Montana Law Review

Volume 80 | Issue 2 Article 1

8-1-2019

2019 James R. Browning Distinguished Lecture in Law, "Holding the Delicate Balance Steady and True": The History of FISA's Grand Bargain

Richard C. Tallman
Richard C. Tallman, Senior U.S. Circuit Judge for the Ninth Circuit and Judge on the Foreign Intelligence Surveillance Court of Review

Tania M. Culbertson
Tania M. Culbertson, Career Law Clerk to Judge Tallman

Recommended Citation
Richard C. Tallman & Tania M. Culbertson, *2019 James R. Browning Distinguished Lecture in Law, "Holding the Delicate Balance Steady and True": The History of FISA's Grand Bargain*, 80 Mont. L. Rev. 137 (2019).

\\jciprod01\productn\M\MON\80-2\MON201.txt unknown Seq: 1 1-AUG-19 11:49

LECTURE

"HOLDING THE DELICATE BALANCE STEADY AND TRUE": THE HISTORY OF FISA'S GRAND BARGAIN

The Honorable Richard C. Tallman* & Tania M. Culbertson**

I. Introduction

Good evening. I am honored to be asked to deliver this lecture named in honor of a great Montanan and my beloved colleague for several years before his passing. Judge Jim Browning remains a legend on our court and this lecture series is a fitting tribute to a brilliant jurist and genuinely caring human being. We all miss him.

In 2008, then-Chief Judge Bruce Selya, while serving on the Foreign Intelligence Surveillance Court of Review, which we call the FISCR, articulated the mission statement of the judiciary when reviewing the domestic surveillance powers exercised by the United States in furtherance of national security:

> Our government is tasked with protecting an interest of utmost significance to the nation—the safety and security of its people. But the Constitution is the cornerstone of our freedoms, and government cannot unilaterally sacrifice constitutional rights on the altar of national security. Thus, in carrying out its national security mission, the government must simultaneously fulfill its constitutional responsibility to provide reasonable protections for the pri-

* Senior U.S. Circuit Judge for the Ninth Circuit and Judge on the Foreign Intelligence Surveillance Court of Review

* Career Law Clerk to Judge Tallman. The authors wish to thank Professor Bobby Chesney and Professor Steve Vladeck for their National Security Law Podcast three-part series on the Foreign Intelligence Surveillance Act, from which some of the themes in this lecture are drawn. The first of the three-part series is found here: https://www.nationalsecuritylawpodcast.com/episode-96-a-deep-dive-into-the-foreign-intelligence-surveillance-act/ (last visited May 19, 2019).

\\jciprod01\productn\M\MON\80-2\MON201.txt unknown Seq: 2 1-AUG-19 11:49

> vacy of United States persons. The judiciary's duty is to hold that delicate balance steady and true.[1]

Tonight, I will explain what led to the passage of the Foreign Intelligence Surveillance Act ("FISA") and its creation of the FISA courts, and describe the grand bargain that was struck between our three branches of government when creating FISA's judicial review procedures over domestic espionage and counter-terrorism investigations. My hope is to leave you with a keener understanding of how we have arrived at where we are today, and how the judiciary understands its oversight role within FISA's statutory framework and under our Constitution.

A word of caution: as a currently-serving judge on the FISCR, charged with reviewing sensitive classified matters, I will not be discussing with you any of the cases underlying the more sensational news items concerning the FISA courts that you may have heard or read about over the past few years. My talk will deal with history more than with current events. I begin with a brief overview of the current structure of the United States Intelligence Community in order to provide you with a sense of its scope, and then I will turn to the history and case law that led to FISA's passage and subsequent evolution. I will close by reiterating the key concepts I hope you take away from my lecture to aid you in understanding what the FISA framework requires the judiciary to weigh in considering the substantial questions of constitutional law impacting the privacy-versus-security debate, which continues to this day. As judges, we do this work in order to ensure that we all remain safe and secure while holding steadfast our fealty to the cornerstone of our freedoms.

