collection of evidence for criminal prosecution, fit into this scheme?

2. THE USA PATRIOT ACT

THE 9/11 COMMISSION REPORT

Excerpt from pp. 254-75 (2004)

"The System Was Blinking Red"

As 2001 began, counterterrorism officials were receiving frequent but fragmentary reports about threats. Indeed, there appeared to be possible threats almost everywhere the United States had interests — including at home. . . .

Threat reports surged in June and July, reaching an even higher peak of urgency. The summer threats seemed to be focused on Saudi Arabia, Israel, Bahrain, Kuwait, Yemen, and possibly Rome, but the danger could be anywhere — including a possible attack on the G-8 summit in Genoa. . . .

A terrorist threat advisory distributed in late June indicated a high probability of near-term "spectacular" terrorist attacks resulting in numerous casualties. Other reports' titles warned, "Bin Ladin Attacks May Be Imminent" and "Bin Ladin and Associates Making Near-Term Threats." . . .

Most of the intelligence community recognized in the summer of 2001 that the number and severity of threat reports were unprecedented. Many officials told us that they knew something terrible was planned, and they were desperate to stop it.

Despite their large number, the threats received contained few specifics regarding time, place, method, or target. . . .

["Jane," an FBI analyst assigned to the FBI's investigation of the terrorist attack on the USS *Cole*] began drafting what is known as a lead for the FBI's New York Field Office. A lead relays information from one part of the FBI to another and requests that a particular action be taken. . . . [H]er draft lead was not sent until August 28. Her email told the New York agent that she wanted him to get started as soon as possible, but she labeled the lead as "Routine" — a designation that informs the receiving office that it has 30 days to respond.

The agent who received the lead forwarded it to his squad supervisor. That same day, the supervisor forwarded the lead to an intelligence agent to open an intelligence case — an agent who thus was behind "the wall" keeping FBI intelligence information from being shared with criminal prosecutors. He also sent it to the *Cole* case agents and an agent who had spent significant time in Malaysia searching for another Khalid: Khalid Sheikh Mohammad.

The suggested goal of the investigation was to locate Mihdhar, [a member of al Qaeda and a 9/11 hijacker] determine his contacts and reasons for being in the United States, and possibly conduct an interview. Before sending the lead, "Jane" had discussed it with "John," the CIA official on detail to the FBI. . . . The discussion seems to have been limited to whether the search should be classified as an intelligence investigation or as a criminal one. It appears that no one informed higher levels of management in either the FBI or CIA about the case. . . .

One of the *Cole* case agents read the lead with interest, and contacted "Jane" to obtain more information. "Jane" argued, however, that because the agent was designated a "criminal" FBI agent, not an intelligence FBI agent, the wall kept him from participating in any search for Mihdhar. In fact, she felt he had to destroy his copy of the lead because it contained NSA information from reports that included caveats ordering that the information not be shared without OIPR's permission. The agent asked "Jane" to get an opinion from the FBI's National Security Law Unit (NSLU) on whether he could open a criminal case on Mihdhar.

"Jane" sent an email to the *Cole* case agent explaining that according to the NSLU, the case could be opened only as an intelligence matter, and that if Mihdhar was found, only designated intelligence agents could conduct or even be present at any interview. She appears to have misunderstood the complex rules that could apply to this situation.

The FBI agent angrily responded:

> Whatever has happened to this — someday someone will die — and the wall or not — the public will not understand why we were not more effective at throwing every resource we had at certain "problems." . . .

"Jane" replied that she was not making up the rules; she claimed that they were in the relevant manual and "ordered by the [FISA] Court and every office of the FBI is required to follow them including FBI NY."

It is now clear that everyone involved was confused about the rules governing the sharing and use of information gathered in intelligence channels. Because Mihdhar was being sought for his possible connection to or knowledge of the *Cole* bombing, he could be investigated or tracked under the existing *Cole* criminal case. No new criminal case was need for the criminal agent to begin searching for

Mihdhar. And as NSA had approved the passage of its information to the criminal agent, he could have conducted a search using all available information. As a result of this confusion, the criminal agents who were knowledgeable about al Qaeda and experienced with criminal investigative techniques, including finding suspects and possible criminal charges, were thus excluded from the search. . . .

We believe that if more resources had been applied and a significantly different approach taken, Mihdhar and Hazmi might have been found. They had used their true names in the United States. Still, the investigators would have needed luck as well as skill to find them prior to September 11 even if such searches had begun as early as August 23, when the lead was first drafted.

Many FBI witnesses have suggested that even if Mihdhar had been found, there was nothing the agents could have done except follow him onto the planes. We believe this is incorrect. Both Hazmi and Mihdhar could have been held for immigration violations or as material witnesses in the *Cole* bombing case. Investigation or interrogation of them, and investigation of their travel and financial activities, could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise. . . .

On August 15, 2001, the Minneapolis FBI Field Office initiated an intelligence investigation on Zacarias Moussaoui. . . . [H]e had entered the United States in February 2001, and had begun flight lessons at Airman Flight School in Norman, Oklahoma. He resumed his training at the Pan Am International Flight Academy in Eagan, Minnesota, starting on August 13. He had none of the usual qualifications for light training on Pan Am's Boeing 747 flight simulators. He said he did not intend to become a commercial pilot but wanted the training as an "ego boosting thing." Moussaoui stood out because with little knowledge of flying, he wanted to learn to "take off and land" a Boeing 747.

The agent in Minneapolis quickly learned that Moussaoui possessed jihadist beliefs. Moreover, Moussaoui had $32,000 in a bank account but did not provide a plausible explanation for this sum of money. He traveled to Pakistan but became agitated when asked if he had traveled to nearby countries while in Pakistan. He planned to receive martial arts training, and intended to purchase a global positioning receiver. The agent also noted that Moussaoui became extremely agitated whenever he was questioned regarding his religious beliefs. The agent concluded that Moussaoui was "an Islamic extremist preparing for some future act in furtherance of radical fundamentalist goals." He also believed Moussaoui's plan was related to his flight training.

Moussaoui can be seen as an al Qaeda mistake and a missed opportunity. An apparently unreliable operative, he had fallen into the hands of the FBI. . . . If Moussaoui had been connected to al Qaeda, questions should instantly have arisen about a possible al Qaeda plot that involved piloting airliners, a possibility that had never been seriously analyzed by the intelligence community. . . .

As a French national who had overstayed his visa, Moussaoui could be detained immediately. The INS arrested Moussaoui on the immigration violation. A deportation order was signed on August 17, 2001.

The agents in Minnesota were concerned that the U.S. Attorney's office in Minneapolis would find insufficient probable cause of a crime to obtain a criminal warrant to search Moussaoui's laptop computer. Agents at FBI headquarters

believed there was insufficient probable cause. Minneapolis therefore sought a special warrant under the Foreign Intelligence Surveillance Act. . . .

To do so, however, the FBI needed to demonstrate probable cause that Moussaoui was an agent of a foreign power, a demonstration that was not required to obtain a criminal warrant but was a statutory requirement for a FISA warrant. The agent did not have sufficient information to connect Moussaoui to a "foreign power," so he reached out for help, in the United States and overseas. . .

[Based on information supplied by the French government, Moussaoui was linked to a rebel leader in Chechnya.] This set off a spirited debate between the Minneapolis Field Office, FBI headquarters, and the CIA as to whether Chechen rebels . . . were sufficiently associated with a terrorist organization to constitute a "foreign power" for purposes of the FISA statute. FBI headquarters did not believe this was good enough, and its National Security Law Unit declined to submit a FISA application. . . .

Although the Minneapolis agents wanted to tell the FAA from the beginning about Moussaoui, FBI headquarters instructed Minneapolis that it could not share the more complete report the case agent had prepared for the FAA. . . .

NOTES & QUESTIONS

1. ***Confusion About the Law Before 9/11.*** The 9/11 Commission Report excerpted above indicated that many law enforcement officials were confused about what FISA required and how information could be shared. The 9/11 Commission Report stated that the FBI headquarters concluded that Moussaoui's association with Chechen rebels was not adequate to justify a FISA order because Chechen rebels were not "sufficiently associated with a terrorist organization to constitute a 'foreign power' for purposes of the FISA statute." Does FISA require that a foreign power involve a terrorist organization? Consider the following excerpt from a Senate Report discussing the problems with the Moussaoui investigation:

> *First,* key FBI personnel responsible for protecting our country against terrorism did not understand the law. The SSA at FBI Headquarters responsible for assembling the facts in support of the Moussaoui FISA application testified before the Committee in a closed hearing that he did not know that "probable cause" was the applicable legal standard for obtaining a FISA warrant. In addition, he did not have a clear understanding of what the probable cause standard meant. . . . In addition to not understanding the probable cause standard, the SSA's supervisor (the Unit Chief) responsible for reviewing FISA applications did not have a proper understanding of the legal definition of the "agent of a foreign power" requirement.[13]

A footnote in the report explained that the FBI agent "was under the incorrect impression that the statute required a link to an already identified or 'recognized' terrorist organization, an interpretation that the FBI and the supervisor himself admitted was incorrect."

[13] Senate Report No. 108-040.

According to Senator Arlen Specter (R-PA), the consequences of this misunderstanding of law were grave:

> The failure to obtain a warrant under the Foreign Intelligence Surveillance Act for Zacarias Moussaoui was a matter of enormous importance, and it is my view that if we had gotten into Zacarias Moussaoui's computer, a treasure trove of connections to Al-Qeada, in combination with the FBI report from Phoenix where the young man with Osama bin Laden's picture seeking flight training, added to [the fact that] the CIA knew about two men who turned out to be terrorist pilots on 9/11 . . . there was a veritable blueprint and 9/11 might well have been prevented. . . .
>
> [I]n a way which was really incredulous, the FBI agents didn't know the standard. They didn't know it when they were dealing with the Moussaoui case, and they didn't know it almost a year later when we had the closed-door hearing.[14]

Does this indication regarding law enforcement confusion point to a need for changes in the law, changes in FBI training, or some other action?

2. ***What Did the FISA "Wall" Require?*** Since information validly obtained pursuant to a FISA court order can be used for criminal prosecution, the FISA "wall" prevented criminal enforcement officials from directing the implementation of FISA orders. Consider the following remarks by Jamie Gorelick, who was part of the 9/11 Commission:

> At last week's hearing, Attorney General John Ashcroft, facing criticism, asserted that "the single greatest structural cause for September 11 was the wall that segregated criminal investigations and intelligence agents" and that I built that wall through a March 1995 memo. This simply is not true.
>
> First, I did not invent the "wall," which is not a wall but a set of procedures implementing a 1978 statute (the Foreign Intelligence Surveillance Act, or FISA) and federal court decisions interpreting it. In a nutshell, that law, as the courts read it, said intelligence investigators could conduct electronic surveillance in the United States against foreign targets under a more lenient standard than is required in ordinary criminal cases, but only if the "primary purpose" of the surveillance were foreign intelligence rather than a criminal prosecution.
>
> Second, according to the FISA Court of Review, it was the justice departments under Presidents Ronald Reagan and George H.W. Bush in the 1980s that began to read the statute as limiting the department's ability to obtain FISA orders if it intended to bring a criminal prosecution. . . .
>
> [N]othing in the 1995 guidelines prevented the sharing of information between criminal and intelligence investigators. Indeed, the guidelines require that FBI foreign intelligence agents share information with criminal investigators and prosecutors whenever they uncover facts suggesting that a crime has been or may be committed. . . .[15]

According to Gorelick, why was the "wall" in place? What function did it serve? What precisely did it require?

---

[14] *The USA Patriot Act in Practice: Shedding Light on the FISA Process,* S. Hearing 107-947 (Sept. 10, 2002).

[15] Jamie S. Gorelick, *The Truth About "the Wall,"* Wash. Post, Apr. 18, 2004, at B7.

3. ***FISA and the USA PATRIOT Act.*** Prior to the USA PATRIOT Act, FISA applied when foreign intelligence gathering was "the purpose" of the investigation. Courts interpreted "the purpose" to mean that the primary purpose of the investigation had to be foreign intelligence gathering. Criminal enforcement could be a secondary purpose, but not the primary one. The USA PATRIOT Act, § 204, changed this language to make FISA applicable when foreign intelligence gathering is "a significant purpose" of the investigation. 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B). Why do you think that this change was made in the USA PATRIOT Act?

IN RE SEALED CASE

310 F.3d 717 (FIS Ct. Rev. 2002)

[In 2002, Attorney General John Ashcroft submitted to the FISA court new procedures for minimization, which significantly curtailed the screening walls. The procedures were reviewed by the FISA court in *In re All Matters Submitted to the Foreign Intelligence Surveillance Court* (May 17, 2002). The court expressed concern over the new procedures in light of the fact that in September 2000, the government had confessed error in about 75 FISA applications, including false statements that the targets of FISA surveillance were not under criminal investigations, that intelligence and criminal investigations were separate, and that information was not shared with FBI criminal investigators and assistant U.S. attorneys. The FISA court rejected the proposed procedures because they would allow criminal prosecutors to advise on FISA information gathering activities. The government appealed to the Foreign Intelligence Surveillance (FIS) Court of Review, which is composed of three judges on the D.C. Circuit. In 2002, the FIS Court of Review published its first and, thus far, only opinion.]

PER CURIAM. This is the first appeal from the Foreign Intelligence Surveillance Court to the Court of Review since the passage of the Foreign Intelligence Surveillance Act (FISA) in 1978. The appeal is brought by the United States from a FISA court surveillance order which imposed certain restrictions on the government. . . .

The court's decision from which the government appeals imposed certain requirements and limitations accompanying an order authorizing electronic surveillance of an "agent of a foreign power" as defined in FISA. There is no disagreement between the government and the FISA court as to the propriety of the electronic surveillance; the court found that the government had shown probable cause to believe that the target is an agent of a foreign power and otherwise met the basic requirements of FISA. . . . The FISA court authorized the surveillance, but imposed certain restrictions, which the government contends are neither mandated nor authorized by FISA. Particularly, the court ordered that law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division [of the Department of Justice] shall ensure that law enforcement officials do not direct or

control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.

To ensure the Justice Department followed these strictures the court also fashioned what the government refers to as a "chaperone requirement"; that a unit of the Justice Department, the Office of Intelligence Policy and Review (OIPR) (composed of 31 lawyers and 25 support staff), "be invited" to all meetings between the FBI and the Criminal Division involving consultations for the purpose of coordinating efforts "to investigate or protect against foreign attack or other grave hostile acts, sabotage, international terrorism, or clandestine intelligence activities by foreign powers or their agents." . . .

[The FISA court opinion below] appears to proceed from the assumption that FISA constructed a barrier between counterintelligence/intelligence officials and law enforcement officers in the Executive Branch — indeed, it uses the word "wall" popularized by certain commentators (and journalists) to describe that supposed barrier.

