Article

No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror

Walter F. Mondale,[†] Robert A. Stein[††] & Caitlinrose Fisher[†††]

Secrecy, even what would be agreed by reasonable men to be necessary secrecy, has, by a subtle and barely perceptible accretive process, placed constraints upon the liberties of the American people.—Church Committee, 1976[1]

† Walter F. Mondale is a 1956 graduate of the University of Minnesota Law School, which now holds his name—Mondale Hall. He served on the *Minnesota Law Review* and as a law clerk for the Minnesota Supreme Court. Just four years out of law school, Mondale became the youngest Attorney General of Minnesota. Later, as a United States Senator, Mondale was an instrumental member of the Church Committee. He chaired the Domestic Task Force and investigated intelligence abuses against Americans by its own agencies. The Domestic Task Force uncovered numerous violations of constitutional rights, and the proposals of the Church Committee called for permanent Senate and House committees on intelligence that would have authority over the entire intelligence community. In 1976, Mondale was elected Vice President of the United States. In the White House, Mondale continued to shape intelligence policy. In particular, in 1978, the Foreign Intelligence Surveillance Act (FISA) was passed and the Foreign Intelligence Surveillance Court (FISC) was created to oversee requests for surveillance warrants against suspected foreign intelligence agents inside the United States. Mondale has a recurrent long-term interest in the operation of FISA and remains a strong advocate for the privacy rights of Americans.

†† Professor Robert A. Stein rejoined the faculty of the University of Minnesota Law School as Everett Fraser Professor of Law in the fall of 2006. Previously, from 1994 to 2006, Stein was the Executive Director and Chief Operating Officer of the American Bar Association (ABA), the world's largest voluntary professional membership association, with more than 400,000 members. Prior to that, Stein was Dean of the University of Minnesota Law School from 1979 to 1994 and was the first William S. Pattee Professor of Law from 1990 until 1994.

††† Caitlinrose Fisher received her J.D. *summa cum laude* from the University of Minnesota Law School in 2015. She is currently a law clerk on the United States Court of Appeals for the Ninth Circuit.

The authors wish to thank Frederick A.O. (Fritz) Schwarz, Jr., Elizabeth

INTRODUCTION

Our nation's founders put in place constitutional checks, such as the Fourth Amendment and three co-equal branches of government, to ensure that the very constitutional liberties we fight for abroad are not undermined domestically in the name of "foreign intelligence" and "national security." Since the founding of our republic, however, the government has struggled with maintaining an appropriate balance between gathering intelligence for national security purposes and protecting the privacy of United States citizens throughout the course of that intelligence gathering. Often in times of "crisis," executive and intelligence officials act with impunity under the guise of national security, eroding the very values that are the bedrock of our constitutional republic.

In response to executive overreach in the mid-twentieth century, the United States Senate formed the United States Select Committee to Study Governmental Operations with Respect to Intelligence Activities (Church Committee)[2]—a committee charged with investigating overreach and illegal activities by the executive branch.[3] The revelations of that committee led to significant reform, including: (1) the permanent establishment of congressional intelligence committees to oversee intelligence agencies, and (2) the enactment of the Foreign Intelligence Surveillance Act (FISA).[4] The lessons learned by the Church Committee and enshrined in FISA, however, were quickly forgotten in the wake of 9/11.[5]

Goitein, Faiza Patel, and Laura Donohue for their thoughtful comments on this Article. We are also grateful to Andrew Lugar, United States Attorney for the District of Minnesota, for providing us with a practical perspective of law enforcement challenges on the ground. Any errors are, of course, our own.

1. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, FOREIGN AND MILITARY INTELLIGENCE, S. REP. NO. 94-755, at 9 (1976) [hereinafter CHURCH COMM. REPORT, BOOK I].

2. The Church Committee is so named for its chairman, Senator Frank Church.

3. That committee engaged in the most "thorough investigation ever made of United States intelligence" and consisted of a staff of 100, which conducted over 800 interviews, 250 executive hearings, and compiled over 110,000 pages of documentation. CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 7.

4. An Act to Authorize Electronic Surveillance to Obtain Foreign Intelligence Information (Foreign Intelligence Surveillance Act of 1978), Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § 1801 (1978)).

5. *See* Margo Schlanger, *Infiltrate the NSA*, ATLANTIC (Dec. 30, 2014), http://www.theatlantic.com/politics/archive/2014/12/civil-libertarians-need-to

Two of the authors previously wrote an essay on the "strange and challenging subject" of national security and individual justice.[6] That essay, as does this Article, drew upon the unique perspective of Vice President Mondale to inform the authors' analysis of the appropriate balance between national security and personal liberties. As a senator, Vice President Mondale served on the Church Committee. In particular, Vice President Mondale served as chairman of the subcommittee that drafted the Church Committee's final report on domestic intelligence activities. Later, when in the White House, Vice President Mondale was not only instrumental to the passage of the Foreign Intelligence Surveillance Act but also served on the National Security Council, observing and working with executive intelligence agencies from a distinct perspective. The Vice President is described as someone who recognizes that "[c]ivil liberties and protecting homeland security are bound together, not inevitable foes," and "[o]pen government and loyalty are allies rather than tools of subversion."[7] Vice President Mondale thus offers a unique, pragmatic, and particularly informed perspective on maintaining an appropriate balance between security and liberty.

The parallels between the intelligence community's overreach that catalyzed the formation of the Church Committee and the current actions of the intelligence community are troubling.[8] We may lack a comprehensive report detailing the extent of modern government surveillance. But, there is evidence of misuse of surveillance technology by the government, and, because of a lack of meaningful congressional and judicial oversight, we can fairly infer that the government's use of surveil-

-infiltrate-the-nsa/383932 ("The intelligence scandals of the 1970s arose out of programs remarkably similar to post-9/11 mass surveillance.").

6. Walter F. Mondale, Robert A. Stein & Monica C. Fahnhorst, *National Security and the Constitution: A Conversation Between Walter F. Mondale and Robert A. Stein*, 98 MINN. L. REV. 2011 (2014).

7. Lawrence R. Jacobs, Walter F. Mondale: In the Tradition of James Madison (Apr. 2008) (unpublished essay), http://mondale.law.umn.edu/pdf/JacobsEssay.pdf.

8. Intelligence overreach is neither a partisan nor temporal issue. The Committee investigated six administrations from Franklin Roosevelt's through Richard Nixon's and concluded that all had abused their secret powers: "intelligence excesses, at home and abroad, have been found in every administration. They are not the product of any single party, administration, or man." SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at viii (1976) [hereinafter CHURCH COMM. REPORT, BOOK II].

lance technology has the potential to infringe on citizens' constitutional liberties. This Article addresses the myriad ways that FISA and today's Foreign Intelligence Surveillance Court (FISA Court or FISC)—established in response to the Church Committee's revelations—have veered off course from their original design, tipping the balance once again toward "national security" at the cost of fundamental constitutional liberties. Part I begins by providing a historical overview of the intersection between national security and personal liberties—from the original intent of the framers, to revelations of the Church Committee, to post-9/11 practices exposed by Edward Snowden and subsequent Freedom of Information Act (FOIA) requests. Part II explores the intelligence community's difficulty balancing intelligence operations with individual liberties, focusing on the ways in which post-9/11 amendments to FISA decrease the FISA Court's ability to serve its intended role as an impartial arbiter and check on intelligence agencies. Part III proposes a series of reforms that would realign intelligence activities and the FISA Court with the findings and recommendations of the Church Committee. Finally, Part IV concludes by considering broader systemic changes that should be made to ensure the intelligence community does not revert back to unconstitutional practices in the name of "security" when the next crisis arises.

Before diving into the delicate topic of the nexus between national security and individual liberty, we want to make a few points clear. We strongly support two goals: first, a vigorous and effective national security program; second, effective constraints on that program, to ensure national security is pursued within the bounds of the Constitution. We recognize and support the necessity of a strong and effective foreign intelligence program. It is a dangerous world and there are numerous real threats to the safety of the United States and its citizens. It is a first priority of government to provide for the safety of its citizens. An equally important obligation of our government, however, is to ensure preservation of the constitutional liberties established by our founders and developed through the decades, for which generations of Americans have given their lives to defend. We believe—as discussed throughout this Article—that it is necessary and possible to develop a strong and effective foreign intelligence program within the constitutional constraints established by our founders. Such a system is not only constitutionally required but also likely to result in more effective intelligence operations.

I. TOEING THE LINE BETWEEN SECURITY AND LIBERTY—A HISTORICAL PERSPECTIVE

After leaving England's system of unchecked monarchical authority, our nation's founding fathers recognized the importance of enshrining systems of checks and balances and separation of powers in the Constitution. One notable constitutional provision is the Fourth Amendment, which has evolved along with technology and notions of privacy. Since the founding of our nation, however, the coordinate branches of government have struggled with the scope of constitutionally protected personal liberties, especially in the wake of national tragedies such as 9/11. This Part traces the evolution of the relationship between the Fourth Amendment and surveillance in the name of "national security," beginning in Section A with seminal cases. Section B then turns to the intelligence community's invasion of personal liberties in the mid-twentieth century, which catalyzed the Church Committee and, eventually, FISA. Section C discusses fundamental changes Congress made to FISA in the wake of 9/11. Those changes eroded the structural and procedural protections recommended by the Church Committee and opened the door to intelligence overreach similar to what existed before the formation of the Church Committee. Section D concludes by discussing society's—and Congress's—response to that overreach, concluding with an overview of the recently enacted FREEDOM Act. This Part sets forth the push and pull historically inherent in the government's prioritization of intelligence and individual liberties.

A. FOUNDATIONAL PRINCIPLES

Central to the constitutional democracy envisioned by the founding fathers were personal liberties and privacy interests. The framers sought to create a system in which no single individual or entity would "be blindly trusted to wield power wisely."[9] This was not only a concern of the framers but also of the colonists in general—a core issue throughout ratification was whether the Constitution would establish sufficient checks on government so that the rights of the individual would not fall victim to the powers of the government.[10] The Fourth Amend-

9. FREDERICK A.O. SCHWARZ, JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED 2 (2007).

10. *See, e.g.*, *Debates in the Convention of the Commonwealth of Virginia, on the Adoption of the Federal Constitution*, *in* 3 DEBATES IN THE SEVERAL STATE CONVENTIONS, ON THE ADOPTION OF THE FEDERAL CONSTITUTION, AS

ment itself was a response to British kings' revenue officers' use of "general warrants" to conduct "unrestricted, indiscriminate searches of persons and homes."[11] Thus, the framers recognized the importance of individual liberties to the democratic society they envisioned and put specific provisions into the Constitution to ensure the protection of those liberties, regardless of the status of national and foreign policy.