II. Overview of the United States Intelligence Community

When you think of intelligence agencies, you probably think of the Central Intelligence Agency ("CIA"), the Federal Bureau of Investigation ("FBI"), and the National Security Agency ("NSA"). And, in fact, prior to 2004, the United States Intelligence Community was supervised by the Director of Central Intelligence, who also oversaw the CIA. But in 2004, as part of its response to the terrorist attacks of September 11, 2001, Congress passed the Intelligence Reform and Terrorism Prevention Act which, among other things, established the Office of the Director of National Intelligence ("ODNI") to better unify and manage the efforts of the Intelligence Community.[2]

1. *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

2. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108–458, 118 Stat. 3638.

In the words of the ODNI, the "U.S. Intelligence Community is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States."[3] The ODNI supervises the gathering and analysis of intelligence for the President, the National Security Council, the heads of departments and agencies of the executive branch, the Chairman of the Joint Chiefs of Staff and senior military commanders, and Congress.[4]

In addition to the ODNI, the U.S. Intelligence Community members include the CIA—an independent agency—and various agencies and the military branches within the Departments of Defense (including the NSA), Energy, Homeland Security, Justice (including the FBI and the DEA), State, and Treasury.[5] These members, to varying degrees, oversee or employ six basic intelligence collection disciplines: (1) signals intelligence (think: the NSA); (2) human intelligence (think: not just espionage, but also overt collection by, for example, de-briefers and military attachés); (3) imagery intelligence (think: photography, film, and radar, among others); (4) geospatial intelligence (think: satellites); (5) open source intelligence (think: the same news sources you review); and, (6) likely of least familiarity to you, measurement and signature intelligence, which is technically derived intelligence data other than imagery or signals intelligence that draws from various disciplines—for instance, optical, acoustic, seismic, and materials sciences.[6] An example of acoustical intelligence is capturing the sonar "signature" of a ballistic missile submarine as it cruises underwater. As you can see, the distinct members of the Intelligence Community make up a complex and highly-technical network, which is important to bear in mind as we look at the evolution of the legal framework used to govern sophisticated intelligence gathering in the modern era, including the ways in which technological developments drive that evolution.

III. Technological Developments Drive the "Modern Era" of Surveillance Law, and the Checks and Balances Between the Branches of Government Begin

We begin our discussion of the history of electronic surveillance law with the Supreme Court's 1928 decision in *Olmstead v. United States*,[7]

3. *See* Office of the Director of National Intelligence, *What is Intelligence?*, Office of the Director of National Intelligence (April 20, 2019), https://perma.cc/6ZLX-WEGW.

4. *Id.*

5. Office of the Director of National Intelligence, *Members of the IC*, Office of the Director of National Intelligence (April 20, 2019), https://perma.cc/4QXG-58W9.

6. *What is Intelligence?*, *supra* note 3. R

7. 277 U.S. 438 (1928).

which addressed the question of whether "the use of evidence of private telephone conversations between the defendants and others, intercepted by means of wiretapping, amounted to a violation of the Fourth and Fifth Amendments."[8] The case actually arose in my former duty station of Seattle, Washington, where petitioners plus some seventy-two others were indicted for violations of the National Prohibition Act—in other words, bootlegging whiskey on a scale so grand that it involved numerous cargo vessels, underground storage caches, "a central office manned with operators, and the employment of executives, salesmen, deliverymen dispatchers, scouts, bookkeepers, collectors, and an attorney."[9]

The information which led to the discovery of the liquor conspiracy was largely obtained from wiretaps clipped to the ordinary telephone wires leading from the residences of the petitioners and from the basement of the central office building.[10] Importantly, the taps were installed "without trespass upon any property of the defendants."[11] One of the questions before the Supreme Court, then, was whether a wiretap was the kind of qualifying search protected by the Fourth Amendment, which provides: "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[12]

Here is what the Court decided: "The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants."[13] Although this sounds surprising to us now in light of subsequent case law, the Supreme Court in 1928 held that wiretapping simply was not the kind of search against which the Fourth Amendment protects. But the Court also issued an explicit invitation to Congress to legislate in this arena, writing, "Congress may, of course, protect the secrecy of telephone messages by making them, when intercepted, inadmissible in evidence in federal criminal trials, by direct legislation."[14] And that is what Congress did in the Communications Act of 1934.[15] So here, I submit to you, is an example of a technological development—the widespread use of Alexander Graham Bell's new telephone—

8. *Id.* at 456.
9. *Id.*
10. *Id.* at 456–57.
11. *Id.* at 457.
12. U.S. CONST. amend. IV.
13. *Olmstead*, 277 U.S. at 464.
14. *Id.* at 465.
15. 47 U.S.C. §§ 151–624 (2018).

causing the judicial branch to answer a novel legal question about the investigatory powers of the executive branch. But when the legislative branch did not like the answer given by the judiciary, it stepped in to adjust the balance by statute.