The "wall" emerges from the court's implicit interpretation of FISA. The court apparently believes it can approve applications for electronic surveillance only if the government's objective is *not* primarily directed toward criminal prosecution of the foreign agents for their foreign intelligence activity. But the court neither refers to any FISA language supporting that view, nor does it reference the Patriot Act amendments, which the government contends specifically altered FISA to make clear that an application could be obtained even if criminal prosecution is the primary counter mechanism.

Instead the court relied for its imposition of the disputed restrictions on its statutory authority to approve "minimization procedures" designed to prevent the acquisition, retention, and dissemination within the government of material gathered in an electronic surveillance that is unnecessary to the government's need for foreign intelligence information. 50 U.S.C. § 1801(h). . . .

. . . [I]t is quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents — even for foreign intelligence crimes. To be sure, section 1804, which sets forth the elements of an application for an order, required a national security official in the Executive Branch — typically the Director of the FBI — to certify that "the purpose" of the surveillance is to obtain foreign intelligence information (amended by the Patriot Act to read "a significant purpose"). But as the government now argues, the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism. Indeed, it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes, most importantly because, as we have noted, the definition of an agent of a foreign power — if he or she is a U.S. person — is grounded on criminal conduct. . . .

. . . In October 2001, Congress amended FISA to change "the purpose" language in § 1804(a)(7)(B) to "a significant purpose." It also added a provision allowing "Federal officers who conduct electronic surveillance to acquire foreign intelligence information" to "consult with Federal law enforcement officers to

coordinate efforts to investigate or protect against" attack or other grave hostile acts, sabotage or international terrorism, or clandestine intelligence activities, by foreign powers or their agents. 50 U.S.C. § 1806(k)(1). . . . Although the Patriot Act amendments to FISA expressly sanctioned consultation and coordination between intelligence and law enforcement officials, in response to the first applications filed by OIPR under those amendments, in November 2001, the FISA court for the first time adopted the 1995 Procedures, as augmented by the January 2000 and August 2001 Procedures, as "minimization procedures" to apply in all cases before the court.

The Attorney General interpreted the Patriot Act quite differently. On March 6, 2002, the Attorney General approved new "Intelligence Sharing Procedures" to implement the Act's amendments to FISA. The 2002 Procedures supersede prior procedures and were designed to permit the complete exchange of information and advice between intelligence and law enforcement officials. They eliminated the "direction and control" test and allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance." . . .

Unpersuaded by the Attorney General's interpretation of the Patriot Act, the court ordered that the 2002 Procedures be adopted, *with modifications,* as minimization procedures to apply in all cases. . . .

. . . [W]hen Congress explicitly authorizes consultation and coordination between different offices in the government, without even suggesting a limitation on who is to direct and control, it necessarily implies that either could be taking the lead. . . .

That leaves us with something of an analytic conundrum. On the one hand, Congress did not amend the definition of foreign intelligence information which, we have explained, includes evidence of foreign intelligence crimes. On the other hand, Congress accepted the dichotomy between foreign intelligence and law enforcement by adopting the significant purpose test. Nevertheless, it is our task to do our best to read the statute to honor congressional intent. The better reading, it seems to us, excludes from the purpose of gaining foreign intelligence information a sole objective of criminal prosecution. We therefore reject the government's argument to the contrary. Yet this may not make much practical difference. Because, as the government points out, when it commences an electronic surveillance of a foreign agent, typically it will not have decided whether to prosecute the agent (whatever may be the subjective intent of the investigators or lawyers who initiate an investigation). So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test.

The important point is — and here we agree with the government — the Patriot Act amendment, by using the word "significant," eliminated any justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses. If the certification of the application's purpose articulates a broader objective than criminal prosecution — such as stopping an ongoing conspiracy — and includes other potential non-prosecutorial responses, the government meets the statutory test. Of course, if the court concluded that the government's sole objective was merely to gain evidence of past criminal conduct — even foreign intelligence crimes — to

punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied. . . .

It can be argued, however, that by providing that an application is to be granted if the government has only a "significant purpose" of gaining foreign intelligence information, the Patriot Act allows the government to have a primary objective of prosecuting an agent for a non-foreign intelligence crime. Yet we think that would be an anomalous reading of the amendment. . . . That is not to deny that ordinary crimes might be inextricably intertwined with foreign intelligence crimes. For example, if a group of international terrorists were to engage in bank robberies in order to finance the manufacture of a bomb, evidence of the bank robbery should be treated just as evidence of the terrorist act itself. But the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes.

Having determined that FISA, as amended, does not oblige the government to demonstrate to the FISA court that its primary purpose in conducting electronic surveillance is *not* criminal prosecution, we are obliged to consider whether the statute as amended is consistent with the Fourth Amendment. . . . [I]n asking whether FISA procedures can be regarded as reasonable under the Fourth Amendment, we think it is instructive to compare those procedures and requirements with their Title III counterparts. Obviously, the closer those FISA procedures are to Title III procedures, the lesser are our constitutional concerns. . . .

With limited exceptions not at issue here, both Title III and FISA require prior judicial scrutiny of an application for an order authorizing electronic surveillance. 50 U.S.C. § 1805; 18 U.S.C. § 2518. And there is no dispute that a FISA judge satisfies the Fourth Amendment's requirement of a "neutral and detached magistrate."

The statutes differ to some extent in their probable cause showings. Title III allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines on the basis of the facts submitted in the government's application that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a specified predicate offense. 18 U.S.C. § 2518(3)(a). FISA by contrast requires a showing of probable cause that the target is a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(3). We have noted, however, that where a U.S. person is involved, an "agent of a foreign power" is defined in terms of criminal activity. . . . FISA surveillance would not be authorized against a target engaged in purely domestic terrorism because the government would not be able to show that the target is acting for or on behalf of a foreign power. . . .

FISA's general programmatic purpose, to protect the nation against terrorists and espionage threats directed by foreign powers, has from its outset been distinguishable from "ordinary crime control." After the events of September 11, 2001, though, it is hard to imagine greater emergencies facing Americans than those experienced on that date.

We acknowledge, however, that the constitutional question presented by this case — whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment — has no definitive jurisprudential answer.

. . . Our case may well involve the most serious threat our country faces. Even without taking into account the President's inherent constitutional authority to conduct warrantless foreign intelligence surveillance, we think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close.

NOTES & QUESTIONS

1. ***Assessing the Benefits and Problems of the "Wall."*** Paul Rosenzweig argues: "Prior to the Patriot Act, a very real wall existed. . . . While information could be 'thrown over the wall' from intelligence officials to prosecutors, the decision to do so always rested with national security personnel — even though law-enforcement agents are in a better position to determine what evidence is pertinent to their case."[16]

   Consider Peter Swire:

   > The principal argument [in favor of the wall] is that criminal prosecutions should be based on the normal rules of criminal procedure, not on evidence gathered in a secret court system. The norm should be the usual constitutional protections rather than the exceptional circumstances that arise in foreign intelligence investigations. . . .
   >
   > "[T]he wall" serves essential purposes. . . . [R]emoval of "the wall" may violate the Constitution for investigations that are primarily not for foreign intelligence purposes. At some point an investigation is so thoroughly domestic and criminal that the usual Fourth Amendment and other protections apply. . . . Second, "the wall" may be important in preventing the spread of the secret FISA system over time. As of 2002, seventy-one percent of the federal electronic surveillance orders were FISA orders rather than Title III orders. The Patriot Act reduction of safeguards in the FISA system means that this figure may climb in the future. . . .
   >
   > . . . [E]arly in an investigation, it may be difficult or impossible for investigators to know whether the evidence will eventually be used for intelligence purposes or in an actual prosecution. For instance, imagine that a FISA wiretap is sought for a group of foreign agents who are planning a bomb attack. On these facts, there would be a strong foreign intelligence purpose, to frustrate the foreign attack. In addition, there would be a strong law enforcement basis for surveillance, to create evidence that would prove conspiracy beyond a reasonable doubt. On these facts, it would be difficult for officials to certify honestly that "the primary purpose" of the surveillance was for foreign intelligence rather than law enforcement. The honest official might say that the surveillance has a dual use — both to create actionable foreign intelligence information and to create evidence for later prosecution.
   >
   > Faced with this possibility of dual use, the Patriot Act amendment was to require only that "a significant purpose" of the surveillance be for foreign intelligence. Under the new standard, an official could honestly affirm both a significant purpose for foreign intelligence and a likely use for law enforcement.

   Swire is troubled by the USA PATRIOT Act's changing FISA's requirement that "the purpose" of the investigation be foreign intelligence gathering to a looser requirement that "a significant purpose" of the investigation constituting foreign intelligence gathering:

[16] Paul Rosenzweig, *Civil Liberty and the Response to Terrorism,* 42 Duq. L. Rev. 663 (2004).

> The problem with the "significant purpose" standard, however, is that it allows too much use of secret FISA surveillance for ordinary crimes. The FISCR interpreted the new statute in a broad way: "So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test." The range of "realistic options" would seem to be so broad, however, that FISA orders could issue for an enormous range of investigations that ordinarily would be handled in the criminal system. . . . The Patriot Act amendment, as interpreted by the FISCR, thus allows the slippery slope to occur. A potentially immense range of law enforcement surveillance could shift into the secret FISA system.[17]

In lieu of the standard that "a significant purpose" of the investigation consists of foreign intelligence gathering, Swire recommends that FISA orders should be granted only if the surveillance is "sufficiently important for foreign intelligence purposes." Will Swire's proposed standard ("sufficiently important for foreign intelligence purposes") make a material difference from that of "a significant purpose"?

2. ***The Constitutionality of FISA and the Protect America Act.*** At the end of *In re Sealed Case,* the court concludes: "[W]e think the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close." Is coming close to meeting minimum warrant standards adequate enough to be constitutional?

Prior to the USA PATRIOT Act amendments, a few courts considered the constitutionality of FISA, with all concluding that the statute passed constitutional muster. For example, in *United States v. Duggan,* 743 F.2d 59 (2d Cir. 1984), the Second Circuit concluded that FISA did not violate the Fourth Amendment because

> [p]rior to the enactment of FISA, virtually every court that had addressed the issue had concluded that the President had the inherent power to conduct warrantless electronic surveillance to collect foreign intelligence information, and that such surveillances constituted an exception to the warrant requirement of the Fourth Amendment. The Supreme Court specifically declined to address this issue in *United States v. United States District Court,* but it had made clear that the requirements of the Fourth Amendment may change when differing governmental interests are at stake, and it observed . . . that the governmental interests presented in national security investigations differ substantially from those presented in traditional criminal investigations. . . .
>
> Against this background, Congress passed FISA to settle what it believed to be the unresolved question of the applicability of the Fourth Amendment warrant requirement to electronic surveillance for foreign intelligence purposes, and to "remove any doubt as to the lawfulness of such surveillance." . . .
>
> We regard the procedures fashioned in FISA as a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information. . . .

[17] Peter Swire, *The System of Foreign Intelligence Surveillance Law,* 72 Geo. Wash. L. Rev. 1306, 1342, 1360-65 (2004).

In 2008, the Foreign Intelligence Surveillance Court of Review (FISCR) upheld the constitutionality of the Protect America Act (PAA) of 2007, a stopgap law enacted before the FISA Amendment Act of 2008. *In re Directives [redacted text]*, 551 F.3d 1004 (FISCR 2008). The FISCR found that the PAA, applied through the relevant directives, satisfied the Fourth Amendment's reasonableness requirements. It observed, "The more important the government's interest, the greater the intrusion that may be constitutionally tolerated under the Fourth Amendment." Moreover, the PAA and accompanying directives provide safeguards, including "targeting procedures, minimization procedures, [and] a procedure to ensure that a significant purpose of a surveillance is to obtain foreign intelligence information." It concluded that "our decision recognizes that where the government has instituted several layers of serviceable safeguards to protect individuals against unwarranted harms and to minimize incidental intrusions, its effort to protect national security should not be frustrated by the courts."

Why should different Fourth Amendment requirements exist for foreign intelligence purposes as opposed to regular domestic law enforcement? Is the distinction between foreign intelligence and domestic law enforcement tenable in light of international terrorism, where investigations often have both a foreign intelligence and domestic law enforcement purpose? Do the USA PATRIOT Act amendments affect FISA's constitutionality?

3. ***After-the-Fact Reasonableness Review?*** In a critique of the FISA warrant-procedure as amended by the PATRIOT Act, a Note in the *Yale Law Journal* proposes that FISA be repealed and that the United States return to use of warrantless foreign intelligence surveillance in which "targets could challenge the reasonableness of the surveillance in an adversary proceeding in an Article III court after the surveillance was complete."[18]

Do you think that the foreign intelligence context is well suited to the proposed warrantless regime? For the Note, "the possibility of after-the-fact reasonableness review of the merits of their decisions in Article III courts (in camera or note) would help guarantee careful and calm DOJ decisionmaking." Is reasonableness a sufficiently strict standard of review? Furthermore, one of the hallmarks of the Fourth Amendment's warrant procedure is before-the-fact review; law enforcement officials must seek judicial authorization *before* they conduct their search. Would after-the-fact review result in hindsight bias? Another consideration is the extent to which warrantless surveillance would allow the government to "bootstrap" an investigation — the government could undertake broad, unregulated surveillance knowing that it could lead to evidence that may be admissible in court.

4. ***Stare Decisis.*** Many FISA court opinions remain secret; only some opinions are released. Jack Boeglin and Julius Taranto argue that the FISA courts "should publish any opinion that they consider binding precedent."[19] This action is needed because stare decisis is inconsistent with secret opinions. They

[18] Nola K. Breglio, Note, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 Yale L.J. 179, 203-04, 209, 212 (2003).

[19] Jack Boeglin & Julius Taranto, Comment, *Stare Decisis and Secret Law: On Precedent and Publication in the Foreign Intelligence Surveillance Court*, 124 Yale L.J. 2189 (2015).

argue that "Granting stare decisis value to secret opinions threatens to entrench legal precedent that has not been subject to the many direct and indirect benefits of public scrutiny." In their view, "Secrecy deprives FISA court judges of helpful external feedback from scholars, the public, and Congress." On the other hand, would the publication of all FISA court opinions harm national security by exposing sensitive security information?

5. ***The USA PATRIOT Act § 215.*** Section 215 of the USA PATRIOT Act adds a new § 501 to the Foreign Intelligence Surveillance Act (FISA):

> (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.
>
> (2) An investigation conducted under this section shall —
>
> (A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and
>
> (B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

Applications for court orders shall be made to a judge and "shall specify that the records are sought for an authorized investigation" and "to protect against international terrorism or clandestine intelligence activities." § 501(b). This section also has a gag order:

> (d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section. § 501(d).

The American Library Association (ALA) led a spirited campaign against § 215. It issued a resolution stating, in part, that

> the American Library Association encourages all librarians, library administrators, library governing bodies, and library advocates to educate their users, staff, and communities about the process for compliance with the USA PATRIOT Act and other related measures and about the dangers to individual privacy and the confidentiality of library records resulting from those measures.