The Fourth Amendment quickly operated as a check on executive authority, serving the role envisioned by the framers. The Fourth Amendment required following certain "judicial processes" to curb executive overreach.[12] For example, an impartial magistrate had to rule on the validity of a search *before* it was conducted.[13] These procedural requirements not only served to protect individual liberties but also sent a message to the executive branch that no person or entity, including those wielding the most power in society, was "above the law."[14]

As technology evolved (permitting intelligence agencies to collect significantly more information without ever entering a home) and intelligence agencies continued to push constitutional boundaries, the Supreme Court stepped in to limit domestic surveillance activities and redefine the scope of the Fourth Amendment. In *Katz v. United States*,[15] the Court overruled a prior decision[16] and held that the Fourth Amendment

RECOMMENDED BY THE GENERAL CONVENTION AT PHILADELPHIA IN 1787, at 44, 58, 445, 588, 663 (Jonathan Elliot ed., 2d ed., rev. vol. 1891).

11. SCHWARZ & HUQ, *supra* note 9, at 27–28. These "general warrants" raise similar concerns to the wiretaps used by the intelligence community today.

12. United States v. Jeffers, 342 U.S. 48, 51 (1951); *see also* Byars v. United States, 273 U.S. 28 (1926) (rejecting the argument that an unlawful search can be remedied by any evidence of wrongdoing it uncovers).

13. *See* Agnello v. United States, 269 U.S. 20, 32–33 (1925). Therefore, even if probable cause may have existed, without that determination prior to execution of the search, the search violated the Fourth Amendment. *See* Wong Sun v. United States, 371 U.S. 471, 481–82 (1963) (noting that the warrant requirement insures a "deliberate, impartial judgment" is "interposed between the citizen and the police").

14. Rule of law principles, drawn from the Magna Carta, greatly influenced the constitutional framers. One of the key tenants of the rule of law is "government by laws and not by men"—a concept attributable to Aristotle. *See, e.g.*, Robert Stein, *Rule of Law: What Does It Mean?*, 18 MINN. J. INT'L L. 293, 297 (2009).

15. 389 U.S. 347 (1967).

16. In *Olmstead v. United States*, 277 U.S. 438 (1928), the Supreme Court held that the Fourth Amendment only applied to tangible things, not the search and seizure of intangible things, such as conversations. In dissent, Justice Brandeis criticized the majority's narrow conception of searches, noting

prohibits warrantless electronic surveillance, recognizing that electronic surveillance can be just as intrusive as physically entering a private space.[17] However, *Katz* did not involve "national security," and the Court declined to consider the scope of the Fourth Amendment in the national security context. Injecting ambiguity into the opinion, the majority included a footnote stating that there may be an exception to the warrant requirement in cases involving "national security."[18] Concurring, Justice Douglas challenged the footnote, arguing that the President (or his agent) could "not [be] detached, disinterested, and neutral" in cases involving national security.[19] Justice Douglas concluded that the Fourth Amendment thus did not permit the executive branch to fulfill the inherently incompatible positions of adversary, prosecutor, and neutral/disinterested magistrate.[20]

In response to *Katz*, Congress enacted Title III of the Omnibus Crime Control and Safe Streets Act of 1968 to govern wiretapping and electronic surveillance.[21] In doing so, Congress codified the dicta in *Katz* and explicitly exempted any surveillance relating to "national security information" from Title III's

that "[t]he progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping" and questioning how it could be "that the Constitution affords no protection against such invasions of individual security." *Id.* at 474 (Brandeis, J., dissenting).

17. *Katz*, 389 U.S. at 353 ("The 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 . . . . The fact that the electronic device employed to achieve that end did not happen to penetrate the wall of the booth can have no constitutional significance."). This holding was subsequently codified in the Omnibus Crime Control and Safe Street Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 42 U.S.C. § 3711 (1968)).

18. *Katz*, 389 U.S. at 358 n.23 ("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.").

19. *Id.* at 359 (Douglas, J., concurring). Justice Douglas's concurrence was a response to Justice White's, which wholeheartedly supported permitting the executive alone to determine whether national security permitted deviation from the traditional warrant requirements. *See id.* at 364 (White, J., concurring) ("We should not require the warrant procedure and the magistrate's judgment if the President of the United States . . . has considered the requirements of national security and authorized electronic surveillance as reasonable."). The Church Committee revealed that Presidents and their subordinates abused their power in the very way feared by Justice Douglas—by invoking the term "national security" to justify excessive surveillance.

20. *Id.* at 360 (Douglas, J., concurring).

21. Omnibus Crime Control and Safe Street Act of 1968 §§ 801–804.

procedural requirements.[22] As later exposed by the Church Committee, in the years following *Katz* and Title III, enforcement officials utilized Title III's exception and conducted excessive surveillance in the name of "security," fulfilling Justice Douglas's prophecy. The scope of any national security exception to the Fourth Amendment warrant requirement thus quickly returned to the Supreme Court.

Within five years of *Katz* and the enactment of Title III, the Court was called upon to clarify the scope of *Katz*'s footnote twenty-three. In *United States v. United States District Court for the Eastern District of Michigan* (*Keith*),[23] the Court held that the Fourth Amendment prohibits warrantless electronic surveillance in cases of *domestic* security. *Keith* characterized *Katz* as recognizing that the "broad and unsuspected governmental incursions into conversational privacy which electronic surveillance entails necessitate the application of Fourth Amendment safeguards."[24] Central to the Court's reasoning was the risk of executive overreach in the name of national security. Because executive officers are "charged with . . . investigative and prosecutorial dut[ies], [they] should not be the sole judges of when to utilize constitutionally sensitive means in pursuing their tasks."[25] The Court stressed, however, that its decision was limited to domestic security and that the Court expressed no opinion on warrantless surveillance of "foreign powers or their agents."[26] Despite the Court's attempts to constrain executive surveillance authority in *Katz* and *Keith*, revelations of executive overreach in the name of "security" soon came to light, catalyzing the formation of the Church Committee and Foreign Intelligence Surveillance Court.

22. In whole, the Act stated that:

> Nothing . . . 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.

Id. § 802 (codified at 18 U.S.C. § 2511(3) (1968), *repealed by* Pub. L. No. 95-511, 92 Stat. 1783 (1978)).

23. 407 U.S. 297 (1972).

24. *Id.* at 313 (footnote omitted).

25. *Id.* at 317.

26. *Id.* at 321–22. Following *Keith*, the Justice Department limited warrantless wiretapping to cases "involving a 'significant connection with a foreign power, its agents or agencies,'" but did not apply that limitation to the NSA's electronic surveillance programs. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 189.

B. THE FORMATION AND RECOMMENDATIONS OF THE CHURCH COMMITTEE

For the majority of the twentieth century, the FBI, CIA, and NSA escaped meaningful congressional oversight and scrutiny. The Church Committee found that there was a "clear and sustained failure by those responsible to control the intelligence community and to ensure its accountability."[27] Minimal oversight occurred not only so that members of congress could plead ignorance of intelligence gathering activities but also because intelligence agencies, and the FBI in particular, "[had a] trove of embarrassing evidence" they could unleash on any public official.[28] In the 1970s, however, after the Watergate scandal and other revelations of executive overreach, Congress could no longer plead willful blindness.[29] On January 27, 1975, Congress established the Senate Select Committee to Study Government Operations with Respect to Intelligence Activity—or "Church Committee"—to investigate the "allegations of abuse and improper activities by the intelligence agencies" and "take action to bring the intelligence agencies [within] the constitutional framework."[30] The Church Committee found that the executive branch had engaged in decades of warrantless electronic surveillance under the guise of "national security," predominantly by relying on "vague" and "fuzzy loopholes" in the law.[31]

27. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 15; *see also* SCHWARZ & HUQ, *supra* note 9, at 20 (noting that it was "easier" and "safer" to give intelligence agencies "a free pass than to do any oversight"). As Senator Mike Mansfield observed, it was "fashionable . . . for members of Congress to say that insofar as the intelligence agencies were concerned, the less they knew about such questions, the better." *Id.*

28. SCHWARZ & HUQ, *supra* note 9, at 19–20.

29. *Id.* at 20.

30. CHURCH COMM. REPORT, BOOK I, *supra* note 1, at III (Letter of Transmittal by Senator Frank Church, Committee Chairman). The Committee's charge was two-fold: first, the Committee investigated charges of wrongdoing; second, and more important to our inquiry, the Committee sought "to learn enough about [the intelligence agencies'] past and present activities to make the legislative judgments required to assure the American people that whatever necessary secret intelligence activities were being undertaken were subject to constitutional processes." *Id.* at 5. As an example of the type of illegal government activity to be investigated, the Senate listed "CIA domestic activities." CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 1 n.1.

31. SCHWARZ & HUQ, *supra* note 9, at 27–29; *see, e.g.*, CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 302 (describing the exceedingly broad and vague "foreign intelligence" standard). For example, the CIA positively engaged in subversion and sabotage under a vague catchall provision of the 1957 National Security Act, which authorized the CIA "to perform such other functions and duties related to intelligence affecting the national security as the

The scope of domestic surveillance was troubling. Often, groups and individuals were targeted for their political opinion rather than any risk to national security. Under the guise of "national security," intelligence agencies collected information on: women who attended "Women's Liberation Movement" meetings;[32] Dr. Martin Luther King, Jr., members of the National Association for the Advancement of Colored People (NAACP), and other supporters of the civil rights movement;[33] anti-Vietnam protestors;[34] student groups, including Students for a Democratic Society and "every Black Student Union and similar group";[35] and even members of congress.[36] The FBI gathered intelligence about the above-mentioned (and other) groups allegedly to determine whether communists were infiltrating organizations, although the FBI also documented legitimate activities unrelated to communist infiltration.[37]

Intelligence agencies collected intelligence through a variety of means. Agencies "frequently wiretapped and bugged American citizens without the benefit of judicial warrant."[38] The NSA obtained millions of private telegrams from 1947 to 1975 under a secret arrangement with private telegraph companies.[39] The CIA also instituted a mail-opening program, focusing on mail sent between the Soviet Union and United States.[40] The CIA and NSA would then share the information collected (which rarely distinguished between foreign and domestic targets) with the FBI, for domestic law enforcement purposes.[41] Despite the clear infringements on individual priva-

National Security Council may from time to time direct." CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 44.

32. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 7.

33. *Id.* at 7–9, 50, 71–72, 167. The Church Committee collected extensive information on the surveillance of Dr. Martin Luther King, Jr. The FBI launched a campaign against Dr. King intended to "'neutralize' him as an effective civil rights leader." *Id.* at 11. Attorney General Robert Kennedy approved the bugging of Dr. King's home. *Id.* at 118. For an in-depth discussion of surveillance of Dr. King, see *id.* at 219–23.

34. *Id.* at 49. The CIA collected intelligence on anti-war protestors at the request of both Presidents Johnson and Nixon. *Id.* at 98.

35. *Id.* at 8–9.

36. *Id.* at 8–10.

37. *See id.* at 48–49, 81–82, 175, 179–80.

38. *Id.* at 12. Government officials would often break in and install microphones to capture the conversations of individuals and organizations. *See id.* at 13, 60.

39. *See id.* at 6, 168.

40. *See id.* at 58–59.