The Communications Act of 1934 combined and organized federal regulation of telephone, telegraph, and radio communications, and created a new agency, the Federal Communications Commission ("FCC"), to oversee and regulate these industries.[16] And as written in 1934, it provided, among other things, that "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect, or meaning of such intercepted communication to any person," on threat of fines and imprisonment for willful and knowing violations.[17] In 1937, in *Nardone v. United States*,[18] the Supreme Court had to decide whether, in view of these statutory provisions, "evidence procured by a federal officer's tapping telephone wires and intercepting messages" was admissible in a federal criminal trial.[19] It concluded that, "[t]aken at face value the phrase 'no person' comprehends federal agents, and the ban on communication to 'any person' bars testimony to the content of an intercepted message."[20]

In response to the government's argument that surely Congress did not intend to "hamper and impede the activities of the government in the detection and punishment of crime," the Court responded that it would not address this policy question and that "Congress may have thought it less important that some offenders should go unwhipped of justice than that officers should resort to methods deemed inconsistent with ethical standards and destructive of personal liberty."[21] Again, we see the judiciary acknowledging that it is the responsibility of the legislative branch to adjust the balance when it comes to privacy issues.

But the judiciary has a role in protecting privacy too. In the case of *Katz v. United States*,[22] in 1967, the Supreme Court once again examined the question whether the Fourth Amendment protects against electronic surveillance, and this time it reached a somewhat different conclusion than in *Olmstead*. In *Katz*, the petitioner was charged with transmitting illegal bets from Los Angeles to Miami and Boston using a public payphone in an enclosed booth.[23] Federal agents had placed a listening device on the

16. Communications Act of 1934, c. 652, Title I, § 1, 48 Stat. 1064.
17. Nardone v. United States, 302 U.S. 379, 380–81 (1937) (quoting 47 U.S.C. § 605 (1934)).
18. 302 U.S. 379 (1937).
19. *Id.* at 380.
20. *Id.* at 381.
21. *Id.* at 383.
22. 389 U.S. 347 (1967).
23. *Id.* at 348.

outside of the phone booth without obtaining a warrant, and Mr. Katz asked the Supreme Court to decide "[w]hether a public telephone booth is a constitutionally protected area so that evidence obtained by attaching an electronic listening recording device to the top of such a booth is obtained in violation of the right to privacy of the user of the booth."[24]

Rather than answering that question directly, the Supreme Court came up with a different formulation: "[T]his effort to decide whether or not a given 'area,' viewed in the abstract, is 'constitutionally protected' deflects attention from the problem presented by this case."[25] The Court continued, "For the Fourth Amendment protects people, not places. What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection . . . . But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[26] Accordingly, the Court held that "[t]he Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."[27] Or, in the words of Justice Harlan's concurrence—the language with which you are likely all familiar—the unauthorized listening device violated Katz's "constitutionally protected reasonable expectation of privacy."[28]

In the wake of the *Katz* case, and in response to investigations showing the widespread continued use of wiretaps without legal authority, Congress passed Title III of the Omnibus Crime Control and Safe Streets Act of 1968,[29] also known as the Wiretap Act, which established stringent warrant procedures for monitoring and recording telephone calls that prosecutors must follow to be consistent with the Fourth Amendment for use in criminal investigations. I'll talk about those judicially supervised procedures more in a moment, but here again, you see Congress acting in response to actions by the executive branch, and decisions by the judicial branch, in order to strike a better balance between privacy rights and law enforcement.