In 2003, Attorney General John Ashcroft stated that § 215 had never been used to access library records. He further stated: "The fact is, with just 11,000 FBI agents and over a billion visitors to America's libraries each year, the Department of Justice has neither the staffing, the time nor the inclination to monitor the reading habits of Americans. . . . No offense to the American Library Association, but we just don't care." In 2005, the ALA revealed the results of a survey of librarians indicating a minimum of 137 formal law enforcement inquiries to library officials since 9/11, 49 of which were by federal officials and the remainder by

state and local officials. The study did not indicate whether any of these were pursuant to § 215.

The National Security Agency relied on § 215 of the USA PATRIOT Act as authorization for its collection of bulk telephone metadata. The existence of this secret program was first revealed through unauthorized disclosures of classified documents by Edward Snowden, a contractor for the NSA, in June 2013. This chapter addresses the NSA's telephone records program below.

3. NATIONAL SECURITY LETTERS

Provisions in several laws permit the FBI to obtain personal information from third parties merely by making a written request in cases involving national security. No court order is required. These requests are called "National Security Letters" (NSLs).

The Stored Communications Act. ECPA's Stored Communications Act contains an NSL provision, 18 U.S.C. § 2709. This provision allows the FBI to compel communications companies (ISPs, telephone companies) to release customer records when the FBI makes a particular certification. Before the USA PATRIOT Act, the FBI had to certify that the records were "relevant to an authorized foreign counterintelligence investigation" and that "there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801)."

Section 505 of the USA PATRIOT Act amended the National Security Letters provision of ECPA by altering what must be certified. The existing requirements regarding counterintelligence and specific and articulable facts that the target was an agent of a foreign power were deleted. The FBI now needs to certify that the records are "relevant to an authorized investigation to protect against terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." 18 U.S.C. § 2709.

This provision also has a gag order:

> No wire or electronic communication service provider, or officer, employee, or agent thereof, shall disclose to any person that the Federal Bureau of Investigation has sought or obtained access to information or records under this section. § 2709(c).

Unlike § 215, Ashcroft made no statement about § 505.[20]

The Right to Financial Privacy Act. The Right to Financial Privacy Act (RFPA) also contains an NSL provision. As amended by the Patriot Act, this provision states that the FBI can obtain an individual's financial records if it "certifies in writing to the financial institution that such records are sought for

[20] Mark Sidel, *More Secure, Less Free?: Antiterrorism Policy and Civil Liberties After September 11*, at 14 (2004).

foreign counter intelligence purposes to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States." 12 U.S.C. § 3414(a)(5)(A). As with the Stored Communications Act NSL provision, the RFPA NSL provision contains a "gag" rule prohibiting the financial institution from disclosing the fact it received the NSL. § 3414(a)(5)(D).

The Fair Credit Reporting Act. Likewise, the Fair Credit Reporting Act provides for NSLs. Pursuant to a written FBI request, consumer reporting agencies "shall furnish to the Federal Bureau of Investigation the names and addresses of all financial institutions . . . at which a customer maintains or has maintained an account." 15 U.S.C. § 1681u(a). Consumer reporting agencies must also furnish "identifying information respecting a consumer, limited to name, address, former addresses, places of employment, or former places of employment." 15 U.S.C. § 1681u(b). To obtain a full consumer report, however, the FBI must obtain a court order ex parte. 15 U.S.C. § 1681u(c). Like the other NSL provisions, the FCRA NSL provisions restrict NSLs for investigations based "solely" upon First Amendment activities. The FCRA NSL also has a "gag" rule. 15 U.S.C. § 1681u(d).

The USA PATRIOT Reauthorization Act. In the USA PATRIOT Reauthorization Act of 2005, Congress made several amendments that affected NSLs. It explicitly provided for judicial review of NSLs. It also required a detailed examination by the DOJ's Inspector General "of the effectiveness and use, including any improper or illegal use" of NSLs. This kind of audit proved its value in March 2006 when the Inspector General issued its review of the FBI's use of NSLs. First, the Inspector General found a dramatic underreporting of NSLs. Indeed, the total number of NSL requests between 2003 and 2005 totaled at least 143,074. Of these NSLs requests, as the Inspector General found, "[t]he overwhelming majority . . . sought telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transaction records under the ECPA NSL statute."[21]

The Inspector General also carried out a limited audit of investigative case files, and found that 22 percent of them contained at least one violation of investigative guidelines or procedures that was not reported to any of the relevant internal authorities at the FBI. Finally, the Inspector General also found over 700 instances in which the FBI obtained telephone records and subscriber information from telephone companies based on the use of a so-called "exigent letter" authority. This authority, absent from the statute, was invented by the FBI's Counterterrorism Division. Having devised this new power, the FBI did not set limits on its use, or track how it was employed. Witnesses told the Inspector General that many of these letters "were not issued in exigent circumstances, and the FBI was unable to determine which letters were sent in emergency circumstances due to inadequate recordkeeping." Indeed, "in most instances, there

[21] Office of the Inspector General, *A Review of the Federal Bureau of Investigations Use of National Security Letters* x-xiv (Mar. 2007).

was no documentation associating the requests with pending national security investigations."[22]

NSL Litigation. In *Doe v. Ashcroft*, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district court invalidated 18 U.S.C. § 2709 (*Doe I*). It found that § 2709 violated the Fourth Amendment because, at least as applied, it barred or at least substantially deterred a judicial challenge to an NSL request. It did so by prohibiting an NSL recipient from revealing the existence of an NSL inquiry. The court also found that the "all inclusive sweep" of § 2709 violated the First Amendment as a prior-restraint and content-based restriction on sweep that was subject to strict scrutiny review. Additionally, the court found that in some instances the use of an NSL might infringe upon people's First Amendment rights. For example, suppose that the FBI uses an NSL to find out the identity of an anonymous speaker on the Internet. Does the First Amendment limit using an NSL in this manner? Does the First Amendment restriction on the NSL provisions, which prohibits NSLs for investigations based "solely" upon First Amendment activities, adequately address these potential First Amendment problems?

Shortly after *Doe I,* another district court invalidated 18 U.S.C. § 2709(c), which prevented a recipient of an NSL to disclose information about the government's action. *Doe v. Gonzales*, 386 F. Supp. 2d 66, 82 (D. Conn. 2005) (*Doe II*).

While appeals in *Doe I* and *Doe II* were pending, Congress enacted the USA PATRIOT Reauthorization Act of 2005, which made several changes to § 2709 and added several provisions concerning judicial review of NSLs, which were codified at 18 U.S.C. § 3511. Following enactment of these provisions, plaintiffs challenged the amended nondisclosure provisions of §§ 2709(c) and 3511. The same district court that issued the *Doe I* opinion then found §§ 2709(c) and 3511(b) to be facially unconstitutional. *Doe v. Gonzales*, 500 F. Supp. 2d 379 (S.D.N.Y. 2007) (*Doe III*).

The newly enacted § 3511 provided for judicial review of NSLs. As a result, the *Doe III* plaintiffs did not challenge it on Fourth Amendment grounds as in *Doe I*. Instead, they argued, and the court agreed, that the nondisclosure provisions of § 2709(c) remained an unconstitutional prior restraint and content-based restriction on speech. The court also concluded that § 3511(b) was unconstitutional under the First Amendment and the doctrine of separation of powers. Among its conclusions, the court noted that Congress in amending § 2709(c) allowed the FBI to certify on a case-by-case basis whether nondisclosure was necessary. Yet, this narrowing of the statute to reduce the possibility of unnecessary limitation of speech also means that the FBI could conceivably engage in viewpoint discrimination. As a consequence, the amended statute was a content-based restriction as well as a prior restraint on speech and, therefore, subject to strict scrutiny.

The Second Circuit modified the district court's opinion. In *Doe v. Mukasey*, 549 F.3d 861 (2008), the court found that the challenged statutes did not comply with the First Amendment, although not to the extent that the district court found. It also concluded that the lower court's ordered relief was too broad. The Second

[22] *Id.* at xxxviii, xxxiv.

Circuit began by construing § 2709(c) to permit a nondisclosure requirement only when senior FBI officials certify that disclosure may result in an enumerated harm that is related to "an authorized investigation to protect against international terrorism or clandestine intelligence activities." It also interpreted § 3511(b)(2) and (b)(3) as placing the burden on the Government "to show that a good reason exists to expect that disclosure of receipt of an NSL will risk an enumerated harm." Additionally, it held the relevant subsections unconstitutional to the extent that they would impose a nondisclosure requirement without placing the burden on the government to initiate judicial review of that obligation, and to the extent that judicial review would treat "a government official's certification that disclosure may endanger the national security of the United States or interfere with diplomatic relations . . . as conclusive."

More recently, the Northern District of California declared NSLs to be unconstitutional due to the statute's nondisclosure and judicial review provisions. *In re: National Security Letter*, 930 F.Supp.2d 1064 (N.D. Cali 2013) found that the nondisclosure provisions represented a significant infringement on speech regarding controversial government powers that violated the First Amendment. The restrictions on judicial review violated the First Amendment as well as separation of powers principles. Given the significant constitutional and national security issues at stake, the district court judge stayed enforcement of the court's order. This decision is now on appeal to the Ninth Circuit as *In re: National Security Letter, Under Seal v. Holder*. Although the litigation is proceeding as a sealed matter, the Ninth Circuit has ordered various litigation documents to be made public and created a website devoted to the case due to the high level of interest in it.[23]

4. INTERNAL OVERSIGHT

Judicial oversight is not the only mechanism that regulates intelligence agencies. There are also several guidelines, internal governance structures and processes, privacy officials, and oversight boards that regulate the activities of various intelligence agencies.

(a) The Attorney General's FBI Guidelines

Unlike many government agencies, the FBI was not created by Congress through a statute. In 1907, Attorney General Charles Bonaparte requested that Congress authorize him to create a national detective force in the Department of Justice (DOJ). The DOJ had been using investigators from the Secret Service, but Bonaparte wanted a permanent force. Congress rejected his request due to concerns over this small group developing into a secret police system. Nevertheless, Bonaparte went ahead with his plans and formed a new subdivision of the DOJ, called the "Bureau of Investigation." President Theodore Roosevelt later authorized the subdivision through an executive order in 1908. J. Edgar

[23] *In re: National Security Letter, Under Seal v. Holder (Sealed)*, at http://www.ca9.uscourts.gov/content/view.php?pk_id=0000000715.

Hoover began running the Bureau, which was renamed the Federal Bureau of Investigation in 1935.[24]

The FBI grew at a great pace. In 1933, the FBI had 353 agents and 422 support staff; in 1945, it had 4,380 agents and 7,422 support staff.[25] Today, the FBI has 11,000 agents and 16,000 support staff, as well as 56 field offices, 400 satellite offices, and 40 foreign liaison posts.[26]

FBI surveillance activities are regulated through the U.S. Constitution and electronic surveillance laws, as well as by guidelines promulgated by the Attorney General. In 1976, responding to Hoover's abuses of power, Attorney General Edward Levi established guidelines to control FBI surveillance activities.[27] As William Banks and M.E. Bowman observe:

> The most pertinent Levi Guidelines focused on freedom of speech and freedom of the press. First, investigations based solely on unpopular speech, where there is no threat of violence, were prohibited. Second, techniques designed to disrupt organizations engaged in protected First Amendment activity, or to discredit individuals would not be used in any circumstance.
>
> At the same time, Attorney General Levi emphasized that the Guidelines were intended to permit domestic security investigations where the activities under investigation "involve or will involve the use of force or violence and the violation of criminal law." . . .
>
> On March 7, 1983, Attorney General William French Smith revised the Guidelines regarding domestic security investigations. . . .
>
> The Smith Guidelines were intended to increase the investigative avenues available to the FBI in domestic terrorism cases. Where the Levi/Civiletti Guidelines had established a predicate investigative standard of "specific and articulable facts," the Smith version lowered the threshold to require only a "reasonable indication" as the legal standard for opening a "full" investigation. . . . The "reasonable indication" standard is significantly lower than the Fourth Amendment standard of probable cause required in law enforcement. To balance the lowered threshold for opening an investigation, Attorney General Smith emphasized that investigations would be regulated and would "not be based solely on activities protected by the First Amendment or the lawful exercise of other rights secured by the Constitution."
>
> Nonetheless, the Smith Guidelines authorized FBI Headquarters to approve the use of informants to infiltrate a group "in a manner that may influence the exercise of rights protected by the First Amendment." The Smith Guidelines also stated: "In the absence of any information indicating planned violence by a group or enterprise, mere speculation that force or violence might occur during the course of an otherwise peaceable demonstration is not sufficient grounds for initiation of an investigation." . . .
>
> According to the criminal guidelines, a full investigation may be opened where there is "reasonable indication" that two or more persons are engaged in an enterprise for the purpose of furthering political or social goals wholly or in part

[24] Curt Gentry, *J. Edgar Hoover: The Man and the* Secrets 111-13 (1991).

[25] Ronald Kessler, *The Bureau: The Secret History of the FBI* 57 (2002).

[26] Federal Bureau of Investigation, Frequently Asked Questions, http://www.fbi.gov/aboutus/faqs/faqsone.html (Dec. 4, 2003).

[27] *See* United States Attorney General Guidelines on Domestic Security Investigation (1976).

> through activities that involve force or violence and are a violation of the criminal laws of the United States. . . .
>
> In order to determine whether an investigation should be opened, the FBI must also take into consideration the magnitude of the threat, the likelihood that the threat will come to fruition, and the immediacy of the jeopardy. In addition to physical danger, the FBI must consider the danger to privacy and free expression posed by an investigation. For example, unless there is a reasonable indication that force or violence might occur during the course of a demonstration, initiation of an investigation is not appropriate. . . .[28]

In 2002, Attorney General John Ashcroft issued revised FBI guidelines. Whereas under the preexisting guidelines, the FBI could engage in surveillance of public political activity and search the Internet when "facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed,"[29] Ashcroft's guidelines eliminate this requirement. The FBI is permitted to gather "publicly available information, whether obtained directly or through services or resources (whether nonprofit or commercial) that compile or analyze such information; and information voluntarily provided by private entities." The FBI can also "carry out general topical research, including conducting online searches and accessing online sites and forums."[30]

Daniel Solove argues that Congress should pass a legislative charter to regulate the FBI:

> . . . [E]xecutive orders and guidelines can all be changed by executive fiat, as demonstrated by Ashcroft's substantial revision to the guidelines in 2002. Moreover, the Attorney General Guidelines are not judicially enforceable. The problem with the current system is that it relies extensively on self-regulation by the executive branch. Much of this regulation has been effective, but it can too readily be changed in times of crisis without debate or discussion. Codifying the internal executive regulations of the FBI would also allow for public input into the process. The FBI is a very powerful arm of the executive branch, and if we believe in separation of powers, then it is imperative that the legislative branch, not the executive alone, become involved in the regulation of the FBI. The guidelines should be judicially enforceable to ensure that they are strictly followed.[31]

Should other government security agencies have more oversight? Does Solove overlook the FBI's internal administrative processes that serve to limit its power?