41. *See id.* at 59.

cy, "question[s] of legality or constitutionality" were either not raised or consciously disregarded.[42]

The Church Committee identified four fundamental institutional flaws that permitted intelligence agencies to subvert personal liberties in the name of national security. First, national security institutions and laws were organized under "ambiguous laws and fuzzy instructions."[43] Malleable terms such as "subversion," "national security," and "foreign intelligence" provided intelligence agencies with fodder to collect excessive information.[44] Second, senior executive officials furthered a culture of impunity by giving implicit orders to violate the law.[45] Third, the intelligence community presumed absolute and permanent secrecy of their operations.[46] Without anticipated testing of actions by Congress and the public, those agencies acted with greater impunity and less adherence to reasonable interpretations of the law. Finally, due to a lack of congressional oversight,[47] intelligence agencies acted like a "monarchical executive,"[48] unaccountable to any coequal branch of government. Essentially, the Committee reaffirmed a principle recognized by the founding fathers—"unchecked power is prone to unwise, inefficient application and . . . leads inescapably to abuse."[49]

Because of the Church Committee's revelations, Congress created the Senate and House Select Committees on Intelligence to provide the requisite "oversight" of intelligence agen-

42. *Id.* at 140–46.

43. SCHWARZ & HUQ, *supra* note 9, at 5; *see* CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 4 ("Where statutes do exist, as with the CIA, they are vague and have failed to provide the necessary guidelines defining missions and limitations."); CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 165 ("The absence of precise standards for intelligence investigations of Americans contributed to overbreadth.").

44. SCHWARZ & HUQ, *supra* note 9, at 31; *see also* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 24–28 (describing the ambiguity of the term "subversive").

45. *See* CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 11.

46. *See id.* at 11–12.

47. *See id.* at 11 ("[I]t is clear that Congress did not carry out effective oversight.").

48. SCHWARZ & HUQ, *supra* note 9, at 2–3. The "monarchical executive" theory is essentially one of "unchecked presidential power." *Id.* at 1–2. As noted by Frederick A.O. Schwarz, Jr., this theory has been "deployed to many ends," including "to spy on Americans' telephone calls and e-mails in violation of federal statutes and, at times, the Fourth Amendment; and to infiltrate and keep watch on domestic groups protesting government policy." *Id.* at 2.

49. *Id.* at 50.

cies,[50] and enacted the Foreign Intelligence Surveillance Act of 1978[51] to provide a more concrete legal framework capable of limiting and guiding intelligence agencies. These changes were intended to "strik[e] a fair and just balance between protection of national security and protection of personal liberties."[52] The intelligence committees would serve as a permanent check on executive authority, deterring intelligence agencies from engaging in the overreach that led to the formation of the Church Committee. And newly enacted legislation, such as FISA, established more concrete statutory guidance and limitations on the power of those agencies. The Act also created the Foreign Intelligence Surveillance Court.[53] FISC is "a specialized Article III court established under FISA to review and approve governmental applications" seeking to obtain intelligence through certain methods.[54] FISA also created the Foreign Intelligence Surveillance Court of Review (FISCR), to which the government may appeal denials of applications to conduct surveillance.[55]

From 1978 to 2001, Congress and the executive branch adhered to the model recommended by the Church Committee,

50. S. Res. 400, 94th Cong. (1976); H.R. Res. 591, 94th Cong. (1976).

51. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § 1801 (1978)); *see also* S. REP. NO. 95-604, at 7 (1977) (stating that Congress enacted FISA "in large measure [as] a response to the revelations that warrantless electronic surveillance in the name of national security ha[d] been seriously abused").

52. S. REP. NO. 95-604, at 7.

53. Foreign Intelligence Surveillance Act of 1978 § 103(a). FISC is composed of eleven district court judges appointed by the Chief Justice of the United States. Additionally, there is a Foreign Intelligence Surveillance Court of Review, with jurisdiction to hear appeals from the government. That court is composed of three judges designated by the Chief Justice. For a general background of the composition of FISC, see generally ELIZABETH B. BAZAN ET AL., CONG. RESEARCH SERV., RL33833, THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND THE U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW: AN OVERVIEW (2007) (discussing the creation and structure of the Foreign Intelligence Surveillance Court and the Foreign Intelligence Court of Review).

54. EDWARD C. LIU ET AL., CONG. RESEARCH SERV., R43459, OVERVIEW OF CONSTITUTIONAL CHALLENGES TO NSA COLLECTION ACTIVITIES AND RECENT DEVELOPMENTS 1–2 (2014). Initially, FISA only authorized wiretaps and bugs, but it was subsequently amended to cover physical searches, pen registers and trap and trace devices, and business records. *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601(2), 112 Stat. 2396, 2404–05 (codified at 50 U.S.C. § 1843 (1999)); Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807(a)(3), 108 Stat. 3423, 3443 (codified at 50 U.S.C. § 1827 (1994)).

55. Foreign Intelligence Surveillance Act of 1978 § 103(b).

and three key components of FISA and the FISA Court remained intact. First, the FISA Court only approved applications for individualized warrants before a search occurred.[56] Second, those warrants only approved gathering of intelligence information from "foreign power[s]" or "agents of foreign power[s]."[57] And third, the information requested, if it related to or concerned a United States person, had to be "necessary" to obtaining foreign intelligence information.[58] Those key components changed drastically in the wake of 9/11.

C. ALTERING THE BALANCE POST 9/11

Two laws significantly changed FISA and FISC in the wake of 9/11. First, in 2001, Congress enacted the PATRIOT Act,[59] which expanded the scope of information subject to FISA orders.[60] Second, in the FISA Amendments Act of 2008 (FAA),[61] Congress created a statutory regime for collecting foreign intelligence information, which was previously governed by executive order.[62] Together, these changes opened the door for the executive branch to expand the scope of signals intelligence—or electronic communications and business records about those communications—collected.[63] Each statutory change will be addressed in turn.

56. The Department of Justice's Office of Legal Counsel relied on the individual warrant requirement to establish FISA/FISC's conformity with Article III of the Constitution.

57. Foreign Intelligence Surveillance Act of 1978 § 101(e)(1)(A) (defining "foreign intelligence information").

58. *Id.* § 101(e)(1).

59. Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

60. As will be discussed later, it was a broad view of the term "relevant" that led FISC to secretly rule that the PATRIOT Act permitted bulk collection of metadata.

61. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. § 1801 (2008)).

62. *See generally* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 144–53 (2015) [hereinafter Donohue, *Section 702*] (describing the evolution of the FISA Amendments Act).

63. Signals intelligence is the information captured pursuant to current programmatic surveillance. *See* Nat'l Research Council, Bulk Collection of Signals Intelligence: Technical Options S-2 (2015) (prepublication copy).

The PATRIOT Act modified various provisions of FISA and expanded the scope of information subject to FISC warrants.[64] Prior to the PATRIOT Act, the government could request business records solely from common carriers if and only if the government provided "specific and articulable facts" that the person the records pertained to was a "foreign power or agent of a foreign power."[65] Under Section 215 of the PATRIOT Act, the FBI could now apply to FISC for an order permitting "the production of *any tangible thing*[]" (not only business records) from any business (not only common carriers).[66] Moreover, while the government previously had to show that the subject of the business records request was a foreign power or its agent, the new law permitted the government to obtain any tangible thing so long as there were reasonable grounds to believe it was "relevant" to an authorized investigation.[67] The "foreign power/agent of a foreign power" requirement was similarly replaced with a mere "relevance" standard for Pen Register and Trap and Trace orders, which allow the government to track numbers calling in or from a given phone number.[68] These changes reduced FISC's ability to thoroughly examine and question the government's need for a given search warrant.

Although the PATRIOT Act seemingly retained the requirement of individualized court orders, the administration

64. Section 215 of the PATRIOT Act amended 50 U.S.C. § 1861 and expanded the ability of intelligence agencies to obtain information from businesses. USA PATRIOT Act § 215 (permitting the FBI to request the production of "any tangible thing[]"). Prior to the PATRIOT Act, Congress amended various provisions of FISA to cover: (1) physical searches, Intelligence Authorization Act for Fiscal Year 1995, Pub L. No. 103-359, § 302(c), 108 Stat. 3423, 3445 (codified as amended at 50 U.S.C. §§ 1821–1829 (1994)); (2) pen-trap and trace devises, Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396, 2404–10 (codified as amended at 50 U.S.C. §§ 1841–1846 (1998)); and (3) searches of business records, *id.* § 602. *See generally* Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 793–802 (2014) [hereinafter Donohue, *Bulk Metadata Collection*] (describing evolution of FISA and the metadata collection program).

65. *See* Intelligence Authorization Act for Fiscal Year 1999 § 602.

66. USA PATRIOT Act § 501 (emphasis added) (expanding the definition of "business record" to include "any tangible things (including books, records, papers, documents, and other items)"); *see* Donohue, *Bulk Metadata Collection*, *supra* note 64, at 797–98.

67. Intelligence Authorization Act for Fiscal Year 1999 § 505.

68. *Id.* § 404(c)(2) (requiring the government to certify that the "information likely to be obtained is relevant to an ongoing foreign intelligence or international terrorism investigation"); *see* 18 U.S.C. § 3127(3) (2012) (defining pen register); *id.* § 3127(4) (defining trap and trace device).

ignored that requirement. Relying on the President's "inherent" constitutional authority, the executive branch engaged in "bulk collection" of both phone and Internet metadata without any involvement of the FISA Court.[69] Eventually, to salvage these programs, the administration sought to bring them under the auspices of FISA and the FISA Court, arguing that the term "relevant" justified mass collection of phone and Internet data.[70] In decisions that remained confidential until Snowden's disclosures, FISC accepted this seemingly limitless interpretation of the word "relevant."[71] Indeed, a 2013 FISC decision went so far as to hold that *all* Americans' phone records were relevant to authorized international terrorism investigations because they may be used in some unforeseen, future search.[72]

The PATRIOT Act modified not only the scope of searchable material but also the standard applicable to obtaining surveillance authorization. Previously, the executive branch had to establish that the "purpose" of the surveillance was to obtain intelligence information. Courts interpreted the "purpose" language to mean "primary purpose," requiring the government to show that gathering foreign intelligence (rather than, say, criminal prosecution) was the primary purpose of the surveil-

69. Letter from Alberto R. Gonzales, Attorney Gen., U.S. Dep't of Justice, to Patrick Leahy and Arlen Specter, Comm. on the Judiciary, U.S. Senate (Jan. 17, 2007) (explaining the administration's position on the legality of the Terrorist Surveillance Program); *see also* OFFICE OF INSPECTOR GEN., OVERSIGHT & REVIEW DIV., A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S ACTIVITIES UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 2008 (2012) [hereinafter OIG REPORT, SECTION 702]; SCHWARZ & HUQ, *supra* note 9, at 125 (describing the development of FISA after September 11, 2001). After public exposure of that warrantless surveillance, the administration brought its mass surveillance program once again before the FISC. *See* OIG REPORT, SECTION 702, *supra*, at 9–11.

70. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 12 (July 2, 2014) [hereinafter PCLOB REPORT, SECTION 702]. A separate type of information is also collected under Section 702, referred to as "upstream" collection. Rather than merely collecting information to or from a given selector, upstream collection captures entire transactions and communications travelling across the Internet "backbone," which may mention, but do not contain, the selector. *See id.*

71. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, slip op. at 18–23 (FISA Ct. 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf; *see also* ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 22 (2015) (explaining FISC's interpretation of the word "relevance").