But what about cases involving not just ordinary crimes, but national security concerns? The Supreme Court had deliberately refused to reach that question in *Katz*, noting in a footnote that "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security is a question not

24. *Id.* at 349.
25. *Id.* at 351.
26. *Id.*
27. *Id.* at 353.
28. *Id.* at 360 (Harlan, J., concurring).
29. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90–351, Title III, § 802, 82 Stat. 212; 18 U.S.C. §§ 2510–2522 (2018).

presented in this case."[30] The Court did not consider, and did not decide, whether there could be a national security exception to the Fourth Amendment's warrant requirement. And Title III, as originally drafted, included a proviso that nothing therein "shall limit the constitutional power of the President to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to protect national security information against foreign intelligence activities."[31]

Indeed, national security surveillance authorized solely by the President was then ongoing, and largely not subject to judicial review of any kind. For example, in May 1940, President Franklin D. Roosevelt authorized Attorney General Robert H. Jackson to use wiretapping in matters "involving the defense of the nation," and "electronic surveillance [was] used . . . in domestic security cases at least since . . . 1946."[32] In my office, I have a copy of the one-paragraph justification signed by FBI Director J. Edgar Hoover during the administration of President John F. Kennedy, and the signed authorization by Attorney General Robert Kennedy, permitting the tapping of the telephone of the Reverend Dr. Martin Luther King, dated October 10, 1963. Most famously, these practices intensified under President Richard Nixon, who blurred the line between foreign and domestic security purposes and used wiretapping as a tool to identify political enemies both abroad and at home. As you may know, these abuses were eventually uncovered, and aggressively investigated by the Church and Pike committees in Congress.[33] But the judiciary was also examining some of these issues, as illustrated by the *Keith* case decided by the Supreme Court in 1972.[34]

The *Keith* case arose from a criminal proceeding in the Eastern District of Michigan, in which the United States charged three defendants with conspiracy to destroy government property.[35] One of the defendants, Larry Plamondon, an anti-Vietnam War activist, was charged with the dynamite bombing of a CIA office in Ann Arbor, Michigan.[36] During pretrial proceedings, it was revealed that the Attorney General had approved warrant-

30. *Katz*, 389 U.S. at 358 n.23.

31. United States v. U.S. Dist. Ct. for E.D. Mich., 407 U.S. 297, 302 (1972) [hereinafter "*Keith* case"].

32. *Id.* at 310 n. 10; *see also* Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: the FDR Precedent*, 60 STAN. LAW REV. 1023 (2008).

33. *See* Select Comm. to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities and the Rights of Americans*, S. Rep. No. 94-755 (1976).

34. *Keith* case, 407 U.S. 297.

35. *Id.* at 299.

36. *Id.*

less wiretaps "to gather intelligence information deemed necessary to protect the nation from attempts of *domestic organizations* to attack and subvert the existing structure of the Government."[37] The government argued that this was a reasonable exercise of the President's constitutional power to protect the national security and therefore no warrant was required.[38] The Court was faced with deciding, this time in a case that concededly did not involve any foreign power or foreign intelligence, whether there is a national security exception to the Fourth Amendment warrant requirement.[39]

Once again, the Supreme Court managed to dodge the question, this time by distinguishing between *foreign* intelligence and *domestic* intelligence. The Court refused to say how it would rule if the case had involved foreign threats, stating "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."[40] The Court also acknowledged the difference between attempts to gather evidence for specific criminal prosecutions, which the government argued it was not initially engaged in here, and "surveillances . . . directed primarily to the collecting and maintaining of intelligence with respect to subversive forces,"—that is, "ongoing intelligence gathering," as authorized by the Attorney General in this case.[41] But as to the latter, the Court concluded that it would not make "the requested departure from Fourth Amendment standards" because these circumstances did not "justify complete exemption of domestic security surveillance from prior judicial scrutiny."[42] It held that the government was required to follow "an appropriate warrant procedure" in this case.[43]

Interestingly, however, the Court signaled it was open to employing different, and perhaps less stringent, warrant procedures in the domestic intelligence context than in the realm of criminal investigations governed by Title III. The Court said:

> Given th[e] potential distinctions between Title III criminal surveillances and those involving 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 govern-