(b) The Homeland Security Act

In 2002, Congress passed the Homeland Security Act, 6 U.S.C. § 222, which consolidated 22 federal agencies into the Department of Homeland Security (DHS). Agencies and other major components at the DHS include the

[28] William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance,* 50 Am. U. L. Rev. 1, 69-74 (2000).

[29] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Domestic Security/Terrorism Investigations § II.C.1 (Mar. 21, 1989).

[30] The Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations § VI (May 30, 2002).

[31] Daniel J. Solove, *Reconstructing Electronic Surveillance Law,* 72 Geo. Wash. L. Rev. 1264, 1304 (2004).

Transportation Security Administration, Customs and Border Protection, Federal Emergency Management Agency, U.S. Citizenship and Immigration Services, U.S. Coast Guard, and U.S. Secret Service. The Office of the Secretary of DHS includes the Office of the Chief Privacy Officer, the Office of Civil Rights and Civil Liberties, the Office of Counter Narcotics, and the Office of State and Local Government Coordination.

Among other things, the Act creates a Privacy Office. 6 U.S.C. § 222. The Secretary must "appoint a senior official to assume primary responsibility for privacy policy." The privacy official's responsibilities include ensuring compliance with the Privacy Act of 1974; evaluating "legislative and regulatory proposals involving the collection, use, and disclosure of personal information by the Federal Government"; and preparing an annual report to Congress.

(c) The Intelligence Reform and Terrorism Prevention Act

Information Sharing and Institutional Culture. The 9/11 Commission found that in addition to the legal restrictions on sharing of foreign intelligence information, limitations in the FBI's institutional culture as well as technology had also prevented the circulation of data. In its final report, the 9/11 Commission stated: "The importance of integrated, all-source analysis cannot be overstated. Without it, it is not possible to 'connect the dots.' "[32] The 9/11 Commission called for a restructuring of the United States Intelligence Community (USIC) through creation of a National Intelligence Director to oversee this process.

In an Executive Order of August 27, 2004, President Bush required executive branch agencies to establish an environment to facilitate sharing of terrorism information.[33] Responding to the 9/11 Commission Report, Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRPTA), codifying the requirements in Bush's Executive Order. The Act mandates that intelligence be "provided in its most shareable form" that the heads of intelligence agencies and federal departments "promote a culture of information sharing."

The Long and Winding Road: The Creation of the Privacy and Civil Liberties Oversight Board. The IRTPA seeks to establish protection of privacy and civil liberties by setting up a five-member Privacy and Civil Liberties Oversight Board (PCLOB). The Board gives advice to the President and agencies of the executive branch and provides an annual report of activities to Congress. Among its oversight activities, the Board is to review whether "the information sharing practices of the departments, agencies, and elements of the executive branch . . . appropriately protect privacy and civil liberties." The Board is also to "ensure that privacy and civil liberties are appropriately considered in the development and implementation of . . . regulations and executive branch policies." Regarding FISA surveillance, IRTPA mandates that the Attorney General provide more detailed reporting to Congress on governmental surveillance practices and the government's legal interpretations of FISA.

[32] The 9/11 Commission Report 408 (2004).

[33] Exec. Order No. 13356, 69 Fed. Reg. 53,599, 53,600-01 (Sept. 1, 2004).

The Privacy and Civil Liberties Board has been the subject of controversy. A year after its creation, in February 2006, the Board still had not met a single time. When the Board issued its first annual report in May 2007, it led to the resignation of Lanny Davis, the Board's only Democratic member. The Bush Administration made more than 200 revisions to the report. The White House defending the actions as "standard operating procedure," and stated that it was appropriate because the board was legally under the President's supervision. In his resignation letter, Davis contested "the extensive redlining of the board's report to Congress by administration officials and the majority of the Board's willingness to accept most [of the edits.]"

Later that year, Congress enacted legislation to strengthen the independence and authority of the Board. It is now an "independent agency" located within the executive branch. No more than three members of the same political party can be appointed to the Board, and the Senate is to confirm all appointments to it. As before, however, the Board cannot issue subpoenas itself. Rather, a majority of Board members have the power to ask the Attorney General to issue a subpoena.[34]

Finally, in August 2012, the Senate confirmed the Board's four part-time members. The Senate confirmed David Medine, the Board's chairman and its only full-time member, in late May 2013. The timing was auspicious as it was five days before news stories began to appear based on Edward Snowden's leaked NSA documents. PCLOB has now issued semi-annual reports to Congress summarizing its initial activities as well as detailed studies of the NSA's telephone records program conduction under Section 214 of the PATRIOT Act and the NSA's surveillance program under Section 702 of the Foreign Intelligence Surveillance Act.[35] We discuss both NSA programs and the PCLOB reports below.

D. NSA SURVEILLANCE

In December 2005, a front page article in the *New York Times* first revealed that the National Security Agency (NSA) was intercepting communications where one party was located outside the United States and another party inside the United States.[36] The Bush Administration named this surveillance program the "Terrorist Surveillance Program" (TSP).

Created in 1952, the NSA collects and analyzes foreign communications. As Frederick Schwarz and Aziz Huq explain, "The NSA collects signals intelligence from telegrams, telephones, faxes, e-mails, and other electronic communications, and then disseminates this information among other agencies of the executive

[34] Ronald D. Lee & Paul M. Schwartz, *Beyond the "War on Terrorism": Towards the New Intelligence Network*, 103 Mich. L. Rev. 1446 (2005).

[35] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014); PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* (Jan. 23, 2014).

[36] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. Times, Dec. 16. 2005, at A1.

branch."[37] Schwarz and Huq also point out that the Church Committee investigation in 1975-76 found that "the NSA had not exercised its vast power with restraint or due regard for the Constitution." In the past, the NSA had engaged in activities such as collecting every international telegram sent from the United States and maintaining watch lists of U.S. citizens involved in political protests.

After 9/11, the NSA again began secret surveillance activities within the United States. Although the Bush Administration has discussed aspects of the NSA surveillance of telecommunications, the complete dimensions of the NSA activities remain unknown. And while the Department of Justice has issued a white paper justifying these activities,[38] the legal opinions said to declare the program lawful are secret.

Several lawsuits ensued, challenging the legality of the NSA surveillance. Some of these cases were brought against telecommunications companies that cooperated with the NSA in conducting the surveillance. Plaintiffs alleged that these companies violated FISA and ECPA.

Early in 2007, a secret FISC decision denied permission for certain NSA surveillance activities. The FISC judgment was said to concern a NSA request for a so-called "basket warrant," under which warrants are issued not on a case-by-case basis for specific suspects, but more generally for surveillance activity involving multiple targets. One anonymous official was quoted as saying that the FISC ruling concerned cases "where one end is foreign and you don't know where the other is."[39] The Administration leaked information about this ruling and argued that it impeded the government's ability to investigate threats of imminent terrorist attacks.

In the summer of 2007, Congress enacted the Protect America Act to authorize the NSA surveillance program.[40] This statute was subject to sunset in 120 days, and it expired without Congress enacting a new law or renewing it.[41] At that point, without the Protect America Act's amendments, the original FISA once again took effect, until Congress enacted FAA in July 2008.

A major roadblock to amending FISA had been the subject of immunity for the telecommunications companies that participated or participate in TSP or similar programs. President Bush stated that telecommunications immunity was needed to provide "meaningful liability protection to those who are alleged to have assisted our nation following the attacks of September 11, 2001." FISA already did contain immunity provisions, and this language was in effect at the time that the TSP began. *See* 18 U.S.C. § 2511(2)(a)(ii). The cooperation of the

[37] Frederick A.O. Schwarz Jr. & Aziz Z. Huq, *Unchecked and Unbalanced: Presidential Power in a Time of Terror* 127 (2007).

[38] United States Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (Jan. 19, 2006).

[39] Greg Miller, *Court Puts Limits on Surveillance Abroad*, L.A. Times, Aug. 2, 2007.

[40] The Protect America Act created an exception to FISA's requirements. The exception was found in the statute's § 105A. This part of the law exempted all communications "directed at" people outside of the United States from FISA's definition of "electronic surveillance." Once a communication fell within § 105A, the government could carry it out subject to § 105B and its requirements --- rather than FISA and its obligation to seek a warrant from the FISC.

[41] As discussed above, the Foreign Intelligence Surveillance Court of Review upheld the constitutionality of the PAA. *In re Directives [redacted text]*, 551 F.3d 1004 (FISCR 2008).

telecommunication companies with the NSA must have been outside the existing safe harbor language.

The FAA of 2008, discussed earlier in this chapter, establishes new rules for at least some of this NSA behavior. Title II of the FAA raises a new challenge to the litigation against the NSA behavior prior to its enactments — it provides statutory defenses for the telecommunications companies that assisted the NSA. Specifically, the FAA prohibits "a civil action" against anyone "for providing assistance to an element of the intelligence community" in connection "with an intelligence activity involving communications" following a specific kind of certification by the Attorney General. § 802. The certification in question requires a determination that the assistance was (1) authorized by the President during the period beginning on September 11, 2001 and ending on January 17, 2007; (2) designed to detect or prevent a terrorist attack; and (3) the subject of a written request from the Attorney General or the head of the intelligence community. A court presented with such a certificate is to review it for the support of "substantial evidence."

As noted above, the FAA of 2008 added a new provision, Section 702, to FISA, which permits the Attorney General and the Director of National Intelligence to jointly authorize surveillance conducted within the U.S. but targeting only non-U.S. persons reasonably believed to be located outside of the U.S. In *Clapper v. Amnesty International USA*, the Supreme Court deciding a standing issue that determined whether a challenge against Section 702 could be brought by "attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad."

1. STANDING

CLAPPER V. AMNESTY INTERNATIONAL USA

133 S. Ct. 1138 (2013)

ALITO, J. . . . Section 702 of the Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1881a, allows the Attorney General and the Director of National Intelligence to acquire foreign intelligence information by jointly authorizing the surveillance of individuals who are not "United States persons"[42] and are reasonably believed to be located outside the United States. Before doing so, the Attorney General and the Director of National Intelligence normally must obtain the Foreign Intelligence Surveillance Court's approval. Respondents are United States persons whose work, they allege, requires them to engage in sensitive international communications with individuals who they believe are likely targets of surveillance under § 1881a. Respondents seek a declaration that § 1881a is unconstitutional, as well as an injunction against §1881a-authorized surveillance.

42 The term "United States person" includes citizens of the United States, aliens admitted for permanent residence, and certain associations and corporations. 50 U.S.C. § 1801(i); see § 1881(a).

The question before us is whether respondents have Article III standing to seek this prospective relief.

Respondents assert that they can establish injury in fact because there is an objectively reasonable likelihood that their communications will be acquired under § 1881a at some point in the future. But respondents' theory of *future* injury is too speculative to satisfy the well-established requirement that threatened injury must be "certainly impending." And even if respondents could demonstrate that the threatened injury is certainly impending, they still would not be able to establish that this injury is fairly traceable to § 1881a. As an alternative argument, respondents contend that they are suffering *present* injury because the risk of § 1881a-authorized surveillance already has forced them to take costly and burdensome measures to protect the confidentiality of their international communications. But respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending. We therefore hold that respondents lack Article III standing.. . .

In 1978, after years of debate, Congress enacted the Foreign Intelligence Surveillance Act (FISA) to authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes. In enacting FISA, Congress legislated against the backdrop of our decision in *United States v. United States Dist. Court for Eastern Dist. of Mich.*, 407 U.S. 297 (1972) (*Keith*), in which we explained that the standards and procedures that law enforcement officials must follow when conducting "surveillance of 'ordinary crime' " might not be required in the context of surveillance conducted for domestic national-security purposes.

When Congress enacted the FISA Amendments Act of 2008 (FISA Amendments Act), it left much of FISA intact, but it "established a new and independent source of intelligence collection authority, beyond that granted in traditional FISA." As relevant here, § 702 of FISA, 50 U.S.C. § 1881a, which was enacted as part of the FISA Amendments Act, supplements pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting the communications of non-U.S. persons located abroad. Unlike traditional FISA surveillance, § 1881a does not require the Government to demonstrate probable cause that the target of the electronic surveillance is a foreign power or agent of a foreign power. And, unlike traditional FISA, § 1881a does not require the Government to specify the nature and location of each of the particular facilities or places at which the electronic surveillance will occur.

The present case involves a constitutional challenge to § 1881a. . . .

Respondents are attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad. Respondents believe that some of the people with whom they exchange foreign intelligence information are likely targets of surveillance under § 1881a. Specifically, respondents claim that they communicate by telephone and e-mail with people the Government "believes or believed to be associated with terrorist organizations," "people located in geographic areas that are a special focus" of the Government's counterterrorism or

targeting procedures, and minimization procedures—including assessing whether the targeting and minimization procedures comport with the Fourth Amendment. § 1881a(a), (c)(1), (i)(2), (i)(3). Any dissatisfaction that respondents may have about the Foreign Intelligence Surveillance Court's rulings—or the congressional delineation of that court's role—is irrelevant to our standing analysis.

Additionally, if the Government intends to use or disclose information obtained or derived from a § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition. §§ 1806(c), 1806(e), 1881e(a). . . .

Finally, any electronic communications service provider that the Government directs to assist in § 1881a surveillance may challenge the lawfulness of that directive before the FISC. § 1881a(h)(4), (6).

We hold that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm. We therefore reverse the judgment of the Second Circuit and remand the case for further proceedings consistent with this opinion.

BREYER, J. joined by GINSBURG, SOTOMAYOR, and KAGAN, JJ. dissenting. The plaintiffs' standing depends upon the likelihood that the Government, acting under the authority of 50 U.S.C. § 1881a will harm them by intercepting at least some of their private, foreign, telephone, or e-mail conversations. In my view, this harm is not "speculative." Indeed it is as likely to take place as are most future events that commonsense inference and ordinary knowledge of human nature tell us will happen. This Court has often found the occurrence of similar future events sufficiently certain to support standing. I dissent from the Court's contrary conclusion. . . .

. . . No one here denies that the Government's interception of a private telephone or e-mail conversation amounts to an injury that is "concrete and particularized." Moreover, the plaintiffs, respondents here, seek as relief a judgment declaring unconstitutional (and enjoining enforcement of) a statutory provision authorizing those interceptions; and, such a judgment would redress the injury by preventing it. Thus, the basic question is whether the injury, *i.e.,* the interception, is "actual or imminent."

Since the plaintiffs fear interceptions of a kind authorized by § 1881a, it is important to understand just what kind of surveillance that section authorizes. Congress enacted § 1881a in 2008, as an amendment to the pre-existing Foreign Intelligence Surveillance Act of 1978, 50 U.S.C. § 1801 *et seq*. Before the amendment, the Act authorized the Government (acting within the United States) to monitor private electronic communications between the United States and a foreign country if (1) the Government's purpose was, in significant part, to obtain foreign intelligence information (which includes information concerning a "foreign power" or "territory" related to our "national defense" or "security" or the "conduct of ... foreign affairs"), (2) the Government's surveillance target was "a foreign power or an agent of a foreign power," and (3) the Government used surveillance procedures designed to "minimize the acquisition and retention, and prohibit the dissemination, of" any private information acquired about Americans. §§ 1801(e), (h), 1804(a).