72. *In re Order Requiring the Prod. of Tangible Things*, No. BR 13-109, slip op. at 28–29.

lance.[73] The PATRIOT Act amended FISA so that gathering intelligence only had to be a "significant purpose" of the surveillance,[74] and permitted law enforcement agencies to share information acquired through FISA searches.[75] This change permitted the executive branch to comingle law enforcement and intelligence activities to a greater extent and inserted into the statutory scheme the ambiguity inherent in the term "significant."[76]

In 2008, Congress altered FISC's role and relationship to the executive branch once again through the FISA Act Amendments, further eroding portions of FISA that codified the Church Committee's structural and procedural recommendations. Of particular relevance, Section 702 codified new procedures for targeting non-United States persons abroad. First, the FAA eliminated the requirement for individual court orders, even if a United States citizen's information would be collected, so long as the American was not the "target" of the surveillance.[77] The NSA then interpreted the FAA to permit not

73. *See* USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified as amended at 50 U.S.C. § 1804(a)(7) (2012)).

74. *Id.*; *see also In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (holding that FISA did not require the government to show that its primary purpose in undertaking the surveillance was not criminal prosecution and that the "significant purpose" test did not violate the Fourth Amendment).

75. USA PATRIOT Act § 203(b)(1) ("Any investigative or law enforcement officer . . . who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement . . . official to the extent such contents include foreign intelligence . . . ."); *see also* DEP'T OF JUSTICE, THE USA PATRIOT ACT: PRESERVING LIFE AND LIBERTY, http://www.justice.gov/archive/ll/what_is_the_patriot_act.pdf (last visited Apr. 11, 2016) (noting that the PATRIOT Act "facilitated information sharing and cooperation among government agencies so that they can better 'connect the dots'").

76. *See, e.g.*, Memorandum from Deputy Assistant Judge Advocate Gen., Nat'l Sec. Litig. & Intelligence Law, to Judge Advocates (Sept. 4, 2003), http://fas.org/irp/agency/doj/fisa/navy0903.pdf (discussing the PATRIOT Act's changes to FISA). This potential for commingling intelligence and enforcement activities led to abuse and misstatements to FISC regarding the scope of FISC-approved searches. For example, one FISA certification erroneously stated "that the target of the FISA [search] was not under criminal investigation." *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002). This led the FISA Court to "h[o]ld a special meeting to consider the troubling number of inaccurate FBI affidavits in so many FISA applications." *Id.*

77. However, "if an individual is not *known* to be a U.S. person . . . then the NSA assumes that the individual *is* a non-U.S. person." Donohue, *Section 702*, *supra* note 62, at 158 (emphasis added). Information about U.S. persons

only acquiring information to and from targets of surveillance but also information *about* targets of surveillance in certain contexts, even if the communication was between two non-foreign individuals.[78] The FAA also required the government to establish targeting and minimization procedures to reduce the risk of capturing non-target communications.[79] Unlike the original design of FISA, where FISC adjudicated individual warrant determinations *before* any targeting occurred, the FAA transformed FISC into a meta-arbiter, approving generally applicable targeting and minimization procedures that applied *after* a search occurred.[80]

The FAA also extended the scope of "foreign" targets falling within FISC's protection and jurisdiction. Whereas FISA originally limited intelligence agencies to collecting information from "foreign powers" and "agents of foreign powers"—language that intentionally tracked *Keith*[81]—the FAA extended FISC jurisdiction to "*any* non-U.S. person overseas" so long as collecting that intelligence furthered the goals of collecting "foreign intelligence."[82] Five years after its enactment, Congress reauthorized the FAA with little debate, despite senators previously expressing concern over the scope of information collected.[83]

---

could be acquired in a variety of other ways. For example, information could be acquired when a U.S. person communicates with a non-U.S. person or when two non-U.S. persons discuss a U.S. person. Also, given the complexity of the collection program, sometimes a U.S. person would be "inadvertent[ly]" targeted. PCLOB REPORT, SECTION 702, *supra* note 70, at 6.

78. Donohue, *Section 702*, *supra* note 62, at 161–64.

79. Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436, 2438 (codified at 50 U.S.C. § 1881a (2008)).

80. *Id.* For a detailed description of the evolution of the FAA and the changes it made to FISA, see Donohue, *Section 702*, *supra* note 62, at 124–53.

81. The *Keith* court expressly declined to opine on the government's surveillance authority over "foreign powers or their agents." United States v. U.S. District Court (*Keith*), 407 U.S. 297, 321–22 (1972) ("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.").

82. *Id.*

83. *See* Donohue, *Section 702*, *supra* note 62, at 156–57. As chronicled by national security scholar Laura Donohue, by 2012,

> [M]ore than a dozen senators had joined a letter to Director of National Intelligence James R. Clapper, expressing alarm that the intelligence community ha[d] stated that 'it is not reasonably possible to identify the number of people located inside the United States whose communications may have been reviewed' under the FAA.

Id.

The PATRIOT Act and FAA represented a step back from the Church Committee's structural and procedural recommendations. First, the Committee noted that intelligence agencies need specific and restricted statutory mandates—the potential for abuse of intelligence authority is too great when agencies operate under "fuzzy" and "ambiguous" directives.[84] However, after 9/11, the warrant parameters were ambiguous: rather than being tied to foreign powers and their agents, searches just had to be "relevant" to "foreign intelligence" investigations; rather than authorizing searches for the primary purpose of national security, that purpose just had to be "significant."[85] Second, the Committee recognized that, to the extent possible, intelligence agencies need continuous oversight.[86] However, after 9/11, the FISA Court had to take the government's word that a given search was "relevant" to a foreign intelligence investigation, and the court no longer pre-approved warrants *before* a search, but rather approved general procedures to apply *after* intelligence agencies gathered information.[87] These statutory changes represented a return to pre-Church Committee processes and tipped the scale once again toward "security" at the expense of "liberty."

D. THE SNOWDEN DISCLOSURES AND FREEDOM ACT

The PATRIOT Act and FAA, together with confidential statutory and constitutional interpretation on the part of the FISA Court, provided intelligence agencies with the necessary fodder to act with impunity like pre-Church agencies. Intelligence agencies conducted expansive searches and collected vast amounts of private information, all without the public's knowledge. That veil of secrecy fell in June of 2013, when Edward Snowden, a former NSA contractor and CIA employee, began releasing classified information about NSA surveillance

84. *See supra* notes 43–44 and accompanying text.

85. The 9/11 Commission, for example, found that intelligence agencies acted with "little guidance" from Congress in the wake of 9/11 and evolving national security threats. *See* EXECUTIVE SUMMARY, THE 9/11 COMMISSION REPORT: FINAL REPORT ON THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 15–16 (2004), http://www.9-11commission.gov/report/911Report_Exec.pdf.

86. *See id.* at 25–26.

87. *See supra* note 80 and accompanying text. FISC still approves individualized warrants, but this Article focuses on post-9/11 changes to FISC's jurisdiction.

activities.[88] Among other things, Snowden disclosed a sweeping FISC opinion, in which FISC ordered Verizon Communications to furnish all telephone metadata to the NSA once a day under the auspices of Section 215 of the PATRIOT Act.[89] Regardless of whether Snowden is considered a whistleblower or a traitor, he catalyzed a conversation about government secrecy, as a result of which Congress enacted the FREEDOM Act.[90]

On June 2, 2015, one day after the expiration of Section 215, Congress enacted the FREEDOM Act,[91] for the purpose of "prohibit[ing] bulk collection of records under Section 215 of the USA PATRIOT Act."[92] Among other things, the Act requires FISC to publish opinions in certain circumstances[93] and establishes a system for the appointment of amicus curiae.[94] According to the House Judiciary Report, "[t]he Act creates a new program for the targeted collection of telephone metadata, provides greater privacy and civil liberties protections for Americans, expands existing congressional oversight provisions, and creates greater transparency of national security programs operated pursuant to FISA."[95] The FREEDOM Act *does* accomplish each of the aforementioned goals—but, given the status quo before its enactment, saying that it "improves" liberty protections and congressional oversight is not, by itself, saying too much.[96]

88. *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; *see also* Tom McCarthy, *Edward Snowden Identifies Himself as Source of NSA Leaks—As It Happened*, GUARDIAN (June 9, 2013, 5:16 PM), http://www.theguardian.com/world/2013/jun/09/nsa-secret-surveillance-lawmakers-live.

89. *See* H.R. REP. NO. 114-109, pt. 1, at 2 (2015); Ian Black, *NSA Spying Scandal: What We Have Learned*, GUARDIAN (June 10, 2013, 2:48 PM), http://www.theguardian.com/world/2013/jun/10/nsa-spying-scandal-what-we-have-learned; *see also In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 06-05 (FISA Ct. May 24, 2006). The NSA collected information from not only Verizon but also other U.S. telecommunications providers. *See* H.R. REP. NO. 114-109, pt. 1, at 8.

90. *See* H.R. REP. NO. 114-109, pt. 1, at 2–10 (describing the background of, and the need for, legislation).

91. Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline over Monitoring (FREEDOM) Act of 2015, Pub. L. No. 114-23, 129 Stat. 268 (2015).

92. H.R. REP. NO. 114-109, pt. 1, at 2.

93. *See* FREEDOM Act § 402.

94. *See id.* § 401.

95. H.R. REP. NO. 114-109, pt. 1, at 2.

96. Throughout the remainder of this Article we will note where the

II. INFRINGEMENTS ON CONSTITUTIONAL RIGHTS IN THE NAME OF SECURITY

As discussed in Part I, the PATRIOT Act and FAA inserted ambiguity and expansive executive authority—two characteristics the Church Committee recognized contributed to executive overreach—into FISA's framework. Both the intelligence community, exercising wide-ranging investigative authority, and the FISA Court, avoiding questioning executive action in the delicate area of national security, embraced this ambiguity and newly sanctioned authority. Those structural changes set society up for another pre-Church Committee moment, particularly when coupled with unnecessary secrecy and a culture of impunity.

This Part explores the impact the PATRIOT Act and FAA had on civil liberties. Lessons learned by the Church Committee and memorialized in FISA were quickly forgotten in the wake of the "War on Terror." Because of statutory changes to FISA, intelligence agencies were in a position to broadly construe "foreign intelligence" and other ambiguous statutory terms, and to permit a desire for national security to infringe upon citizens' constitutional liberties. Although we lack a comprehensive report detailing executive overreach, there remains evidence of misuse of executive authority, and we can infer additional, unknown infringements on constitutional liberties are occurring.