37. *Id.* at 300 (emphasis added).
38. *Id.* at 301.
39. *Id.* at 309.
40. *Id.* at 321–22.
41. *Id.* at 318–19.
42. *Id.* at 320.
43. *Id.*

> mental interest to be enforced and the nature of citizen rights deserving protection.[44]

If Congress had responded to this invitation from the Supreme Court, perhaps we would now have a DISA—that is, a Domestic Intelligence Surveillance Act—in addition to a FISA. As it happened, however, given the wide range of intelligence abuses by federal agencies, during administrations of both parties, identified in the Church Committee Report, there was no appetite in Congress to carve out a separate procedure for domestic intelligence surveillance. Rather, distinguishing only between foreign intelligence surveillance and domestic criminal prosecutions, Congress focused its energies on developing FISA, to which I will now turn.

IV. FISA AND THE FISA COURTS: THE GRAND BARGAIN

Congress passed the Foreign Intelligence Surveillance Act in 1978. It is codified at 50 U.S.C. §§ 1801 et seq. As originally enacted, FISA was designed to provide a process for intelligence agencies to seek a warrant for surveillance inside the United States of foreign powers and their agents.[45] After I review for you what FISA, as originally conceived, authorizes, I will describe what each branch of government gave and what each branch got out of this grand bargain. At the most basic level, FISA gave a role to each of the three branches of government in regulating foreign intelligence surveillance, which, as is hopefully apparent from the historical background I have just discussed, was not always the case.

FISA, simply put, authorizes the federal government to engage in four types of investigative activity in connection with certain national security investigations: (1) electronic surveillance; (2) physical searches; (3) the use of pen registers and trap-and-trace devices; and (4) compelling the production of tangible things.[46] All of this activity must be directed at a foreign power or an agent of a foreign power.[47] And for purposes of conducting counter-terrorism investigations, terrorists are treated like agents of foreign powers even if they owe allegiance to an international terrorist group, which is treated akin to a non-nation State.

As with applications for Title III warrants in the federal criminal context, FISA requires an affidavit of probable cause,[48] although the probable cause showing is distinct from that required under Title III. Instead of showing that there is probable cause to believe that an individual is commit-

44. *Id.* at 322–23.

45. *See generally* An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information, Pub. L. No. 95-511, 92 Stat 1783 (1978).

46. 50 U.S.C. §§ 1802, 1822, 1842, 1861 (2018).

47. *Id.*

48. *See generally Id.* §§ 1804, 1823, 1842, 1861.

ting, has committed, or is about to commit a particular enumerated offense, a FISA affidavit must establish probable cause to believe: (1) that the target of the surveillance is a foreign power or agent of a foreign power (which can include agents of foreign political organizations and groups engaged in international terrorism, as well as agents of foreign nations); (2) that each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power; (3) that a significant purpose of the surveillance is to obtain foreign intelligence information; and, (4) that appropriate minimization procedures are in place.[49] Also distinct from a Title III warrant sought by street-level case agents, FISA applications must be approved at the highest levels of government, for example by the Attorney General or the Deputy Attorney General, and must be certified by the President's National Security Advisor or an equally senior designee (often the FBI, CIA, or NSA Director or Deputy Director).[50]

FISA also established the Foreign Intelligence Surveillance Court ("FISC"), to review FISA applications and issue orders, and its Court of Review, to hear government appeals from denials of applications or challenges by third parties ordered to produce information. The Chief Justice of the United States designates federal district court judges to serve as judges on the FISC; currently, there are 11 such judges who serve staggered seven-year terms.[51] The judges designated must represent at least seven of the judicial circuits, and three of the judges must live within 20 miles of the District of Columbia.[52] The Chief Justice also appoints three federal circuit court judges to the FISCR.[53] I was appointed in 2014, and my term will end in 2021. Appeals from the FISCR may be taken to the Supreme Court, but to date the Supreme Court has not yet taken a case from the FISA courts.