In addition the Government had to obtain the approval of the Foreign Intelligence Surveillance Court. To do so, it had to submit an application describing (1) each "specific target," (2) the "nature of the information sought," and (3) the "type of communications or activities to be subjected to the surveillance." § 1804(a). It had to certify that, in significant part, it sought to obtain foreign intelligence information. *Ibid.* It had to demonstrate probable cause to believe that each specific target was "a foreign power or an agent of a foreign power." §§ 1804(a), 1805(a). It also had to describe instance-specific procedures to be used to minimize intrusions upon Americans' privacy (compliance with which the court subsequently could assess). §§ 1804(a), 1805(d)(3).

The addition of § 1881a in 2008 changed this prior law in three important ways. First, it eliminated the requirement that the Government describe to the court each specific target and identify each facility at which its surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis. § 1881a(g). Second, it eliminated the requirement that a target be a "foreign power or an agent of a foreign power." *Ibid.* Third, it diminished the court's authority to insist upon, and eliminated its authority to supervise, instance-specific privacy-intrusion minimization procedures (though the Government still must use court-approved general minimization procedures). § 1881a(e). Thus, using the authority of § 1881a, the Government can obtain court approval for its surveillance of electronic communications between places within the United States and targets in foreign territories by showing the court (1) that "a significant purpose of the acquisition is to obtain foreign intelligence information," and (2) that it will use general targeting and privacy-intrusion minimization procedures of a kind that the court had previously approved. § 1881a(g).

Several considerations, based upon the record along with commonsense inferences, convince me that there is a very high likelihood that Government, *acting under the authority of § 1881a,* will intercept at least some of the communications just described. First, the plaintiffs have engaged, and continue to engage, in electronic communications of a kind that the 2008 amendment, but not the prior Act, authorizes the Government to intercept. These communications include discussions with family members of those detained at Guantanamo, friends and acquaintances of those persons, and investigators, experts and others with knowledge of circumstances related to terrorist activities. These persons are foreigners located outside the United States. They are not "foreign power[s]" or "agent[s] of ... foreign power [s]." And the plaintiffs state that they exchange with these persons "foreign intelligence information," defined to include information that "relates to" "international terrorism" and "the national defense or the security of the United States." See 50 U.S.C. § 1801.

Second, the plaintiffs have a strong *motive* to engage in, and the Government has a strong *motive* to listen to, conversations of the kind described. A lawyer representing a client normally seeks to learn the circumstances surrounding the crime (or the civil wrong) of which the client is accused. . . . Journalists and human rights workers have strong similar motives to conduct conversations of this kind.

At the same time, the Government has a strong motive to conduct surveillance of conversations that contain material of this kind. The Government, after all, seeks to learn as much as it can reasonably learn about suspected terrorists (such as those detained at Guantanamo), as well as about their contacts and activities, along with

those of friends and family members. And the Government is motivated to do so, not simply by the desire to help convict those whom the Government believes guilty, but also by the critical, overriding need to protect America from terrorism.

Third, the Government's *past behavior* shows that it has sought, and hence will in all likelihood continue to seek, information about alleged terrorists and detainees through means that include surveillance of electronic communications. As just pointed out, plaintiff Scott McKay states that the Government (under the authority of the pre-2008 law) "intercepted some 10,000 telephone calls and 20,000 email communications involving [his client] Mr. Al-Hussayen."

Fourth, the Government has the *capacity* to conduct electronic surveillance of the kind at issue. To some degree this capacity rests upon technology available to the Government. See 1 D. Kris & J. Wilson, National Security Investigations & Prosecutions § 16:6, p. 562 (2d ed. 2012) ("NSA's technological abilities are legendary"); *id.*, § 16:12, at 572-577 (describing the National Security Agency's capacity to monitor "*very* broad facilities" such as international switches). . . .

Of course, to exercise this capacity the Government must have intelligence court authorization. But the Government rarely files requests that fail to meet the statutory criteria. As the intelligence court itself has stated, its review under § 1881a is "narrowly circumscribed." In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, No. Misc. 08-01 (Aug. 17, 2008). There is no reason to believe that the communications described would all fail to meet the conditions necessary for approval. Moreover, compared with prior law, § 1881a simplifies and thus expedites the approval process, making it more likely that the Government will use § 1881a to obtain the necessary approval.

The upshot is that (1) similarity of content, (2) strong motives, (3) prior behavior, and (4) capacity all point to a very strong likelihood that the Government will intercept at least some of the plaintiffs' communications, including some that the 2008 amendment, § 1881a, but not the pre–2008 Act, authorizes the Government to intercept.

At the same time, nothing suggests the presence of some special factor here that might support a contrary conclusion. . . . One can, of course, always imagine some special circumstance that negates a virtual likelihood, no matter how strong. But the same is true about most, if not all, ordinary inferences about future events. Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical). But ordinarily a party that seeks to defeat a strong natural inference must bear the burden of showing that some such special circumstance exists. And no one has suggested any such special circumstance here. . . .

The majority more plausibly says that the plaintiffs have failed to show that the threatened harm is "*certainly impending*." But . . . *certainty* is not, and never has been, the touchstone of standing. The future is inherently uncertain. Yet federal courts frequently entertain actions for injunctions and for declaratory relief aimed at preventing future activities that are reasonably likely or highly likely, but not absolutely certain, to take place. And that degree of certainty is all that is needed to support standing here.

The Court's use of the term "certainly impending" is not to the contrary. Sometimes the Court has used the phrase "certainly impending" as if the phrase described a *sufficient,* rather than a *necessary,* condition for jurisdiction. See *Pennsylvania v. West Virginia,* 262 U.S. 553 (1923) ("If the injury is certainly impending that is enough"). . . . Taken together the case law uses the word "certainly" as if it emphasizes, rather than literally defines, the immediately following term "impending." . . .

In some standing cases, the Court has found that a reasonable probability of *future* injury comes accompanied with *present* injury that takes the form of reasonable efforts to mitigate the threatened effects of the future injury or to prevent it from occurring. Thus, in *Monsanto Co.*, plaintiffs, a group of conventional alfalfa growers, challenged an agency decision to deregulate genetically engineered alfalfa. Without expressing views about that probability, we found standing because the plaintiffs would suffer present harm by trying to combat the threat. *Ibid.* The plaintiffs, for example, "would have to conduct testing to find out whether and to what extent their crops have been contaminated." And they would have to take "measures to minimize the likelihood of potential contamination and to ensure an adequate supply of non-genetically-engineered alfalfa." *Ibid.* We held that these "harms, which [the plaintiffs] will suffer even if their crops are not actually infected with" the genetically modified gene, "are sufficiently concrete to satisfy the injury-in-fact prong of the constitutional standing analysis."

Virtually identical circumstances are present here. Plaintiff McKay, for example, points out that, when he communicates abroad about, or in the interests of, a client (*e.g.,* a client accused of terrorism), he must "make an assessment" whether his "client's interests would be compromised" should the Government "acquire the communications." If so, he must either forgo the communication or travel abroad. ("I have had to take measures to protect the confidentiality of information that I believe is particularly sensitive," including "travel that is both time-consuming and expensive").

Since travel is expensive, since forgoing communication can compromise the client's interests, since McKay's assessment itself takes time and effort, this case does not differ significantly from *Monsanto.* And that is so whether we consider the plaintiffs' present necessary expenditure of time and effort as a separate concrete, particularized, imminent harm, or consider it as additional evidence that the future harm (an interception) is likely to occur. . . .

While I express no view on the merits of the plaintiffs' constitutional claims, I do believe that at least some of the plaintiffs have standing to make those claims. I dissent, with respect, from the majority's contrary conclusion.

NOTES & QUESTIONS

1. ***The Holding in* Clapper.** By a 5-4 vote, the Clapper Court found a lack of standing. For the majority, the claimants were unable to demonstrate a future injury in fact that was "certainly impending" by allegations regarding likely government surveillance pursuant to Section 702. Writing in dissent, Justice Breyer argued that it was constitutionally justifiable to rely on "ordinary inferences about future events." He notes: "Perhaps, despite pouring rain, the streets will remain dry (due to the presence of a special chemical)." Indeed, at some point, a party that seeks to defeat a strong natural inference bears the burden of defeating it. In the national security context, how would you assess

the merit of requiring certainly impeding future harm, as the *Clapper* majority does, versus relying on certain "ordinary inferences," as Breyer would do?

2. ***The FISA Amendment Act and TSP.*** In *Hepting v. AT&T Corp.*, 439 F. Supp. 974 (N.D. Cal 2006), the plaintiffs alleged that AT&T was collaborating with the NSA in a massive warrantless surveillance program, namely, the TSP. As customers of AT&T, the plaintiffs alleged that they suffered injury from this surveillance.

   The *Hepting* court found that the existence of the TSP was itself not subject to the state secret privilege. This common law evidentiary privilege protects information from discovery when disclosure of it would harm national security. The *Hepting* court found that (1) the Bush Administration had disclosed "the general contours" of the TSP, which (2) "requires the assistance of a telecommunications provider," and (3) AT&T helps the government in classified matters when asked.

   This litigation ended, however, due to *In re NSA Telecommunications Records Litigation,* 633 F. Supp. 2d 949 (N.D. Cal. 2008). In that case, the district court found that the FISA Amendment Act had provided retroactive immunity for the defendants and dismissed the action. The court found that Congress in enacting the statute "manifested an unequivocal intention to create an immunity that will shield the telecommunications company defendants from liability in these actions."

   At the time of the debates around this law, Congress also considered laws that would have capped the possible liability exposure of the telecommunications companies at fairly modest amounts, but allow the litigation against them to proceed. Do you think that this approach would have been superior to the FISA Amendment Act's outright grant of immunity?

3. ***The End of FISA?*** William Banks argues: "At a minimum, the unraveling of FISA and emergence of the TSP call into question the virtual disappearance of effective oversight of our national security surveillance. The Congress and federal courts have become observers of the system, not even participants, much less overseers."[43] He proposes: "If FISA is to have any meaningful role for the next thirty years, its central terms will have to be restored, one way or another."

   In contrast, John Yoo argues that such surveillance should be permitted where there is a reasonable chance that terrorists will appear, or communicate, even if we do not know their specific identities. A law professor, Yoo was in government service at the time of the TSP and wrote the government memorandums at the Department of Justice's Office of Legal Counsel that approved the program.[44] Subsequently, he has proposed that in cases where there is a likelihood, perhaps "a 50 percent chance" that terrorists would use a certain kind of avenue for reaching each other, "[a] FISA-based approach

[43] William C. Banks, *The Death of FISA*, 91 Minn. L. Rev. 1209, 1297 (2007).

[44] For a discussion of Yoo's role, see *In re: National Security Telecommunications Records Litigation*, 2010 U.S. Dist. LEXIS 136156, *38-*40 (N.D. Cal. 2010)

would prevent computers from searching through that channel for keywords or names that might suggest terrorist communications."[45]

A third approach is proposed by Orin Kerr, who would update FISA beyond its current approach, which depends "on the identity and location of who is being monitored."[46] In contrast to this "person-focused" approach, Kerr would add "a complementary set of data-focused authorities" to the statute. Under this second approach, "Surveillance practices should be authorized when the government establishes a likelihood that surveillance would yield what I call 'terrorist intelligence information' — information relevant to terrorism investigations. . . ." Kerr is unwilling to state, however, whether the data-focused approach ("used when identities and/or location are unknown") should or should not require any kind of warrant.

2. THE SNOWDEN REVELATIONS

In June 2013, government contractor Edward Snowden began to leak classified National Security Agency (NSA) materials. This material appeared in the *Guardian* in the United Kingdom, the *Washington Post*, and other periodicals. Snowden revealed widespread NSA wiretapping and data collection previously unknown to the public. Senator Diane Feinstein called Snowden's action an "act of treason." A warrant was to be issued for his arrest. In contrast, Daniel Ellsberg, who leaked the Pentagon Papers, said, "there has not been in American history a more important leak" than Snowden's and praised his "civil courage." John Cassidy in the *New Yorker* called Snowden "a hero."[47] In that same periodical, Jeffrey Toobin called him "a grandiose narcissist who deserves to be in prison."[48]

The leaks have affected international relations through the disclosures of NSA spying in foreign nations. Snowden's actions have affected the ongoing development of the Proposed Data Protection Regulation at the European Union, led European Union officials to demand reforms to the Safe Harbor Agreement with the United States, and harmed U.S. technology companies seeking international business. Brazil's president called off a state dinner with President Obama, and Germany cancelled a Cold War surveillance cooperation agreement in reaction to revelations of NSA spying in their country. Germany's Chancellor, Angela Merkel, had a "strongly worded" conversation with President Obama about NSA surveillance of her cell phone.[49] At a European Summit in Brussels, Merkel said, "Spying between friends, that's just not done." She added: "Now trust has to be rebuilt."

What are the chief Snowden revelations in a nutshell? We can break the flood of information about the NSA into categories concerning (1) targeting of non-U.S. persons outside the United States through surveillance occurring in the United States (pursuant to Section 702 of FISA); (2) collecting telephone metadata

[45] John Yoo, *War By Other Means: An Insider's Accounts of the War on Terror* 112 (2006).

[46] Orin Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. Chi. L. Rev. 238 (2008).

[47] John Cassidy, *Why Edward Snowden is a Hero*, New Yorker (June 10, 2013).

[48] Jeffrey Toobin, *Edward Snowden is No Hero*, New Yorker (June 10, 2013).

[49] *Embassy Espionage: The NSA's Secret Hub in Berlin*, Der Spiegel (Oct. 13, 2013).

(pursuant to Section 215 of the Patriot Act); (3) spying on foreign countries and their leadership; and (4) acting to weaken encryption standards.

Surveillance of Non-U.S. Persons Outside the United States Conducted Within the United States (Section 702). As the President's Civil Liberties Oversight Board (PCLOB) notes, "Section 702 has its roots in the President's Surveillance Program developed in the immediate aftermath of the September 11th attacks."[50] Following the press disclosures about the Terrorist Surveillance Program in December 2005, the FISA Amendment Acts of 2008 added Section 702 to create a statutory framework for this collection program. Drawing on this section, the NSA then carried out a wide range of surveillance. In particular, and as PCLOB has explained, the NSA has drawn on Section 702 to carry out surveillance under its PRISM program and collection of so-called "upstream communications."