Drawing from the findings of the Church Committee and intent of FISA's drafters, this Part discusses where Congress, intelligence agencies, and the FISA Court strayed from the original design of FISA and FISC. Section A begins by analyzing the bulk collection of individual metadata, via both phone and Internet searches. These programs emerged from the PATRIOT Act and were sanctioned by questionable, and secret, statutory interpretation on the part of the FISA Court. Section B discusses FISC's role post-FAA as an adjudicator of procedures as opposed to individual cases and controversies. Section C pulls back from specific FISC holdings and discusses the culture of impunity that flourished in the wake of 9/11. This culture pervaded the relationship between intelligence agencies and FISC—with intelligence agencies misleading FISC as to the scope of intelligence programs and violating the (limited)

FREEDOM Act has the potential to significantly rein in intelligence overreach and also where the Act is ambiguous enough to leave the door open, once again, for abuse and misuse of executive authority.

restrictions the court imposed on those programs. Finally, Section D suggests that all these potential constitutional violations continued until Snowden's disclosures because of a culture of secrecy and the de minimis potential for collateral review. First, the executive branch increased its invocation of, and expanded the scope of, the state secrets doctrine, precluding judicial review of FISA-related information in public Article III courts. Second, FISC engaged in significant confidential statutory and constitutional interpretation. Combined, these actions have encroached upon constitutionally protected civil liberties and undermined public trust in the government.

A. BULK COLLECTION

After 9/11, intelligence agencies began engaging in bulk collection of phone and Internet "metadata"[97]—information about the telephone numbers dialed, e-mail addresses contacted, and the time and length of calls/e-mails, as opposed to the content of a communication.[98] Although this collection initially took place without judicial authorization, the FISA Court—via confidential opinions—ultimately approved the bulk collection of both telephone and Internet data. These rulings placed "few limits on the government's ability to *collect and retain* large amounts of domestic and international telephone records," but did slightly limit the government's ability to "*search or make further use* of the collected metadata."[99]

The FISA Court held that the collection of telephone and Internet metadata is both statutorily—under a broad interpretation of the term "relevance"—and constitutionally author-

97. The term "bulk" is used to distinguish from the "narrower collection of metadata pertaining to an identified individual or group of individuals." LIU ET AL., *supra* note 54, at 2. See *id.* for a general discussion of the bulk collection program.

98. *See* GOITEIN & PATEL, *supra* note 71, at 21. For a detailed discussion of how much information is obtained from metadata, see *Klayman v. Obama*, 957 F. Supp. 2d 1, 35–36 (D.D.C. 2013), *vacated*, 800 F.3d 559 (D.C. Cir. 2015) ("[T]he 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.").

99. LIU ET AL., *supra* note 54, at 3. The limitation on the executive's authority to search the metadata was scant. First, it only required "reasonable articulable suspicion" (RAS)—a lesser standard than probable cause. *Id.* at 4. Second, it was the agency itself ("a relatively small group of NSA personnel") that determined whether RAS existed to search a particular query. *Id.* After the Snowden disclosures, however, President Obama asked FISC to make the RAS determination. *See id.*

ized.[100] In particular, the court held that metadata "is not protected by the Fourth Amendment because users of e-mail [and telephones] do not have a reasonable expectation of privacy" of "non-content addressing information," since that information is shared with third-party providers, such as Verizon.[101] The court admitted, however, that it was interpreting FISA to "encompass an exceptionally broad form of collection," and that such an interpretation may not have been appropriate under FISA before the PATRIOT Act.[102] Essentially, "[b]y 2007, the FISA [C]ourt and Congress had together, and mostly in secret, broadened FISA into a bulk surveillance statute."[103]

The public remained unaware of this bulk collection until Edward Snowden exposed the NSA's activities in 2013. Once exposed to the public, however, civil society—and, to a lesser extent, Congress—began mobilizing against the bulk collection of metadata. Multiple bills were proposed in Congress that would curtail the program, which expired on June 1, 2015.[104] Before Congress acted, however, the Second Circuit issued an opinion striking down the bulk collection under Section 215 on statutory, rather than constitutional, grounds.[105] The court held that the government read the term "relevant"—added to FISA by the PATRIOT Act—far too broadly,[106] reasoning that the

100. The FISA Court held that "[i]nformation is 'relevant' to an authorized international terrorism investigation if it bears upon, or is pertinent to, that investigation." *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [REDACTED], No. BR 13-109, slip. op. at 18 (FISA Ct. Aug. 22, 2013), http://www.fisc.uscourts.gov/sites/default/files/BR%2013-109%20Order-1.pdf (quoting Government's Memorandum of Law in Support of Application for Certain Tangible Things for Investigations To Protect Against Int'l Terrorism, No. BR 05-06, at 13–14 (filed May 23, 2006)). Although the bulk collection of telephone metadata received greater media attention, the reasoning for that opinion came largely from a prior opinion authorizing bulk collection of Internet metadata. *See* GOITEIN & PATEL, *supra* note 71.

101. Internet Metadata Opinion and Order, No. PR-TT [REDACTED], slip op. at 19 (FISA Ct. 2006), http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf; *see also id.* at 58–61 (explaining the court's determination that the surveillance complied with the Fourth Amendment).

102. *Id.* at 23.

103. Schlanger, *supra* note 5.

104. *See* H.R. REP. NO. 114-109, pt. 1, at 3 (2015) (describing the background of the FREEDOM Act and noting that "various recommendations" for reform were proposed before the Act was passed).

105. *See* Am. Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015).

106. *See id.* at 812 (rejecting the government's argument that metadata is relevant if it "may allow the NSA, at some unknown time in the future, utiliz-

government cannot "collect phone records *only because* they *may become relevant* to a possible authorized investigation in the future."[107] The panel recognized that to hold otherwise would be conceding limitless authority to the NSA under Section 215.[108]

In response to the Second Circuit's decision and mounting public pressure, Congress enacted the FREEDOM Act, which technically eliminated Section 215's authorization of "bulk collection" of metadata.[109] The FREEDOM Act, however, was ambiguous as to whether bulk collection could continue during a 180-day transition period.[110] In June, the FISA Court disagreed with the Second Circuit's statutory interpretation, held that the program was statutorily authorized, and permitted its continued use during the FREEDOM Act's transition period.[111]

The bulk collection of information is a troubling departure from the original intent of Congress in enacting FISA against the immediate backdrop of the Church Committee's findings and recommendations. This bulk collection represented a return to pre-Church Committee government practices. Under the auspices of broad and ambiguous language, intelligence agencies were free to collect vast amounts of information about citizens without the individualized protections of the Fourth

ing its ability to sift through the trove of irrelevant data it has collected up to that point, to identify information that *is* relevant").

107. *Id.* at 818 (emphasis added).

108. *See id.*

109. *See generally* H.R. REP. NO. 114-109, pt. 1, at 5–9 (2015) (describing the need for legislation). Enacting the FREEDOM Act was no simple task and highlights the controversies often associated with regulating the relationship between security and personal liberties. Congress was unable to enact a law by the time Section 215 technically expired. The delays resulted in part from a filibuster by Senator Rand Paul, who argued that the FREEDOM Act did not do enough to protect liberty and privacy. *See* Jeremy Diamond, *Rand Paul Wraps 10-Hour "Filibuster" over NSA Surveillance Program*, CNN (May 21, 2015, 7:31 AM), http://www.cnn.com/2015/05/20/politics/rand-paul-filibuster-patriot-act-nsa-surveillance.

110. *See In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, slip op. at 10 (FISA Ct. June 29, 2015) (acknowledging that there was a question as to "whether Congress has authorized bulk acquisition of call detail records during the [FREEDOM Act's] interim 180-day period").

111. *See id.* at 9–11. The court stated that "Second Circuit rulings are not binding on the FISC, and this Court respectfully disagrees with that Court's analysis." *Id.* at 14–15; *see also* Charles Savage, *Surveillance Court Rules that N.S.A. Can Resume Bulk Data Collection*, N.Y. TIMES (June 30, 2015), http://www.nytimes.com/2015/07/01/us/politics/fisa-surveillance-court-rules-nsa-can-resume-bulk-data-collection.html.

Amendment.[112] Bulk collection is at odds with FISA's original intent in two ways in particular. First, it puts FISC in the position of approving broad searches, as opposed to individual warrant applications in concrete and limited cases and controversies. Such broad approvals are not a common characteristic of Article III courts. Second, bulk collection increases the possibility of the misuse of information. FISC itself recognized, and attempted to rein in, the intelligence community's misuse of the diverse material collected.[113]

Congress did attempt to address these diversions from FISA's original intent in the FREEDOM Act. In an attempt to rein in the "bulk collection" of metadata exposed by Snowden, the FREEDOM Act supplements the ambiguous "relevance" standard by requiring that a "specific selection term" be used as the basis for the production of "tangible things"[114] and "pen register" searches.[115] It remains to be seen, however, whether the FREEDOM Act significantly limits the potential for encroachment on First and Fourth Amendment protections and the

112. For example, the FAA expanded the scope of foreigners that the government could target. The government did not have to show it was targeting a "foreign power" or an "agent of a foreign power," the very key words invoked by the *Keith* Court and used elsewhere in FISA. Instead, the government could target *any* non-U.S. person overseas for the purpose of collecting "foreign intelligence information." *See supra* notes 62, 81–83 and accompanying text.

113. *See infra* Part II.C. *But cf.* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., 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 9–10 (Jan. 23, 2014) [hereinafter PCLOB REPORT, SECTION 215] (finding that "compliance issues" resulted from the complexity and scope of the program, rather than bad faith actions of program administrators).

114. FREEDOM Act, Pub. L. No. 114-23, § 103, 129 Stat. 268, 272 (codified at 50 U.S.C. § 1803 (2015)).

115. *Id.* § 201. It is particularly concerning that the "relevance" standard remains in the FREEDOM Act. As discussed above, the bulk collection program emerged from exceedingly broad interpretations of the relevance standard. Although the Second Circuit has rejected FISC's interpretation of "relevant," *see* Am. Civil Liberties Union v. Clapper, 785 F.3d 787 (2d Cir. 2015), both FISC and the executive branch have made it clear that they prefer FISC's interpretation to the Second Circuit's, *see* Memorandum of Law of the United States, *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 15-75 (FISA Ct. June 2, 2015), http://www.fisc.uscourts.gov/sites/default/files/Misc%2015-01%20Memorandum%20of%20Law.pdf (arguing that the government should be able to continue collecting bulk data during the FREEDOM Act's transition period, despite the Second Circuit's decision in *ACLU v. Clapper*).

misuse of private information.[116] The definition of "specific selection term" is broad enough to include entire Internet Protocol (IP) addresses.[117] Thus, the government may acquire information that hundreds or thousands of non-foreign targets visited a given IP address. The Act also permits collections of information "two hops" away from an original target—what some refer to as "bulky" data—and creates a new phone metadata program that allows the NSA to continuously collect the phone records, not only of suspected terrorists, but of everyone with whom they are in contact.[118] In the FREEDOM Act, Congress addressed a symptom of post-9/11 changes to FISA, but did not address the underlying structural wrongs that permitted that symptom to come to fruition—Congress replaced one broad and ambiguous statutory directive with another.

B. BULK ADJUDICATION

An issue related to the bulk collection of information, which occurred in part because of broad and ambiguous statutory language, is the process by which that collection is approved.[119] The most troubling post-9/11 procedural change is the FAA's (potentially unintentional[120]) amendments to the warrant

116. *See generally* David Cole, *The New America: Little Privacy, Big Terror*, N.Y. REV. BOOKS, Aug. 13, 2015 (noting that the FREEDOM Act did not address myriad issues, including "the NSA's practices of collecting enormous amounts of personal data on and communications of foreigners overseas [(Section 702)], even when they are communicating with Americans").