So, what does the FISA application process look like? Applications are generally presented to the duty judge by Justice Department attorneys from the Office of Intelligence within the National Security Division on behalf of the agency with primary investigative or intelligence gathering authority over a particular matter.[54] Those attorneys first file a proposed Application for an Order, which is reviewed by legal advisors for the FISC. The legal advisors oftentimes begin discussions with the government attorneys regarding the sufficiency of the probable cause showing and the scope of the requested order. The FISC judge on duty to handle the application, after

49. *Id.* § 1804(a).
50. *Id.*
51. *Id.* § 1803(a)(1).
52. *Id.*
53. *Id.* § 1803(b).
54. *Id.* § 1803(a).

consulting with his or her legal advisors, can approve or deny the application or request additional modifications.[55] About 20 to 25% of the time, the FISC judge requires more information or better articulation of probable cause. In the Director of the Administrative Office of the U.S. Courts's most recent report to Congress, the FISC disclosed that it received 1,318 FISA applications in 2018.[56] After consideration by the court, 985 orders were granted, 261 orders were modified, 42 orders were denied in part, and 30 applications were denied in full.[57] The 11 FISC judges examine the applications brought before them with a discerning eye and do not issue these orders lightly. In no way is this court a "rubber stamp" for whatever the government wants to do.

With this process in mind, and compared to how foreign intelligence surveillance was conducted in the past, I think it is fair to say that each of the three branches of government compromised in order to reach FISA's delicate balance. First, the executive branch: it gave up the potentially unilateral authority to conduct foreign intelligence surveillance without any oversight, left open by the Supreme Court's decision in the *Keith* case, and agreed that foreign intelligence surveillance conducted inside the United States is to be governed by statute. In return, the executive gained legitimacy because its practices and procedures are endorsed by the legislature and authorized by the judiciary, and the executive can rest assured that evidence obtained after properly following FISA's provisions can be used in court should a prosecution ensue.

Next, the legislature: it gained the ability to oversee (through regular reporting by the intelligence community) and to regulate (through oversight) the exercise of executive power that heretofore it had not touched. In this regard, it is worth remembering that Congress still does not regulate foreign intelligence surveillance conducted completely outside the United States; that work is mostly governed by Executive Order 12333, which was issued by President Ronald Reagan in 1981 under the President's constitutional authority over foreign relations and as the Commander in Chief.[58] Congress also gained oversight power through its intelligence committees, including the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence, both established shortly before FISA was passed,[59] and the judiciary committees of both chambers. Under-

55. *Id.* § 1804(c).

56. Director of the Administrative Office of the United States Courts, *Report of the Director of the Administrative Office of the U.S. Courts on Activities of the Foreign Intelligence Surveillance Courts for 2018*, Administrative Office of the United States Courts, 1 (2018), https://perma.cc/G2M2-CT4R.

57. *Id.*

58. Exec. Order No. 12,333, 46 FR 59941 (1981).

59. H.R. Res. 658, 95th Cong. (1977); S. Res. 400, 94th Cong. (1976).

standably, however, congressional oversight of foreign intelligence surveillance mostly happens behind closed doors, which is a departure from Congress's usual practice of conducting all proceedings in public; the reason is to prevent the disclosure of the methods and means by which intelligence agencies gather specific information and to protect ongoing investigations.

Finally, the judiciary: it gained oversight over an individualized warrant procedure for the kind of national security surveillance that might impact U.S. citizens that it had previously steered clear of reviewing. Rather than simply deferring to the President's Article II responsibility to protect the security of the nation, the judiciary, at least as to foreign intelligence surveillance conducted within the United States, now had a clearly-articulated role to play. But this role raises some interesting questions. For example, does an application to conduct surveillance under FISA satisfy Article III's case or controversy requirement? Unlike with Title III warrant procedures, where it is understood that obtaining a warrant is very likely ancillary to a subsequent criminal prosecution and adversary proceedings to challenge its issuance or execution, surveillance conducted under a FISA order may not lead to any further proceedings in court. And given that the FISA application process is conducted ex parte, and often only the government's position is represented, how can it be said that the process involves a case or controversy? This question only intensified after FISA was amended in the FISA Amendments Act of 2008 to include authority not just over applications for individualized surveillance orders, but issuance of orders under Section 702.[60] These orders either approve or find deficient the government's proposed annual procedures for the targeting within the United States of persons reasonably believed to be outside the United States, without individualized judicial findings of probable cause as to each target.[61] To put it another way, Section 702 governs the collection, within the United States, of communications of non-U.S. persons outside of the United States when those communications transit portions of the Internet backbone in the U.S. or are handled by U.S. service providers.