PRISM targets Internet communications and stored data of "non-US persons" outside the United States.[51] In PRISM collection, the government sends a "selector," such as an e-mail address, to a U.S.-based electronic service provider, such as an ISP, and the provider shares communications delivered to that "selector" with the government. PRISM collection does not include telephone calls. Susan Landau notes: "The PRISM documents mention 'direct access' to Microsoft, Yahoo, Google, Facebook, and other U.S. technology companies, but that might be a casual claim rather than a precise statement. Several of the companies involved clarified that this occurs only under legal process—and not through direct access at company servers."[52]

Under "upstream collection," acquisition occurs through the compelled assistance of providers that control the telecommunications backbone. "Upstream collection" also includes telephone calls as well as Internet communications.[53]

Telephone Metadata Collection (Section 215). Leaks by Snowden detailed the bulk collection of domestic telephony metadata. Section 215 of the PATRIOT Act allowed for the collection of individual suspects' "business records." The NSA broadened the scope of Section 215 to include all call detail records generated by certain telephone companies in the United States.[54] Although technically requiring FISC warrants, telephone companies generally complied voluntarily until news media reported on the practice in 2006.[55] Snowden's disclosures also revealed the existence of FISC orders authorizing this practice. Unlike a wiretap, metadata does not describe the content of a phone call, but rather the caller's location, call times

[50] PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 5 (July 2, 2014).

[51] Susan Landau, *Making Sense from Snowden: What's Significant in the NSA Surveillance Revelations*, 11:4 IEEE Security & Privacy 54, 54 (July/Aug. 2013).

[52] *Id.* at 58.

[53] PCLOB, *Report on the 702 Surveillance Program,* 7.

[54] For a clear description of the program and its history, see PCLOB, *Report on the Telephone Records Program Conducted Under Section 215* (Jan. 23, 2014).

[55] Landau, *Making Sense from Snowden, Part II*, IEE Security & Privacy Web Extra v (Jan./Feb. 2014). For a discussion of the Section 215 program, see Joseph D. Mornin, *NSA Metadata Collection and the Fourth Amendment*, 29 BTLJ 985 (2014).

and lengths, and which phone numbers the phone contacted. The NSA used metadata to understand webs of relations by "contact chaining" that compares groups of three "hops" from any "seed." In other words, government analysts would retrieve numbers not only directly in contact with the seed number (the "first hop'), but also numbers in contact with all first hop numbers (the "second hop") and all numbers in contact with all second hop numbers (the "third hop").[56]

Spying on China, G20 leaders, Brazil, Germany, and Other Countries. Snowden claimed that the NSA compromised Chinese telecommunications networks. With the help of the British GCHQ, the UK's NSA-equivalent, the NSA spied on G20 leaders during a 2009 summit in London. The NSA is also said to have spied on Petrobas, Brazil's largest oil and gas company. In Germany, the NSA targeted Chancellor's Merkel's cell phone and ran major listening operations from within the U.S. embassy in Berlin and U.S. military bases throughout the company. In France, initial reports of widespread NSA-spying in that country were followed by reports in *Le Monde* that the activity had been carried out with the cooperation of French intelligence agencies.

Weakening of Encryption Standards. Leaked documents from Snowden showed that the NSA worked to insert vulnerabilities into commercial encryption standards. It did so to make these systems "exploitable" by it. As part of this effort, the NSA covertly influenced the standard-setting process at the National Institute of Standards and Technology. As Susan Landau states, "It appears that NSA [...] viewed corrupting cryptography standards as a goal."[57]

In the two cases that follow, *Klayman v. Obama* and *In re FBI*, a district court and the FISC respectively evaluated the legal sufficiency of Section 215.

KLAYMAN V. OBAMA
957 F. Supp. 2d 1 (D.D.C. 2013)

LEON, J. On June 6, 2013, plaintiffs brought the first of two related lawsuits challenging the constitutionality and statutory authorization of certain intelligence-gathering practices by the United States government relating to the wholesale collection of the phone record metadata of all U.S. citizens. These related cases are two of several lawsuits arising from public revelations over the past six months that the federal government, through the National Security Agency ("NSA"), and with the participation of certain telecommunications and internet companies, has conducted surveillance and intelligence-gathering programs that collect certain data about the telephone and internet activity of American citizens within the United States.

On June 5, 2013, the British newspaper *The Guardian* reported the first of several "leaks" of classified material from Edward Snowden, a former NSA contract employee, which have revealed — and continue to reveal — multiple U.S.

[56] PCLOB, *Telephone Records Program*, *supra*, 9.

[57] *Id.* at vii.

government intelligence collection and surveillance programs. *See* Glenn Greenwald, *NSA collecting phone records of millions of Verizon customers daily,* GUARDIAN (London), June 5, 2013. That initial media report disclosed a FISC order dated April 25, 2013, compelling Verizon Business Network Services to produce to the NSA on "an ongoing daily basis ... all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." Secondary Order, *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on Behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services, No. BR 13–80* at 2 (FISC Apr. 25, 2013). According to the news article, this order "show[ed] . . . that under the Obama administration the communication records of millions of US citizens are being collected indiscriminately and in bulk—regardless of whether they are suspected of any wrongdoing." Greenwald, *supra.* In response to this disclosure, the Government confirmed the authenticity of the April 25, 2013 FISC Order, and, in this litigation and in certain public statements, acknowledged the existence of a "program" under which "the FBI obtains orders from the FISC pursuant to Section 215 [of the USA PATRIOT Act] directing certain telecommunications service providers to produce to the NSA on a daily basis electronic copies of 'call detail records.'" Follow-on media reports revealed other Government surveillance programs, including the Government's collection of internet data pursuant to a program called "PRISM." *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism program taps in to user data of Apple, Google and others,* GUARDIAN (London), June 6, 2013. . . .

FISA created a procedure for the Government to obtain ex parte judicial orders authorizing domestic electronic surveillance upon a showing that, *inter alia,* the target of the surveillance was a foreign power or an agent of a foreign power. 50 U.S.C. §§ 1804(a)(3), 1805(a)(2). In enacting FISA, Congress also created two new Article III courts—the Foreign Intelligence Surveillance Court ("FISC"), composed of eleven U.S. district judges, "which shall have jurisdiction to hear applications for and grant orders approving" such surveillance, § 1803(a)(1), and the FISC Court of Review, composed of three U.S. district or court of appeals judges, "which shall have jurisdiction to review the denial of any application made under [FISA]," § 1803(b).

Following the September 11, 2001 terrorist attacks, Congress passed the USA PATRIOT Act, which made changes to FISA and several other laws. Pub. L. No. 107–56, 115 Stat. 272 (2001). Section 215 of the PATRIOT Act replaced FISA's business-records provision with a more expansive "tangible things" provision. Codified at 50 U.S.C. § 1861, it authorizes the FBI to apply "for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." § 1861(a)(1). While this provision originally required that the FBI's application "shall specify that the records concerned are sought for" such an investigation, § 1861(b)(2), Congress amended the statute in 2006 to provide that the FBI's application must include "a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation ... to obtain

foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." § 1861(b)(2)(A); *see* USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109–177, § 106(b), 120 Stat. 192 ("USA PATRIOT Improvement and Reauthorization Act").

Section 1861 also imposes other requirements on the FBI when seeking to use this authority. For example, the investigation pursuant to which the request is made must be authorized and conducted under guidelines approved by the Attorney General under Executive Order No. 12,333 (or a successor thereto). 50 U.S.C. § 1861(a)(2)(A), (b)(2)(A). And the FBI's application must "enumerat[e] . . . minimization procedures adopted by the Attorney General . . . that are applicable to the retention and dissemination by the [FBI] of any tangible things to be made available to the [FBI] based on the order requested." § 1861(b)(2)(B). . . .

While the recipient of a production order must keep it secret, Section 1861 does provide the recipient — but only the recipient — a right of judicial review of the order before the FISC pursuant to specific procedures. Prior to 2006, recipients of Section 1861 production orders had no express right to judicial review of those orders, but Congress added such a provision when it reauthorized the PATRIOT Act that year.

To say the least, plaintiffs and the Government have portrayed the scope of the Government's surveillance activities very differently. For purposes of resolving these preliminary injunction motions, however, as will be made clear in the discussion below, it will suffice to accept the Government's description of the phone metadata collection and querying program.

In broad overview, the Government has developed a "counterterrorism program" under Section 1861 in which it collect, compiles, retains, and analyzes certain telephone records, which it characterizes as "business records" created by certain telecommunications companies (the "Bulk Telephony Metadata Program"). The records collected under this program consist of "metadata," such as information about what phone numbers were used to make and receive calls, when the calls took place, and how long the calls lasted. According to the representations made by the Government, the metadata records collected under the program do *not* include *any* information about the content of those calls, or the names, addresses, or financial information of any party to the calls. Through targeted computerized searches of those metadata records, the NSA tries to discern connections between terrorist organizations and previously unknown terrorist operatives located in the United States.

The Government has conducted the Bulk Telephony Metadata Program for more than seven years. Beginning in May 2006 and continuing through the present,[58] the FBI has obtained production orders from the FISC under Section 1861 directing certain telecommunications companies to produce, on an ongoing daily basis, these telephony metadata records, which the companies create and maintain as part of their business of providing telecommunications services to customers. The NSA then consolidates the metadata records provided by different

[58] The most recent FISC order authorizing the Bulk Telephony Metadata Program that the Government has disclosed (in redacted form, directed to an unknown recipient) expires on January 3, 2014. *See* Oct. 11, 2013 Primary Order at 17.

telecommunications companies into one database, and under the FISC's orders, the NSA may retain the records for up to five years. According to Government officials, this aggregation of records into a single database creates "an historical repository that permits retrospective analysis," enabling NSA analysts to draw connections, across telecommunications service providers, between numbers reasonably suspected to be associated with terrorist activity and with other, unknown numbers.

The FISC orders governing the Bulk Telephony Metadata Program specifically provide that the metadata records may be accessed only for counterterrorism purposes (and technical database maintenance). Specifically, NSA intelligence analysts, *without seeking the approval of a judicial officer,* may access the records to obtain foreign intelligence information only through "queries" of the records performed using "identifiers," such as telephone numbers, associated with terrorist activity. An "identifier" (i.e., selection term, or search term) used to start a query of the database is called a "seed," and "seeds" must be approved by one of twenty-two designated officials in the NSA's Homeland Security Analysis Center or other parts of the NSA's Signals Intelligence Directorate. Such approval may be given only upon a determination by one of those designated officials that there exist facts giving rise to a "reasonable, articulable suspicion" ("RAS") that the selection term to be queried is associated with one or more of the specified foreign terrorist organizations approved for targeting by the FISC. In 2012, for example, fewer than 300 unique identifiers met this RAS standard and were used as "seeds" to query the metadata, but "the number of unique identifiers has varied over the years."

When an NSA intelligence analyst runs a query using a "seed," the minimization procedures provide that query results are limited to records of communications within three "hops" from the seed. The query results thus will include only identifiers and their associated metadata having a direct contact with the seed (the first "hop"), identifiers and associated metadata having a direct contact with first "hop" identifiers (the second "hop"), and identifiers and associated metadata having a direct contact with second "hop" identifiers (the third "hop"). In plain English, this means that if a search starts with telephone number (123) 456–7890 as the "seed," the first hop will include all the phone numbers that (123) 456–7890 has called or received calls from in the last five years (say, 100 numbers), the second hop will include all the phone numbers that each of *those* 100 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 100 "first hop" numbers, or 10,000 total), and the third hop will include all the phone numbers that each of *those* 10,000 numbers has called or received calls from in the last five years (say, 100 numbers for each one of the 10,000 "second hop" numbers, or 1,000,000 total). The actual number of telephone numbers and their associated metadata captured in any given query varies, of course, but in the absence of any specific representations from the Government about typical query results, it is likely that the quantity of phone numbers captured in any given query would be very large.

Once a query is conducted and it returns a universe of responsive records (i.e., a universe limited to records of communications within three hops from the seed), trained NSA analysts may then perform new searches and otherwise perform intelligence analysis *within* that universe of data without using RAS-approved

search terms. According to the Government, following the "chains of communication" — which, for chains that cross different communications networks, is only possible if the metadata is aggregated—allows the analyst to discover information that may not be readily ascertainable through other, targeted intelligence-gathering techniques. For example, the query might reveal that a seed telephone number has been in contact with a previously unknown U.S. telephone number — i.e., on the first hop. And from there, "contact-chaining" out to the second and third hops to examine the contacts made by that telephone number may reveal a contact with other telephone numbers already known to the Government to be associated with a foreign terrorist organization. In short, the Bulk Telephony Metadata Program is meant to detect: (1) domestic U.S. phone numbers calling *outside* of the U.S. to foreign phone numbers associated with terrorist groups; (2) foreign phone numbers associated with terrorist groups calling *into* the U.S. to U.S. phone numbers; and (3) "possible terrorist-related communications" between U.S. phone numbers *inside* the U.S. . . .

When ruling on a motion for preliminary injunction, a court must consider "whether (1) the plaintiff has a substantial likelihood of success on the merits; (2) the plaintiff would suffer irreparable injury were an injunction not granted; (3) an injunction would substantially injure other interested parties; and (4) the grant of an injunction would further the public interest." *Sottera, Inc. v. Food & Drug Admin.,* 627 F.3d 891, 893 (D.C. Cir. 2010) (internal quotation marks omitted). I will address each of these factors in turn.

In addressing plaintiffs' likelihood of success on the merits of their constitutional claims, I will focus on their Fourth Amendment arguments, which I find to be the most likely to succeed. First, however, I must address plaintiffs' standing to challenge the various aspects of the Bulk Telephony Metadata Program.

"To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Clapper v. Amnesty Int'l USA,* 133 S. Ct. 1138 (2013) (internal quotation marks omitted). In *Clapper,* the Supreme Court held that plaintiffs lacked standing to challenge NSA surveillance under FISA because their "highly speculative fear" that they would be targeted by surveillance relied on a "speculative chain of possibilities" insufficient to demonstrate a "certainly impending" injury. Moreover, the *Clapper* plaintiffs' "self-inflicted injuries" (i.e., the costs and burdens of avoiding the feared surveillance) could not be traced to any provable government activity.[59] That is not the case here.

The NSA's Bulk Telephony Metadata Program involves two potential searches: (1) the bulk collection of metadata and (2) the analysis of that data

[59] I note in passing one significant difference between the metadata collection at issue in this case and the electronic surveillance at issue in *Clapper.* As the Court noted in *Clapper,* "if the Government intends to use or disclose information obtained or derived from a [50 U.S.C.] § 1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition." 133 S. Ct. at 1154 (citing 50 U.S.C. §§ 1806(c), 1806(e), 1881e(a)). Sections 1806(c) and (e) and 1881e(a), however, apply only to "information obtained or derived from an electronic surveillance" authorized by specific statutes; they do *not* apply to business records collected under Section 1861. Nor does it appear that any other statute requires the Government to notify a criminal defendant if it intends to use evidence derived from an analysis of the bulk telephony metadata collection.

through the NSA's querying process. For the following reasons, I have concluded that the plaintiffs have standing to challenge both. First, as to the collection, the Supreme Court decided *Clapper* just months *before* the June 2013 news reports revealed the existence and scope of certain NSA surveillance activities. Thus, whereas the plaintiffs in *Clapper* could only speculate as to whether they would be surveilled at all, plaintiffs in this case can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention. In addition, the Government has declassified and authenticated an April 25, 2013 FISC Order signed by Judge Vinson, which confirms that the NSA has indeed collected telephony metadata from Verizon.