117. In an earlier version of the FREEDOM Act proposed in the Senate, the "specific selection term" would have had to "narrowly limit the scope of tangible things sought to the greatest extent reasonably practicable." S. 2685, 113th Cong. § 107(k)(3) (2014). That language was not adopted by the House.

118. PCLOB REPORT, SECTION 215, *supra* note 113, at 29. Given that there is no known instance where the bulk collection "program made a concrete difference in the *outcome* of a counterterrorism investigation," we should be particularly suspect of any new program that strays beyond actual criminal or terrorist suspects. *Id.* at 11 (emphasis added). The PCLOB also found that there was only "one instance over the past seven years [when] the program arguably contributed to the identification of an unknown terrorism suspect," and the FBI would likely have identified that individual even without the use of bulk data collection. *Id.* The report's findings were based on access to "classified briefings and documentation." *Id.*

119. That is, assuming the executive branch invokes the FISA Court's jurisdiction and the FISA Court approves that bulk collection.

120. During congressional debates on the FAA, multiple members of Congress made statements suggesting that the FAA would still require individualized warrants for any surveillance that may implicate a United States citizen. *See, e.g.*, 154 CONG. REC. S6379 (daily ed. July 8, 2008) (statement of Sen. Cardin) ("FISA requires the Government to seek an order or warrant

application procedure. Prior to 2008, FISA required FISC to approve individualized warrant applications *before* a given search occurred, consistent with the recommendations of the Church Committee.[121] After 9/11, the executive branch argued that such an individualized requirement was no longer practicable given evolutions in technology and the nature of foreign enemies, and engaged in bulk collection of metadata without the knowledge or approval of FISC. Section 702 of the FAA attempted to appease those executive concerns and permitted the executive branch to collect "foreign intelligence" information, so long as FISC approved "targeting" and "minimization" procedures, intended to minimize the unlawful collection of information about United States citizens.[122] Those procedures are not applied on individual bases, but rather to "tens of thousands of cases involving [at least] hundreds of millions of communications" annually.[123]

Bulk adjudication of this sort is foreign to Article III courts. The FAA eliminated the role of the factual nuances and intricacies that are inherent in warrant proceedings. Under Section 702, the Attorney General and Director of National Intelligence certify that general categories of information collected serve to "acquire foreign intelligence information" without specifying who will be targeted.[124] Although the FISA Court does review, and has the power to amend, the government's

from the FISA Court before conducting electronic surveillance that *may involve* U.S. persons." (emphasis added)); 154 CONG. REC. H5763 (daily ed. June 20, 2008) (statement of Rep. Heather Wilson) (stating that the FAA would "protect the civil liberties of Americans and continue to require individualized warrants for anyone in the United States or American citizens anywhere in the world"); *see also* Donohue, *Section 702*, *supra* note 62, at 175 (collecting statements).

121. *See* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 324–26 (describing authorized investigative techniques); *see also supra* notes 12–13 and accompanying text (describing the importance of certain processes occurring before a search). The Church Committee explicitly stated that the executive branch lacks authority to "target[] . . . an American for electronic surveillance without a warrant." CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 325.

122. GOITEIN & PATEL, *supra* note 71, at 26.

123. *Id.* at 29. Similar bulk adjudications have been approved by the FISA Court under Section 215. *See, e.g.*, Internet Metadata Opinion and Order, No. PR-TT [REDACTED], slip op. at 69–71 (FISA Ct. 2006), http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf (describing the procedures the NSA must follow when engaging in bulk collection of Internet metadata).

124. PCLOB REPORT, SECTION 702, *supra* note 70, at 6.

targeting and minimization procedures,[125] the FISA Court cannot review the government's certification that a "targeting" procedure serves a "foreign intelligence" purpose.[126] This is particularly problematic because of the arguably tenuous relationship between "foreign intelligence" and the information collected. Collecting "foreign intelligence" does not even need to be the primary purpose of the search—it is sufficient if the information "relates to" national security.[127] Because of the deference the court must give the executive branch regarding the factual aspect of a "foreign intelligence purpose," the lack of a limiting judicial or statutory definition of that term is troubling.[128] As noted by the Church Committee, "foreign intelligence" is an exceedingly broad and malleable term,[129] and has been utilized by intelligence agencies to expand their power and authority beyond its intended scope.[130]

125. *See id.* "The minimization procedures cover the acquisition, retention, use, and dissemination of any non-publicly available U.S. person information acquired through the Section 702 program." *Id.* at 7.

126. GOITEIN & PATEL, *supra* note 71, at 41. Particularly troubling is that under current NSA targeting and minimization procedures, a United States citizen can be used as an identifier, so long as the search satisfies the other Section 702 prerequisites. *See* Memorandum Opinion, No. [REDACTED], slip op. at 22–23 (FISA Ct. Oct. 3, 2011), http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf; *see also* GOITEIN & PATEL, *supra* note 71, at 41.

127. *See* GOITEIN & PATEL, *supra* note 71, at 27.

128. FISA's definition of "foreign intelligence" is nearly limitless:

> "Foreign intelligence information" means—
>
> (1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; (B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or
>
> (2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—(A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e) (2012).

129. *See* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 302.

130. *See id.* at 4. Section 702's language also differs from the remainder of FISA, which requires searches to pertain to a "foreign power" or "agent of a foreign power"—language that had its genesis in the Supreme Court's *Keith* opinion. *See supra* notes 81–83 and accompanying text.

FISC's actions under Section 702 do not resemble the most fundamental roles of Article III courts—judges, adjudicating an individual case or controversy, which is capable of redressing a wrong or protecting a right. FISC is not even approving a specific search, as it at least arguably did (and under the FREEDOM Act is more likely to do) with regard to the approval of bulk data collection. Rather, Section 702 turns FISC into a meta-arbiter of mere search techniques, as opposed to the adjudicator of a specific search request.[131] And FISC lacks the authority to question the most fundamental finding in a 702 request—whether the procedures serve "foreign intelligence" interests. It is thus very questionable whether Section 702 comports with Article III of the Constitution.

These bulk adjudications are also the antithesis of the procedures envisioned by Congress and relied upon by the Justice Department in 1978 to justify FISA's constitutionality. Whether FISC comported with Article III was a subject of debate in 1978. The Act satisfied Article III on the margins because at least the court adjudicated an actual "case," similar to a neutral magistrate in warrant proceedings. After the FAA, however, the court no longer determines the President's "authority to conduct electronic surveillance of a particular target . . . [by] apply[ing] standards of law to the facts of a particular case."[132] Rather, the FISA Court applies general and ambiguous statutory language to (almost always) give judicial credence to intelligence agency procedures in the absence of specific information about the search targets. Notably, the FREEDOM Act did not amend the Section 702 program, except to the extent it limited bulk collection of Internet data to "specific selector terms."

Similar to the bulk collection discussed in Section A, the bulk adjudication represented a step back from the processes recommended by the Church Committee. The FAA placed more unchecked authority in the hands of intelligence agencies, and did so through ambiguous and broad directives. The structural changes that opened the door to bulk adjudication and bulk col-

131. As stated by Laura Donohue, "[FISC] in some ways thus appears to be acting in the capacity of an oversight body, generally ensuring that procedures are in place and asking the NSA to police itself." Donohue, *Section 702*, *supra* note 62, at 195.

132. *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legis. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 27–28 (1978) [hereinafter *Foreign Intelligence Electronic Surveillance Hearings*] (statement of John M. Harmon, Assistant Attorney Gen., Office of Legal Counsel).

lection paved the way for intelligence agencies to exceed their apparent authority. Similar to the pre-Church Committee era, "ambiguous laws and fuzzy instructions,"[133] minimal oversight, and changing technology opened the door to executive overreach.

C. A CULTURE OF IMPUNITY

Although we lack a comprehensive Senate report, there is evidence that the post-9/11 era greatly resembled executive actions in the pre-Church Committee era. Like practices uncovered by the Church Committee, after 9/11, executive agencies targeted individuals for their political opinions and blurred the line between foreign intelligence and national law enforcement. A similar culture of impunity seemingly flourished thanks to ambiguous statutory directives, minimal oversight, and pervasive secrecy.

President George W. Bush's "Terrorist Surveillance Program" exemplified the intelligence community's culture of impunity, operating at the highest levels of administration. Despite Congress's generous post-9/11 legislation, the Bush administration engaged in secret, warrantless electronic surveillance within the United States. The President's Terrorist Surveillance Program authorized the NSA to intercept communications of individuals "linked to" Al-Qaeda.[134] After the *New York Times* reported leaked information about the Terrorist Surveillance Program, the administration had to retroactively justify its actions. Attorney General Alberto Gonzales couched the program—and the administration's failure to seek FISC approval—in the need for "speed and agility" when responding to Al-Qaeda.[135] The Bush administration posited that the President possessed inherent constitutional authority "to order warrantless foreign intelligence surveillance within the United

133. SCHWARZ & HUQ, *supra* note 9, at 5; *see* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 169–72 (describing the effect inadequate statutory guides had on the overbreadth of intelligence gathering).

134. *See* Letter from William E. Moschella, Assistant Attorney Gen., U.S. Dep't of Justice, to Pat Roberts and John D. Rockefeller, IV, Senate Select Comm. on Intelligence, U.S. Senate, and Peter Hoekstra and Jane Harmon, Permanent Select Comm. on Intelligence, U.S. House of Representatives (Dec. 22, 2005) (describing "legal authority" supporting the NSA's collection activities).

135. Letter from Alberto R. Gonzales to Patrick Leahy and Arlen Specter, *supra* note 69, at 1; *see also* Letter from William E. Moschella to Pat Roberts et al., *supra* note 134, at 5 ("FISA could not have provided the speed and agility required for the early warning detection system.").

States," citing a classified FISC decision, the (ambiguous) *Keith* case, and Justice White's concurrence in *Katz*—shaky authority, to say the least, for such a sweeping constitutional interpretation.[136]

The President's reliance on "inherent authority" was at odds with FISA's text and legislative history. The Church Committee Domestic Task Force's first two formal recommendations stated: (1) "[t]here is no inherent constitutional authority for the President or any intelligence agency to violate the law," and (2) "[n]o executive directive or order may be issued which would conflict with [] statutes" implementing the Committee's recommendations with regard to "federal domestic security activities."[137] Codifying the Church Committee's recommendation, FISA specifies that it provides the "exclusive means" by which domestic electronic surveillance for national security purposes can be conducted.[138] A Senate Report stated that the "exclusive means" statement should "put[] to rest the notion that Congress recognizes an *inherent Presidential power* to conduct surveillance in the United States."[139] Eventually, parts of the Terrorist Surveillance Program evolved into Section 702, one of the broadest and most ambiguous grants of executive authority under FISA today.[140] The evolution from the Terrorist Surveillance Program to Section 702 is a paradigmatic example of executive overreach and secrecy breeding further overreach.