Section 702 could be the topic of a whole separate lecture, but for now, I simply wish to note that FISA court proceedings (especially when it comes to the approval of Section 702 procedures) are unlike any other proceedings in the federal court system. They, therefore, can be seen as a form of judicial compromise, albeit a greatly beneficial compromise because they now allow judicial oversight of what had previously been an entirely unsupervised executive function.

60. Pub. L. No. 110-261, 122 Stat. 2436 (2008).

61. 50 U.S.C. § 1881a(j) (2018).

V. Law Enforcement Versus Foreign Intelligence Gathering: the "Primary Purpose" Test and the Wall

The last set of developments I want to discuss tonight brings us to the end of the twentieth century and the immediate aftermath of the terrorist attacks of September 11, 2001. As you have heard, FISA grew out of the distinction between surveillance for law enforcement purposes and surveillance for foreign intelligence gathering. That distinction continued to generate vexing legal questions after FISA's 1978 passage, which had to be squarely addressed after 9/11.

FISA, as originally drafted, required the executive branch to certify, in its application, "that *the purpose* of the surveillance is to obtain foreign intelligence information."[62] But as part of the USA PATRIOT Act of 2001, that language was changed so that the executive must certify "that *a significant purpose* of the surveillance is to obtain foreign intelligence information."[63] Why was this change made?

In part, the change arose out of the fact that the Supreme Court had not—and to this day still has not—decided whether there is a national security exception to the Fourth Amendment's warrant requirement. Although FISA provided statutory procedures understood to comport with the Fourth Amendment because FISA applications are focused on foreign intelligence, federal courts after the *Keith* case and around the time of FISA's passage still wrestled with how to undertake a Fourth Amendment analysis in cases involving both foreign intelligence gathering and domestic law enforcement. This is best illustrated by the Fourth Circuit's *Truong* case, decided in 1980.[64]

David Truong and Ronald Humphrey were convicted of espionage, conspiracy to commit espionage, and several other offenses for transmitting classified U.S. government information to representatives of the government of the Socialist Republic of Vietnam.[65] The warrantless searches and surveillance that led to their convictions were conducted *before* the passage of FISA, so the Fourth Circuit was essentially faced with the question that the Supreme Court had left open in the *Keith* case: namely, is there a national security exception to the warrant requirement when it comes to foreign intelligence? The Fourth Circuit said yes.

The court reasoned that "because of the need of the executive branch for flexibility, its practical experience, and its constitutional competence,

62. An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information, Pub. L. No. 95-511, § 104, 92 Stat 1783 (emphasis added).

63. 50 U.S.C. § 1804 (2002) (emphasis added).

64. United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980).

65. *Id.* at 911.

\\jciprod01\productn\M\MON\80-2\MON201.txt unknown Seq: 14 1-AUG-19 11:49

the courts should not require the executive to secure a warrant each time it conducts foreign intelligence surveillance."[66] Importantly, however, the court held that:

> [T]he executive should be excused from securing a warrant *only* when the surveillance is conducted "primarily" for foreign intelligence reasons . . . because once surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution.[67]

FISA, as originally drafted, appears to satisfy the Fourth Circuit's primary purpose test, and was interpreted in that manner. But the Justice Department had growing concerns, as demonstrated during the Aldrich Ames espionage prosecution in 1994, that due to the "numerous prior consultations between FBI agents and prosecutors, the judge might rule that the FISA warrants [obtained in that case] had been misused"[68]—that is, that the line between surveillance for foreign intelligence information and surveillance for domestic law enforcement had been crossed. In 1995, Attorney General Janet Reno, with the assistance of Deputy Attorney General Jamie Gorelick, issued formal procedures aimed at managing information sharing between the FBI, on the intelligence side, and Justice Department prosecutors, on the criminal side.[69] Over time, these procedures came to be referred to as "the wall," and they eventually came under criticism after 9/11 for "block[ing] the arteries of information sharing" that might have prevented the attacks.[70]