. . . [I]n one footnote, the Government asks me to find that plaintiffs lack standing based on the theoretical possibility that the NSA has collected a universe of metadata so incomplete that the program could not possibly serve its putative function.[60] Candor of this type defies common sense and does not exactly inspire confidence!

Likewise, I find that plaintiffs also have standing to challenge the NSA's querying procedures. . . . When the NSA runs such a query, its system must necessarily analyze metadata for *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the target number. Moreover, unlike a DNA or fingerprint database — which contains only a single "snapshot" record of each person therein — the NSA's database is updated every single day with new information about each phone number. And the NSA can access its database whenever it wants, repeatedly querying any seed approved in the last 180 days (for terms believed to be used by U.S. persons) or year (for all other terms).

The threshold issue that I must address . . . is whether plaintiffs have a reasonable expectation of privacy that is violated when the Government indiscriminately collects their telephony metadata along with the metadata of hundreds of millions of other citizens without any particularized suspicion of wrongdoing, retains all of that metadata for five years, and then queries, analyzes, and investigates that data without prior judicial approval of the investigative targets. If they do — and a Fourth Amendment search has thus occurred — then the next step of the analysis will be to determine whether such a search is "reasonable."

The analysis of this threshold issue of the expectation of privacy must start with the Supreme Court's landmark opinion in *Smith v. Maryland,* 442 U.S. 735 (1979), which the FISC has said "squarely control[s]" when it comes to "[t]he production of telephone service provider metadata." Am. Mem. Op., *In re Application of the [FBI] for an Order Requiring the Production of Tangible Things from [REDACTED],* No. BR 13–109 at 6–9 (FISC Aug. 29, 2013).

The question before me is *not* the same question that the Supreme Court confronted in *Smith.* To say the least, "whether the installation and use of a pen

[60] To draw an analogy, if the NSA's program operates the way the Government suggests it does, then omitting Verizon Wireless, AT & T, and Sprint from the collection would be like omitting John, Paul, and George from a historical analysis of the Beatles. A Ringo-only database doesn't make any sense, and I cannot believe the Government would create, maintain, and so ardently defend such a system.

register constitutes a 'search' within the meaning of the Fourth Amendment," *id.* at 736, under the circumstances addressed and contemplated in that case — is a far cry from the issue in this case.

Indeed, the question in this case can more properly be styled as follows: When do present-day circumstances — the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies — become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply? The answer, unfortunately for the Government, is now.

In *United States v. Jones* (2012), five justices found that law enforcement's use of a GPS device to track a vehicle's movements for nearly a month violated Jones's reasonable expectation of privacy. Significantly, the justices did so *without* questioning the validity of the Court's earlier decision in *United States v. Knotts,* 460 U.S. 276 (1983), that use of a tracking beeper does not constitute a search because "[a] person travelling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another." Instead, they emphasized the many significant ways in which the short-range, short-term tracking device used in *Knotts* differed from the constant month-long surveillance achieved with the GPS device attached to Jones's car.

Just as the Court in *Knotts* did not address the kind of surveillance used to track Jones, the Court in *Smith* was not confronted with the NSA's Bulk Telephony Metadata Program.[61] Nor could the Court in 1979 have ever imagined how the citizens of 2013 would interact with their phones. For the many reasons discussed below, I am convinced that the surveillance program now before me is so different from a simple pen register that *Smith* is of little value in assessing whether the Bulk Telephony Metadata Program constitutes a Fourth Amendment search. To the contrary, for the following reasons, I believe that bulk telephony metadata collection and analysis almost certainly does violate a reasonable expectation of privacy.

First, the pen register in *Smith* was operational for only a matter of days between March 6, 1976 and March 19, 1976, and there is no indication from the Court's opinion that it expected the Government to retain those limited phone records once the case was over. . . . The NSA telephony metadata program, on the other hand, involves the creation and maintenance of a historical database containing *five years'* worth of data. And I might add, there is the very real prospect that the program will go on for as long as America is combatting terrorism, which realistically could be forever!

Second, the relationship between the police and the phone company in *Smith* is *nothing* compared to the relationship that has apparently evolved over the last seven years between the Government and telecom companies. . . . It's one thing to say that people expect phone companies to occasionally provide information to law enforcement; it is quite another to suggest that our citizens expect all phone companies to operate what is effectively a joint intelligence-gathering operation

[61] . . . The Supreme Court itself has recognized that prior Fourth Amendment precedents and doctrines do not always control in cases involving unique factual circumstances created by evolving technology. *See, e.g., Kyllo,* 533 U.S. at 34 ("To withdraw protection of this minimum expectation [of privacy in the home] would be to permit police technology to erode the privacy guaranteed by the Fourth Amendment."). If this isn't such a case, then what is?

with the Government. *Cf. U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press,* 489 U.S. 749 (1989) ("Plainly there is a vast difference between the public records that might be found after a diligent search of [various third parties' records] and a computerized summary located in a single clearinghouse of information.").

Third, the almost-Orwellian technology that enables the Government to store and analyze the phone metadata of every telephone user in the United States is unlike anything that could have been conceived in 1979. In *Smith,* the Supreme Court was actually considering whether local police could collect one person's phone records for calls made after the pen register was installed and for the limited purpose of a small-scale investigation of harassing phone calls. *See Smith,* 442 U.S. at 737. The notion that the Government could collect similar data on hundreds of millions of people and retain that data for a five-year period, updating it with new data every day in perpetuity, was at best, in 1979, the stuff of science fiction.

Finally, *and most importantly,* not only is the Government's ability to collect, store, and analyze phone data greater now than it was in 1979, but the nature and quantity of the information contained in people's telephony metadata is much greater, as well. . . . In fact, some undoubtedly will be reading this opinion *on their cellphones.* Cell phones have also morphed into multi-purpose devices. They are now maps and music players. They are cameras. They are even lighters that people hold up at rock concerts. They are ubiquitous as well. Count the phones at the bus stop, in a restaurant, or around the table at a work meeting or any given occasion. Thirty-four years ago, *none* of those phones would have been there. Thirty-four years ago, city streets were lined with pay phones. Thirty-four years ago, when people wanted to send "text messages," they wrote letters and attached postage stamps.

Admittedly, what metadata *is* has not changed over time. As in *Smith,* the *types* of information at issue in this case are relatively limited: phone numbers dialed, date, time, and the like.[62] But the ubiquity of phones has dramatically altered the *quantity* of information that is now available and, *more importantly,* what that information can tell the Government about people's lives. Put simply, people in 2013 have an entirely different relationship with phones than they did thirty-four years ago. As a result, people make calls and send text messages now that they would not (really, *could not*) have made or sent back when *Smith* was decided — for example, every phone call today between two people trying to locate one another in a public place. This rapid and monumental shift towards a cell phone-centric culture means that the metadata from each person's phone "reflects a wealth of detail about her familial, political, professional, religious, and sexual

[62] There are, however, a few noteworthy distinctions between the data at issue in *Smith* and the metadata that exists nowadays. For instance, the pen register in *Smith* did not tell the government whether calls were completed or the duration of any calls, *see Smith,* 442 U.S. at 741, whereas that information is captured in the NSA's metadata collection. A much more significant difference is that telephony metadata can reveal the user's location, which in 1979 would have been entirely unnecessary given that landline phones are tethered to buildings. . . . That said, not all FISC orders have been made public, and I have no idea how location data has been handled in the past. . . Recent news reports, though not confirmed by the Government, cause me to wonder whether the Government's briefs are entirely forthcoming about the full scope of the Bulk Telephony Metadata Program. *See, e.g.,* Barton Gellman & Ashkan Soltani, *NSA maps targets by their phones,* WASH. POST, Dec. 5, 2013, at A01.

associations," *Jones,* 132 S.Ct. at 955 (Sotomayor, J., concurring), that could not have been gleaned from a data collection in 1979. Records that once would have revealed a few scattered tiles of information about a person now reveal an entire mosaic — a vibrant and constantly updating picture of the person's life.

In sum, the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones. . . .

[The *Klayman* court next examined the totality of the circumstances to determine whether the search is reasonable within the meaning of the Fourth Amendment. In the absence of individualized suspicion of wrongdoing, the search could only be upheld through the "special needs" caselaw of the Supreme Court.]

The factors I must consider include: (1) "the nature of the privacy interest allegedly compromised" by the search, (2) "the character of the intrusion imposed" by the government, and (3) "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Bd. of Educ. v. Earls,* 536 U.S. 822 (2002).

"Special needs" cases, not surprisingly, form something of a patchwork quilt. . . . To my knowledge, however, no court has ever recognized a special need sufficient to justify continuous, daily searches of virtually every American citizen without any particularized suspicion. In effect, the Government urges me to be the first non-FISC judge to sanction such a dragnet.

For reasons I have already discussed at length, I find that plaintiffs have a very significant expectation of privacy in an aggregated collection of their telephony metadata covering the last five years, and the NSA's Bulk Telephony Metadata Program significantly intrudes on that expectation. Whether the program violates the Fourth Amendment will therefore turn on "the nature and immediacy of the government's concerns and the efficacy of the [search] in meeting them." *Earls,* 536 U.S. at 834.

The Government asserts that the Bulk Telephony Metadata Program serves the "programmatic purpose" of "identifying unknown terrorist operatives and preventing terrorist attacks." . . . Yet, turning to the efficacy prong, the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature. In fact, none of the three "recent episodes" cited by the Government that supposedly "illustrate the role that telephony metadata analysis can play in preventing and protecting against terrorist attack" involved any apparent urgency. . . . Given the limited record before me at this point in the litigation—most notably, the utter lack of evidence that a terrorist attack has ever been prevented because searching the NSA database was faster than other investigative tactics—I have serious doubts about the efficacy of the metadata collection program as a means of conducting time-sensitive investigations in cases involving imminent threats of terrorism.

I realize, of course, that such a holding might appear to conflict with other trial courts. . . . Nevertheless, in reaching this decision, I find comfort in the statement in the Supreme Court's recent majority opinion in *Jones* that "[a]t bottom, we must 'assur[e] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted.'" (quoting *Kyllo*). . . . Indeed, I have

little doubt that the author of our Constitution, James Madison, who cautioned us to beware "the abridgement of freedom of the people by gradual and silent encroachments by those in power," would be aghast. . . .

Plaintiffs in this case have also shown a strong likelihood of success on the merits of a Fourth Amendment claim. As such, they too have adequately demonstrated irreparable injury.

. . . [The public interest] looms large in this case, given the significant privacy interests at stake and the unprecedented scope of the NSA's collection and querying efforts, which likely violate the Fourth Amendment. Thus, the public interest weighs heavily in favor of granting an injunction.

. . . [I]n light of the significant national security interests at stake in this case and the novelty of the constitutional issues, I will stay my order pending appeal. In doing so, I hereby give the Government fair notice that should my ruling be upheld, this order will go into effect forthwith.

IN RE FBI

2013 WL 5307991 (FISC 2013)

EAGAN, J. On July 18, 2013, a verified Final "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" (Application) was submitted to the Court by the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA or the Act), Title 50, United States Code (U.S.C.), § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency (NSA) of certain call detail records or "telephony metadata" in bulk. . . .

In conducting its review of the government's application, the Court considered whether the Fourth Amendment to the U.S. Constitution imposed any impediment to the government's proposed collection. Having found none in accord with U.S. Supreme Court precedent, the Court turned to Section 215 to determine if the proposed collection was lawful and that Orders requested from this Court should issue. The Court found that under the terms of Section 215 and under operation of the canons of statutory construction such Orders were lawful and required, and the requested Orders were therefore issued.

Specifically, the government requested Orders from this Court to obtain certain business records of specified telephone service providers. Those telephone company business records consist of a very large volume of each company's call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information (CSLI). The government requested production of this data on a daily basis for a period of 90 days. The sole purpose of this production is to obtain foreign intelligence information in support of [TEXT REDACTED] individual authorized investigations to protect against international terrorism and concerning various international terrorist organizations. In granting the government's request, the Court has prohibited the government from accessing the data for any other intelligence or investigative purpose.

By the terms of this Court's Primary Order, access to the data is restricted through technical means, through limits on trained personnel with authorized access, and through a query process that requires a reasonable, articulable suspicion (RAS), as determined by a limited set of personnel, that the selection term (e.g., a telephone number) that will be used to search the data is associated with one of the identified international terrorist organizations. Moreover, the government may not make the RAS determination for selection terms reasonably believed to be used by U.S. persons solely based on activities protected by the First Amendment. To ensure adherence to its Orders, this Court has the authority to oversee compliance, see 50 U.S.C. § 1803(h), and requires the government to notify the Court in writing immediately concerning any instance of non-compliance, see FISC Rule 13(b). According to the government, in the prior authorization period there have been no compliance incidents.[63]

Finally, although not required by statute, the government has demonstrated through its written submissions and oral testimony that this production has been and remains valuable for obtaining foreign intelligence information regarding international terrorist organizations. . . .

The production of telephone service provider metadata is squarely controlled by the U.S. Supreme Court decision in *Smith v. Maryland*, 442 U.S. 735 (1979). The Smith decision and its progeny have governed Fourth Amendment jurisprudence with regard to telephony and communications metadata for more than 30 years. Specifically, the *Smith* case involved a Fourth Amendment challenge to the use of a pen register on telephone company equipment to capture information concerning telephone calls, but not the content or the identities of the parties to a conversation. The same type of information is at issue here.[64]

The Supreme Court in *Smith* recognized that telephone companies maintain call detail records in the normal course of business for a variety of purposes. Furthermore, the Supreme Court found that once a person has transmitted this information to a third party (in this case, a telephone company), the person "has no legitimate expectation of privacy in [the] information...." The telephone user, having conveyed this information to a telephone company that retains the information in the ordinary course of business, assumes the risk that the company will provide that information to the government. Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing information, it "was not a 'search,' and no warrant was required" under the Fourth Amendment.

In *Smith*, the government was obtaining the telephone company's metadata of one person suspected of a crime. Here, the government is requesting daily

---

[63] The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA's handling of produced information. Through oversight by this Court over a period of months, those issues were resolved.

[64] The Court is aware that additional call detail data is obtained via this production than was acquired through the pen register acquisition at issue in Smith. Other courts have had the opportunity to review whether there is a *Fourth Amendment* expectation of privacy in call detail records similar to the data sought in this matter and have found that there is none. *See United States v. Reed*, 575 F.3d 900, 914 (9th Cir. 2009) (finding that because "data about the 'call origination, length, and time of call' . . . is nothing more than pen register and trap and trace data, there is no *Fourth Amendment* 'expectation of privacy.' "

production of certain telephony metadata in bulk belonging to companies without specifying the particular number of an individual. This Court had reason to analyze this distinction in a similar context in [TEXT REDACTED]. In that case, this Court found that "regarding the breadth of the proposed surveillance, it is noteworthy that the application of the Fourth Amendment depends on the government's intruding into some individual's reasonable expectation of privacy." The Court noted that Fourth Amendment rights are personal and individual, and that "[s]o long as no individual has a reasonable expectation of privacy in meta data, the large number of persons whose communications will be subjected to the . . . surveillance is irrelevant to the issue of whether a Fourth Amendment search or seizure will occur." Put another way, where 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.