Overreach occurred within the confines of FISC's jurisdiction as well, often because the government interpreted FISC's orders in a way that "strain[ed] credulity."[141] Despite amend-

136. Letter from William E. Moschella to Pat Roberts et al., *supra* note 134, at 2.

137. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 293, 297.

138. 18 U.S.C. § 2511(2)(f) (2012). FISA built upon Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended at 42 U.S.C. § 3711 (1968)), which established rules for domestic government wiretaps, but did not explicitly govern wiretaps related to national security.

139. BIRCH BAYH, FOREIGN INTELLIGENCE SURVEILLANCE ACT, S. REP. NO. 95-701, at 71–72 (1978) (emphasis added).

140. *See* PCLOB REPORT, SECTION 702, *supra* note 70, at 5–6. The Foreign Intelligence Surveillance Court reinterpreted FISA and gave life to the program once again after President George W. Bush's attorney general refused to reauthorize the program "based on the president's bare say-so." Schlanger, *supra* note 5.

141. *See In re* Prod. of Tangible Things from [REDACTED], No. BR 08-13, slip op. at 5 (FISA Ct. Mar. 2, 2009).

ments to FISA that substantially broadened the NSA's ability to collect telephone and Internet communications,[142] the NSA repeatedly violated—and exceeded the scope of—FISC orders. In response to those violations, in 2009, FISC required the NSA to submit its queries of bulk metadata on a "case-by-case basis," even though the NSA itself had previously been determining whether it had "reasonable articulable suspicion" to search the database.[143] FISC enforced that case-by-case requirement because of "NSA non-compliance with the FISC's previous orders"—noncompliance that the Department of Justice, not the NSA, reported to FISC.[144] Even after the 2009 "sanction"[145] of actually submitting individualized search queries to FISC, the NSA once again arguably exceeded its court authorization. The NSA misrepresented to FISC the extent of its Internet communication collections, sparking one FISC judge to state that "[t]he Court is troubled that the government's revelations regarding NSA's acquisition of Internet transaction mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[146]

On Christmas Eve of 2014, in response to a Freedom of Information Act lawsuit, the NSA released a "heavily-redacted" report, which summarized the misuse of information and search technology from 2001 to 2013.[147] The agency stated that

142. Even FISC's interpretations "push statutory language to its limit." *See* Donohue, *Section 702*, *supra* note 62, at 122.

143. LIU ET AL., *supra* note 54, at 4–5.

144. *Id.* at 5; *see also In re Prod. of Tangible Things*, No. BR 08-13, at 18–20.

145. It is interesting that limiting FISC to its original role in national security-related search proceedings was considered a "sanction."

146. Memorandum Opinion, No. [REDACTED], slip. op. at 16 n.14 (FISA Ct. Oct. 3, 2011), http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf.

147. David Lerman, *U.S. Spy Agency Reports Improper Surveillance of Americans*, BLOOMBERG (Dec. 24, 2014, 11:45 AM), http://www.bloomberg.com/news/articles/2014-12-24/spy-agency-to-release-reports-documenting-surveillance-errors. It is hard to believe that releasing the documents on Christmas Eve was unintentional. Perhaps the NSA hoped that individuals would be on holidays, paying less attention to the news cycle. This possibility was noted by more than one news agency, one of which stated that the NSA released the report "[w]ith little fanfare," "quietly publish[ing] a trove of declassified data." Javier E. David, *NSA Declassified Reports Showing US Privacy Breaches*, CNBC (Dec. 27, 2014, 4:46 PM), http://www.cnbc.com/2014/12/27/nsa-declassified-reports-showing-inadvertent-us-surveillance.html; *see also* Nicky Woolf, *ACLU Accuses NSA of Using Holiday Lull To "Minimise Impact"*

the "vast majority of compliance incidents involve unintentional technical or human error."[148] Unsurprisingly—given FISC's role as approver of general retention techniques but not individualized searches—some acquisition of information about United States persons occurred because of "overly broad or poorly constructed database queries."[149] There were also instances, however, of "intentional misuse" of the bulk collection systems.[150] These examples of "intentional misuse" of information are similar to those uncovered by the Church Committee.[151]

Although there is evidence of abusive use of surveillance, that evidence is arguably not as extreme as that uncovered by the Church Committee—there is not *as much* evidence of the extreme practices of using surveillance to disrupt social justice

of Documents, GUARDIAN (Dec. 26, 2014, 3:25 PM), http://www.theguardian.com/us-news/2014/dec/26/aclu-nsa-documents-christmas-eve-lessens-impact.

148. *NSA Reports to the President's Intelligence Oversight Board (IOB)*, NAT'L SECURITY AGENCY, http://www.nsa.gov/public_info/declass/IntelligenceOversightBoard.shtml (last visited Apr. 11, 2016).

149. NAT'L SEC. AGENCY, REPORT TO THE INTELLIGENCE OVERSIGHT BOARD ON NSA ACTIVITIES—INFORMATION MEMORANDUM 2 (Mar. 4, 2013). The number of searches that were "overly broad" is redacted from the report, making it difficult to assess the average accuracy of NSA searches. *See id.*

150. *NSA Reports to the President's Intelligence Oversight Board (IOB)*, *supra* note 148.

151. *See generally supra* notes 32–42 and accompanying text. The Church Committee found that "intelligence agencies [] frequently wiretapped and bugged American citizens without the benefit of judicial warrant," CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 12, permitting "the Government to generate vast amounts of information—unrelated to any legitimate government interest—about the personal and political lives of American citizens," SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, U.S. SENATE, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, SEN. REP. NO. 94-755, BOOK III, at 332 (1976). Since 9/11, the NSA has likewise retained wholly domestic e-mails obtained incidentally, including e-mails that contain information about U.S. persons, and retained that information just "because the information may prove relevant in the future." GOITEIN & PATEL, *supra* note 71, at 38. This broad array of information has allegedly been used in ways that infringe on the protected First and Fourth Amendment rights of individuals and organizations. The Church Committee also found that intelligence agencies targeted domestic groups and individuals, including civil rights organizations and Martin Luther King, Jr. *See, e.g.*, CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 51–53. Civil rights organizations today are likewise concerned with unauthorized searches of their private information, resulting in a chilling of their First Amendment rights. *See generally* Brief for Nat'l Assoc. for the Advancement of Colored People et al. as Amici Curiae Supporting Plaintiffs, Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644 (6th Cir. 2006) (Nos. 06-2095, 06-2140).

movements and harass political outsiders.[152] But that does not mean the abuse is not occurring and that the potential for misuse of information is not chilling First Amendment-protected expression.[153] Snowden's disclosures revealed that, post 9/11, the NSA and FBI covertly monitored e-mails of prominent Muslim-Americans ranging from politicians to civil rights activists.[154] Snowden disclosed that the administration deliberately masked evidentiary trails to hide any evidence that originated from a FISA warrant from criminal defendants (parallel construction), so that the FISA searches could not be challenged in criminal proceedings.[155] To assume more unconstitutional surveillance is not occurring is to ignore the lessons learned after the Cold War—"[i]n time of crisis, the Government will exercise its power to conduct domestic activities to the fullest extent. The distinction between legal dissent and criminal conduct is easily forgotten."[156]

The potential for the misuse of intelligence information is particularly troubling because of the inextricable relationship between intelligence and law enforcement. The PATRIOT Act amended FISA to permit greater coordination between intelligence and law enforcement agencies while simultaneously expanding the scope of information subject to FISC-approved searches.[157] Under new standards, the NSA could conduct surveillance so long as it was a "significant"—as opposed to the

152. *See, e.g.*, CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 10–13 (summarizing the Domestic Task Force's findings on the use of illegal or improper means of covert action).

153. For a discussion of the ways in which United States persons have already changed their behavior to avoid federal surveillance of First Amendment protected expression, see Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RES. CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden.

154. *See* Glenn Greenwald & Murtaza Hussain, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On*, INTERCEPT (July 8, 2014, 11:01 PM), http://theintercept.com/2014/07/09/under-surveillance. Also, as discussed further below, there is the potential for misuse of NSA-acquired information by the FBI when conducting purely domestic law enforcement activities. *See infra* notes 157–61 and accompanying text.

155. *See, e.g.*, John Shiffman & Kristina Cooke, *U.S. Direct Agents To Cover Up Program Used To Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805 (discussing governmental surveillance of domestic drug offenders).

156. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 289; *see also id.* at 291 ("The natural tendency of Government is toward abuse of power.").

157. USA PATRIOT Act, Pub. L. No. 107-56, § 218, 115 Stat. 272, 291 (codified as amended at 50 U.S.C. §§ 1804(a)(7)(B), 1832(a)(7)(B) (2001)).

primary—purpose of the search.[158] This change in language led some analysts to conclude that law enforcement may be the primary purpose for a search.[159] Further, the FBI can search the bulk databases collected through FISC order.[160] Because of the NSA's history of non-compliance with court minimization procedures and broad, poorly worded queries, the FBI may then access databases with information about United States citizens. The FBI thus is able to end run the requirements of the Fourth Amendment—the Supreme Court has made it clear that a warrant *is* required to conduct surveillance of Americans' communications in cases that are not foreign intelligence investigations.[161]

Thus, even if we assume every individual searching an NSA database is searching for information to further "foreign intelligence"—a dubious assumption given historical practices by the intelligence community—information about United States persons is vulnerable to collection and analysis in contravention of the Constitution. For persons who may have their civil liberties violated due to an accidental broad query or an intentional misuse of law enforcement power, there are few ways to learn of those abuses and even fewer ways to challenge them in a court.

D. BARRIERS TO COLLATERAL REVIEW

Despite the aforementioned issues currently plaguing *ex ante* FISC authorization of intelligence gathering, it is incredibly difficult for the public to learn of intelligence gathering practices and challenge them *ex post*. As a former FISC judge publicly stated, unlike the subjects of traditional warrants, subjects of FISC searches are unlikely to learn of, let alone be able to challenge, the information acquired by a FISC-approved search.[162] The government is supposed to notify criminal defendants if FISC-acquired evidence is used to build the gov-

158. *Id.*

159. For example, one reported breach occurred when an individual used the signals intelligence system to locate someone believed to be kidnapped. Woolf, *supra* note 147.

160. GOITEIN & PATEL, *supra* note 71, at 39.

161. *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 316–18 (1972) (holding that, in general, the government must secure a warrant before engaging in domestic electronic surveillance).

162. James G. Carr, *A Better Secret Court*, N.Y. TIMES (July 23, 2013), http://www.nytimes.com/2013/07/23/opinon/a-better-secret-court.html.

ernment's criminal case,[163] but Snowden disclosed a policy of attempting to hide the trail of evidence that originated from a FISC order.[164] Furthermore, because the majority of foreign intelligence investigations never result in a criminal prosecution, most targets are never notified that surveillance occurred.[165] Specific challenges to searches are difficult to mount, so it is paramount that there is transparency in FISC proceedings so that those most likely to be targeted may be able to satisfy Article III's standing requirements. The Church Committee recognized that a culture of secrecy limited testing of intelligence practices by Congress and the public, and contributed to executive overreach. Unnecessary secrecy, however, remains a key component of post-9/11 intelligence practices. There are two particular broad policies that currently limit more general challenges to surveillance—the expansion of the state secrets doctrine and FISC's confidential constitutional and statutory interpretations.