In the immediate aftermath of 9/11, the wall came down, with Attorney General John Ashcroft directing as much information sharing as possible, and Congress changing the "purpose" language in the FISA statute. FISA now provides that obtaining foreign intelligence information need only be "a significant purpose" of the surveillance. But would the Fourth Amendment still be satisfied if the primary purpose of surveillance conducted under FISA was law enforcement, and gathering foreign intelligence information was only a secondary purpose? That question came before the FISC, and then the FISCR, in 2002 in *In re Sealed Case*.[71]

In *In re Sealed Case*, the government appealed from an order of the FISC imposing certain requirements and limitations regarding FISA sur-

66. *Id.* at 914.

67. *Id.* at 915 (emphasis added).

68. THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 78 (Official Government ed. 2004).

69. *Id.* at 79.

70. *Id.* at 79–80.

71. 310 F.3d 717 (FISA Ct. Rev. 2002).

veillance.[72] Specifically, the FISC had ordered that "law enforcement officials shall not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances" and that the FBI and DOJ "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."[73] The FISCR, however, pointed out that "[t]he 'wall' emerges from the [FISC]'s implicit interpretation of FISA"—the same wall that the language change in the USA PATRIOT Act was intended to tear down.[74]

In re Sealed case goes on to thoroughly rebut any notion that FISA, as written in 1978, included a "primary purpose" test, and points out that *Truong* was not a FISA decision and dealt only with the Fourth Amendment and the boundaries of the President's inherent executive authority.[75] And the FISCR noted that by "assert[ing] authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I)," the FISA court "may well have exceeded the constitutional bounds that restrict an Article III court."[76] In other words, the FISCR apparently felt that the FISC was not sticking to the grand bargain and that the delicate balance was becoming unsteady.

Ultimately, *In re Sealed* case concluded that the PATRIOT Act "eliminated any [statutory] justification for the FISA court to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence purposes."[77] And without concluding that a FISA order is "a 'warrant' contemplated by the Fourth Amendment," the FISCR held that "FISA as amended is constitutional because the surveillances it authorizes are reasonable."[78] After *In re Sealed* case, the wall—at least with respect to the FISA courts—had well and truly crumbled. In order to satisfy the requirements of FISA and the Fourth Amendment, the government is not required to show that its primary purpose for engaging in surveillance is to gather foreign intelligence information. The balance was shifted through legislation and subsequent judicial interpretation, and there it currently remains.

72. *Id.* at 720.
73. *Id.*
74. *Id.* at 721.
75. *Id.* at 725–26.
76. *Id.* at 731.
77. *Id.* at 735.
78. *Id.* at 741, 746.

\\jciprod01\productn\M\MON\80-2\MON201.txt unknown Seq: 16 1-AUG-19 11:49

VI. Conclusion

There is much more to say about the evolution of FISA since 2002, including the addition of Section 702, the bulk collection of metadata at one time, but no longer, previously conducted under Section 215 of the USA PATRIOT Act, and the ongoing changes underway as various provisions of post-9/11 legislation reach their sunsets. However, I fear I would keep you here all night if I tried to discuss each of them with you. Instead, I hope that you take away a few key concepts from today's national security history lesson. First, that FISA, and the FISA courts, were created to provide an important check on executive power. That role is just as important today as it was in 1978, perhaps even more so in light of current events. Second, that each of the three branches of government worked together to reach the grand bargain that FISA represents, and that they continue to give and take as technology continues to evolve and as the United States continues to face threats both internal and external.

I sincerely hope you trust that the judiciary takes its constitutional and statutory oversight responsibilities very seriously; the executive appreciates that its agencies' determined efforts to protect the country from espionage and terrorist attack must comport with the fundamental principles embodied in our Constitution as judges interpret the law to guide their work; and, Congress continues to refine the statutory scheme in order to achieve the best possible balance between individual privacy and national security. Each branch, throughout FISA's complex history, has earnestly attempted—and continues to attempt—to "hold that delicate balance steady and true."

Thank you.