In sum, because the Application at issue here concerns only the production of call detail records or "telephony metadata" belonging to a telephone company, and not the contents of communications, *Smith v. Maryland* compels the conclusion that there is no Fourth Amendment impediment to the collection. Furthermore, for the reasons stated in [TEXT REDACTED] and discussed above, this Court finds that the volume of records being acquired does not alter this conclusion. Indeed, there is no legal basis for this Court to find otherwise. . . .

Section 215 of the USA PATRIOT Act created a statutory framework, the various parts of which are designed to ensure not only that the government has access to the information it needs for authorized investigations, but also that there are protections and prohibitions in place to safeguard U.S. person information. . .

This Court must verify that each statutory provision is satisfied before issuing the requested Orders.

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 production of the information sought meets the standard for relevance under Section 215.

As an initial matter and as a point of clarification, the government's burden under Section 215 is not to prove that the records sought are, in fact, relevant to an authorized investigation. The explicit terms of the statute require "a statement of facts showing that there are *reasonable grounds to believe* that the tangible things sought are relevant. . . ." 50 U.S.C. § 1861(b)(2)(A) (emphasis added). In establishing this standard, Congress chose to leave the term "relevant" undefined. This Court recognizes that the concept of relevance here is in fact broad and amounts to a relatively low standard. Where there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations.

This Court has previously examined the issue of relevance for bulk collections. *See* [TEXT REDACTED]. While those matters involved different collections from

the one at issue here, the relevance standard was similar. See 50 U.S.C. § 1842(c)(2) ("[R]elevant to an ongoing investigation to protect against international terrorism. . . ."). In both cases, there were facts demonstrating that information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain. As this Court noted in 2010, the "finding of relevance most crucially depended on the conclusion that bulk collection is *necessary* for NSA to employ tools that are likely to generate useful investigative leads to help identify and track terrorist operatives." [TEXT REDACTED] Indeed, in [TEXT REDACTED] this Court noted that bulk collections such as these are "necessary to identify the much smaller number of [international terrorist] communications." [TEXT REDACTED] As a result, it is this showing of necessity that led the Court to find that "the entire mass of collected metadata is relevant to investigating [international terrorist groups] and affiliated persons." [TEXT REDACTED]

This case is no different. The government stated, and this Court is well aware, that individuals associated with international terrorist organizations use telephonic systems to communicate with one another around the world, including within the United States. The government argues that the broad collection of telephone company metadata "is necessary to create a historical repository of metadata that enables NSA to find or identify known *and unknown* operatives . . . , some of whom may be in the United States or in communication with U.S. persons." The government would use such information, in part, "to detect and prevent terrorist acts against the United States and U.S. interests." The government posits that bulk telephonic metadata is necessary to its investigations because it is impossible to know where in the data the connections to international terrorist organizations will be found. The government notes also that "[a]nalysts know that the terrorists' communications are located somewhere" in the metadata produced under this authority, but cannot know where until the data is aggregated and then accessed by their analytic tools under limited and controlled queries. As the government stated in its 2006 Memorandum of Law, "[a]ll of the metadata collected is thus relevant, because the success of this investigative tool depends on bulk collection."

The government depends on this bulk collection because if production of the information were to wait until the specific identifier connected to an international terrorist group were determined, most of the historical connections (the entire purpose of this authorization) would be lost. The analysis of past connections is only possible "if the Government has collected and archived a broad set of metadata that contains within it the subset of communications that can later be identified as terrorist-related." Because the subset of terrorist communications is ultimately contained within the whole of the metadata produced, but can only be found after the production is aggregated and then queried using identifiers determined to be associated with identified international terrorist organizations, the whole production is relevant to the ongoing investigation out of necessity.

As the U.S. Supreme Court has stated, "Congress is presumed to be aware of an administrative or judicial interpretation of a statute and to adopt that interpretation when it re-enacts a statute without change." *Lorillard v. Pons*, 434 U.S. 575 (1978). This doctrine of legislative re-enactment, also known as the doctrine of ratification, is applicable here because Congress re-authorized Section 215 of the PATRIOT Act without change in 2011. The record before this Court . .

. demonstrates that the factual basis for applying the re-enactment doctrine and presuming that in 2011 Congress intended to ratify Section 215 as applied by this Court is well supported. Members were informed that this Court's "orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States." When Congress subsequently re-authorized Section 215 without change, except as to expiration date, that re-authorization carried with it this Court's interpretation of the statute, which permits the bulk collection of telephony metadata under the restrictions that are in place. Therefore, the passage of the PATRIOT Sunsets Extension Act provides a persuasive reason for this Court to adhere to its prior interpretations of Section 215. . . .

This Court is mindful that this matter comes before it at a time when unprecedented disclosures have been made about this and other highly-sensitive programs designed to obtain foreign intelligence information and carry out counter-terrorism investigations. According to NSA Director Gen. Keith Alexander, the disclosures have caused "significant and irreversible damage to our nation." In the wake of these disclosures, whether and to what extent the government seeks to continue the program discussed in this Memorandum Opinion is a matter for the political branches of government to decide.

As discussed above, because there is no cognizable Fourth Amendment interest in a telephone company's metadata that it holds in the course of its business, the Court finds that there is no Constitutional impediment to the requested production. Finding no Constitutional issue, the Court directs its attention to the statute. The Court concludes that there are facts showing reasonable grounds to believe that the records sought are relevant to authorized investigations. This conclusion is supported not only by the plain text and structure of Section 215, but also by the statutory modifications and framework instituted by Congress. Furthermore, the Court finds that this result is strongly supported, if not required, by the doctrine of legislative re-enactment or ratification.

For these reasons, for the reasons stated in the Primary Order appended hereto, and pursuant to 50 U.S.C. § 1861(c)(1), the Court has GRANTED the Orders requested by the government.

Because of the public interest in this matter, pursuant to FISC Rule 62(a), the undersigned FISC Judge requests that this Memorandum Opinion and the Primary Order of July 19, 2013, appended herein, be published.

NOTES & QUESTIONS

1. ***Two Different Results:*** **Klayman *and* In re FBI.** The *Klayman* court found that the time had come to reject *Smith v. Maryland* as valid precedent. In contrast, the FISC in *In re FBI* declared it to be still valid. How do these courts approach the issue of the precedential value of this Supreme Court decision? Which arguments do you find most and least convincing?
2. ***PCLOB on Section 215.*** In its in-depth study of bulk collection of telephone metadata, the Privacy and Civil Liberties Oversight Board (PCLOB) reached highly negative conclusions. In its view, Section 215 "has shown minimal value in safeguarding the nation from terrorism."[65] Moreover, the program's "implications for privacy and civil liberties" were serious. The Section 215 surveillance involved the government's ongoing collection of "virtually all telephone records of every American."

The time had come to end this program. PCLOB concluded: "Any government program that entails such costs requires a strong showing of efficacy. We do not believe that the NSA"s telephone records program conducted under Section 215 meets that standard." Short of its ultimate recommendation to end this surveillance, the PCLOB also called for immediate changes to the program, including reducing the retention period for bulk telephone records from five years to three and restricting the number of "hops" used in contact chaining from three to two. It also called for Congress to enact legislation permitting the FISC to hear from a panel of outside lawyers who would service as Special Advocates before the FISC.

In separate statements, Board Members Rachel Brand and Elisebeth Collins Cook disagreed with some of the Report. While joining in the Board's recommendation for certain immediate modifications to the program, including removing the "third hop," Brand argued that the program should continue. Brand felt that "the Report gives insufficient weight to the need for a proactive approach to combating terrorism."

Like Brand, Board Member Cook noted that she had "a different view from the Board as to the efficacy and utility of the Section 215 program." She thought that "a tool that allows investigators to more fully understand our adversaries in a relatively nimble way, allows investigators to verify and reinforce intelligence gathered from other programs or tools, and provides 'peace of mind,' has value."

3. ***PCLOB on Section 702.*** In contrast to its call for shutting down the Section 215 program, PCLOB had a largely positive reaction to the NSA's surveillance carried out pursuant to Section 702. It stated: "The program has proven valuable in the government's efforts to combat terrorism as well in other areas of foreign intelligence."[66] Perhaps most crucially, "the program has led the government to identify previously unknown individuals who are involved in international terrorism, and it has played a key role in discovering and disrupting specific terrorist plots aimed at the United States and other countries."

   PCLOB also offered specific recommendations regarding this program. It found that the government was unable to assess the precise scope of the incidental collection under the program of information about U.S. persons. As a result, the Board recommended several measures to help provide information about the extent to which the NSA was acquiring and using communications involving U.S. persons or people located in the United States. It also recommended measures to improve accountability and transparency, including the release of declassified versions of the minimization procedures used by the NSA and other government agencies under Section 702.

---

[65] PCLOB, *Telephone Records Program, supra*, 11.
[66] PCLOB, *Section 702 Surveillance Program, supra*, 10.

4. ***President's Review Board.*** Following the Snowden leaks, President Obama created a Review Group on Intelligence and Communications Technologies. The members of the ad hoc committee were Richard A. Clarke, Michael J. Morell, Geoffrey R. Stone, Cass R. Sunstein, and Peter Swire. The announcement of the Review Group took place on August 27, 2013, and on December 12 of that year, the Group released its report, *Liberty and Security in a Changing World*. There were 46 recommendations in this report; of these, several concerned Section 215 and Section 720 oversight.

   The Group offered numerous recommendations based on the central principles of protecting both national security and personal privacy as well as fulfilling the central task of risk management. With regard to Section 215 of FISA, it called for an end to the government's storage of bulk telephone metadata and the transition to a system in which such metadata is held privately by telephone companies. The government would then query this information when necessary for national security purposes. As a broad principle for the future, the Group noted: "without senior policy review, the government should not be permitted to collect and store mass, undigested, non-public personal information about US persons for the purpose of enabling future queries and data mining for foreign intelligence purposes."[67]

   Regarding Section 702, the President's Review Group recommended that if the government legally intercepts a communication under this authority that "either includes a United States person as a participant or reveals information about a United States person[,]" it should purge any information about that United States person "unless it either has foreign intelligence value or is necessary to prevent serious harm to others." It also recommended that in implementing Section 702, the U.S. government should reaffirm that such surveillance "must be directed *exclusively* at the national security of the United States or our allies" and "must *not* be directed at illicit or illegitimate ends, such as the theft of trade secrets or obtaining commercial gain for domestic industries."[68]

5. ***Bulk Metadata: Private Sector or Governmental Control?*** Regarding the issue of leaving the bulk metadata of the Section 215 program with the private sector, the PCLOB's Rachel Brand took a different view from the President's Review Group's recommendation that it remain with telephone companies. It is worthwhile to contrast the two differing approaches. In her separate statement to the PCLOB's Report on the Telephone Records Program, Brand stated, "I doubt I could support a solution that transfers responsibility for the data to telephone service providers."[69] Legislation would be needed to create a data retention mandate, but this law might also "increase privacy concerns by making the data available for a wide range of purposes other than national security." Indeed, such legislation "would raise a host of questions about the legal status and handling of the data and the role and liabilities of the providers holding it." Brand concludes: "In my view, it would be wiser to leave the program as it is with the NSA than to transfer it to a third party."

[67] President's Review Group on Intelligence and Communication Technologies, *Liberty and Security in a Changing World* 17 (2013).

[68] *Id.* at 29-30 (emphasis in original).

[69] PCLOB, *Telephone Records Program, supra*, 6 (Separate Statement by Board Member Rachel Brand).

6. ***Caselaw on Section 702.*** The FISC has heard multiple cases involving the Section 702 program. In particular, it was troubled by the upstream collection program. In *Redacted*, 2012 WL 9189263 (FISC Sept. 25, 2012), the FISC helpfully summarized its 2011 ruling that "the NSA was annually acquiring tens of thousands of Internet transactions containing at least one wholly domestic communication; that many of these wholly domestic communications were not to, from, or about a targeted facility; and that NSA was also likely acquiring tens of thousands of additional Internet transactions containing one or more targeted communications to and from U.S. persons in the United States."

   In its *Redacted* opinion, the FISC decided that the remedial steps taken by the government since October 2011 reduced the risks of past upstream acquisitions under Section 702. For example, the NSA had purged data collected before October 31, 2011 and the utilization of new minimization procedures, which the FISC approved on November 30, 2011. The FISC declared "the outstanding issues raised by NSA's upstream collection of Internet transactions" to be "resolved, subject to the discussion of changes to the minimization procedures that appears below." The subsequent part of the opinion was, however, entirely redacted. Susan Landau argues, "Ultimately, the rules of data minimization should be subject to a public discussion, especially when they directly affect the public." What kind of information do you feel is needed about the Section 702 program to evaluate its policy implications?

   In *United States v. Mohamud*, 2014 WL 2866749 (D. Or. 2014), the district court upheld Section 702 against constitutional and other legal challenges. It found that this provision in FISA did not violate the separation of powers doctrine as safeguarded by the Fourth Amendment. FISC review of Section 702 surveillance submissions "provides prior review by a neutral and detached magistrate." The result? This review "strengthens, not undermines, Fourth Amendment rights." The section was also found more generally to comport with the Fourth Amendment. The district court found that Section 702 fell within the exception in the *Keith* case for foreign intelligence. Following a FISC opinion, [Caption Redacted], 2011 WL 10945618 (FISC 2011), the *Mohamud* court decided that the collection under Section 702 was still as a whole directed at national security even if the NSA also acquired communications concerning U.S. persons inside the United States. The court also decided that the governmental action was also reasonable under the Fourth Amendment due to the numerous safeguards, such as targeting and minimization procedures, built into Section 702.

7. ***Lack of Investigative Capacity.*** Judge Reggie Walton, the chief judge of the FISC, has told the *Washington Post* that the court lacks tools to provide oversight of the government's surveillance programs. He stated, "The FISC is forced to rely upon the accuracy of the information that is provided to the Court. The FISC does not have the capacity to investigate issues of noncompliance,

and in that respect the FISC is in the same position as any other court when it comes to enforcing [government] compliance with its orders."[70] Judge Walton's comments came after the *Post* obtained an NSA classified internal NSA report on its failures to follow certain of the agency's privacy rules and other legal restrictions. Should the FISC's oversight be strengthened, or is such a role best played by the Executive Branch, Congress, or through an internal NSA audit function?

8. ***The USA FREEDOM Act.*** In 2015, the USA Freedom Act, H.R. 2048, S. 1123, banned the bulk collection of Americans' Internet metadata and telephone records under the Patriot Act Section 215. The government must now identify a person, account, address, or personal device when requesting records, limiting the scope of tangible things sought "to the greatest extent reasonably possible." However, the bill permits authorities to collect phone records two degrees (or "hops") of separation from targeted individuals.

[70] Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited,* Washington Post (Aug. 15, 2013).

CHAPTER 6
HEALTH PRIVACY

CHAPTER OUTLINE