1. The State Secrets Doctrine

One way in which the government has attempted to limit challenges to programmatic surveillance and the collection of citizens' private information is through the invocation of the "state secrets" doctrine,[166] created in its modern form by the Supreme Court in *United States v. Reynolds*.[167] In *Reynolds*, the

163. *See* 50 U.S.C. §§ 1806(c), 1825(d) (2012).

164. *See supra* note 155 and accompanying text.

165. Although beyond the scope of this Article, it is worth noting that even when a criminal prosecution is brought as a result of FISC-acquired evidence, it remains difficult for the defendant to challenge that evidence. The government notice of FISC-collected evidence often does not include the basis of collection (who was the "foreign agent," what statutory provision the search was authorized under, etc.), leaving defense counsel unable to effectively bring a motion to suppress the evidence. *See* Faiza Patel, *How a Case of Stolen Corn Seeds Shows the Problem with the FISA Court*, JUST SECURITY (Apr. 1, 2015, 8:59 AM), http://www.justsecurity.org/21709/stolen-corn-seeds-problem-fisa-court.

166. Very little is known "about how the executive branch actually uses the privilege—who invokes it, under what circumstances it is invoked, how frequently it has been threatened, and to what end." Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77, 79 (2010) [hereinafter Donohue, *State Secrets*]. National security scholar Laura Donohue has, however, written a comprehensive and thoughtful article on the issue. *Id.* In that article, she notes that the state secrets privilege has "played a significant role in the executive branch's national security litigation strategy." *Id.* at 87.

167. 345 U.S. 1 (1953). For an overview of the *Reynolds* opinion, see FREDERICK A.O. SCHWARZ, JR., DEMOCRACY IN THE DARK: THE SEDUCTION OF GOVERNMENT SECRECY 208–09 (2015).

Court discussed a common-law privilege against revealing military or state secrets and held that courts should treat a document as privileged if an executive official certified that the document contained sensitive information.[168] Furthermore, the court should do so without reviewing the document to ensure executive honesty when invoking that privilege.[169] The three *Reynolds* dissenters stated their support of the Third Circuit's opinion, which recognized the importance of courts as a check on the constitutionality of executive and legislative action.[170] And those dissenters were correct to worry, since subsequent courts "have viewed assertions of the privilege as a virtual 'automatic win' for the Government."[171] Despite the fact that *Reynolds* limited its remedy to treating a certain document as privileged, recent administrations have more expansively invoked that privilege in litigation related to national security.[172]

The state secrets doctrine has significantly expanded since FISA's enactment. As originally described in *Reynolds*, the state secrets doctrine was a "privilege" used to shield internal government documents that could expose "military matters" that affect "national security" from public disclosure.[173] However, recent administrations have invoked the doctrine as grounds for dismissing entire lawsuits.[174] In response, some courts completely dismiss suits without adequate or logical explanation, often incorrectly invoking the *Totten*[175] doctrine—a doctrine that precludes suits to enforce covert espionage

168. *Reynolds*, 345 U.S. at 10.

169. *Id.* at 7–8 ("The court itself must determine whether the circumstances are appropriate for the claim of privilege, and yet do so without forcing a disclosure of the very thing the privilege is designed to protect.").

170. *See id.* at 12; *see also* Reynolds v. United States, 192 F.2d 987 (3d Cir. 1951).

171. *See* S. REP. NO. 110-442, at 5 (2008).

172. *See id.* at 3 (noting that "a strong public perception has emerged that sees the privilege as a tool for Executive abuse").

173. *Reynolds*, 345 U.S. at 9–10; *see, e.g.*, Pan Am. World Airways, Inc. v. Aetna Cas. & Sur. Co., 368 F. Supp. 1098, 1139–41 (S.D.N.Y. 1973) (applying state secrets doctrine to shield CIA documents listing sources of intelligence information from disclosure), *aff'd*, 505 F.2d 989 (2d Cir. 1974).

174. *See, e.g.*, El-Masri v. Tenet, 437 F. Supp. 2d 530 (E.D. Va. 2006) (dismissing suit when plaintiff's claims could not be litigated without disclosure of secrets protected by the state secrets privilege); *see also* SCHWARZ, *supra* note 167, at 41. The state secrets doctrine has been invoked in four dozen cases that stem from the Terrorist Surveillance Program. Donohue, *State Secrets*, *supra* note 166, at 139–40.

175. Totten v. United States, 92 U.S. 105 (1875).

agreements with the government.[176] Whereas *Totten* does suggest a narrow ground of state secrets that may justify complete dismissal of a suit, that narrow ground was not at issue in *Reynolds*—a case that only discussed a privilege, not jurisdiction—and it is not apposite in most cases challenging FISC orders.[177]

Challenges remain even in those cases where courts properly apply *Reynolds*. Even if courts do not dismiss the suit solely based on "state secrets," many suits are dismissed nonetheless on procedural and constitutional grounds. For example, by precluding access to information collected under Section 702 and Section 215, the government is able to prevent plaintiffs from obtaining the requisite documents to establish standing.[178]

The state secrets doctrine is particularly problematic because there is a tendency for executive officials to invoke it not to further national security, but instead to bury some embarrassing executive action. The *Reynolds* opinion itself—along with subsequent cases such as *Korematsu v. United States*[179]—highlights the risk of inappropriate invocation of the state secrets doctrine. In *Reynolds* and *Korematsu*, respectively, there is evidence that the executive branch misstated evidence to hide its own negligence and misstated the extent of "secret" information to further an executive policy.[180] More recently, the state secrets doctrine has been invoked to preclude relief to in-

176. *See* Tenet v. Doe, 544 U.S. 1, 2, 8–11 (2005) (describing *Totten* as precluding any suit "where success depends upon the existence of [a] secret espionage relationship with the Government").

177. *See, e.g.*, Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1077 (9th Cir. 2010) (en banc). In *Jeppesen*, Judge Hawkins persuasively criticized the majority's description of the *Totten* doctrine, arguing that the doctrine was wholly inapplicable where a claim was brought by third-party plaintiffs (not government agents) against non-governmental defendants for tortious (not espionage-related) activities. *Id.* at 1096–97 (Hawkins, J., dissenting).

178. *See, e.g.*, Am. Civil Liberties Union v. Nat'l Sec. Agency, 493 F.3d 644, 653–57, 687–88 (6th Cir. 2007) ("But the plaintiffs do not—and because of the State Secrets Doctrine cannot—produce any evidence that any of their own communications have ever been intercepted by the NSA, under the [terrorist surveillance program], or without warrants."); Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 919–20 (N.D. Ill. 2006) ("By successfully invoking the state secrets privilege, the government has foreclosed discovery that would allow the plaintiffs to attempt to establish that they are suffering ongoing harm or will suffer harm in the future.").

179. 323 U.S. 214 (1944).

180. *See* S. REP. NO. 110-442, at 5 (2008); Frederick A.O. Schwarz, Jr., *Access to Government Information Is a Foundation of American Democracy—But the Courts Don't Get It*, 65 OKLA. L. REV. 645, 659–62 (2013).

dividuals tortured by the Bush administration, even when the arguably "confidential" information was already publicly disclosed.[181] "The privilege has . . . become part of a broader framework through which the government tries to limit its vulnerability."[182] Without adequate "checks" by courts, there is a significant risk that executive officials will continue "invoking [state secrets] as a shield against embarrassing disclosures,"[183] thus "depriv[ing] the American people of their ability to judge the effectiveness of their Government on national security matters."[184]

The executive branch's invocation of the state secrets doctrine to preclude litigation exacerbates current issues plaguing FISC. It provides a further means of insulation from review by an Article III court other than the FISA Court. Non-FISA proceedings are an especially important means of challenging NSA collection activities because of the actual adversity between two parties, which is almost always lacking in the ex parte proceedings before FISC. Moreover, the drafters of FISA explicitly considered and drafted a provision addressing the relationship between information obtained via FISC-approved searches and admissible evidence in non-FISC proceedings, leading one judge to hold that FISA preempts the state secrets doctrine.[185] Under FISA, the district court may consider certain FISA-acquired evidence "*in camera and ex parte*" if the Attorney General files an affidavit "that disclosure or an adversary hearing would harm the national security of the United States."[186]

181. *See* SCHWARZ, *supra* note 167, at 214–17.

182. Donohue, *State Secrets*, *supra* note 166, at 95. The state secrets doctrine has been invoked not only to limit the government's vulnerability but also to protect—by extension and without any precedential support from *Reynolds*—private government contractors. *Id.* at 95–98.

183. *Background on the State Secrets Privilege*, ACLU, http://www.aclu.org/background-state-secrets-privilege (last visited Apr. 11, 2016).

184. S. REP. NO. 110-442, at 10 (2008) (citing Press Release, Patrick Leahy, U.S. Senate, Examining the State Secrets Privilege: Protecting National Security While Preserving Accountability (Feb. 13, 2008), http://www.leahy.senate.gov/press/examining-the-state-secrets-privilege-protecting-national-security-while-preserving-accountability).

185. *See In re* Nat'l Sec. Agency Telecomm. Records Litig., 564 F. Supp. 2d 1109, 1117–25 (N.D. Cal. 2008).

186. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 106(f), 92 Stat. 1783, 1794 (codified at 50 U.S.C. § 1806(f) (1978)) (emphasis added). "In practice, the government always files such an affidavit, and it appears that no defendant has ever obtained a copy of the government's statement of probable cause or other documents that served as the basis for FISA surveillance." PCLOB REPORT, SECTION 215, *supra* note 113, at 176.

Congress thought that a statutory procedure would better balance security and liberty interests than a common law rule developed by the courts.[187] Notably, unlike *Reynolds*, FISA still permits judges to review the allegedly sensitive evidence, and it certainly does not suggest that the security-related evidence can serve as the basis for complete dismissal of a lawsuit.

The state secrets doctrine has been expanding since FISA. If anything, however, that doctrine should be contracting in the post-FISA regime. FISC provides a confidential forum for adjudication, and FISA provides for in camera review of information if the Attorney General so requests. At the very least, the state secrets doctrine should not completely preclude litigants from bringing suits challenging the government's acquisition of information through FISC-approved searches. In 1978, Congress attempted to establish a regime that would return separation of powers principles to the collection of intelligence. Reviewing certain information in camera still preserves separation of powers principles because a court is actually reviewing the information, verifying the Attorney General's invocation of protecting foreign intelligence information. However, if courts permit the state secrets doctrine to completely prohibit lawsuits, there is no adequate check by the judiciary on the intelligence community. This contravenes the lessons learned by the Church Committee and the delicate regime established by FISA.

2. Confidential Constitutional and Statutory Interpretations

As the state secrets doctrine has expanded, simultaneously has the scope of the orders issued by FISC. When originally enacted, FISC was supposed to be a court of limited jurisdiction, solely possessing the authority to issue investigative subpoenas *before* the government targeted an individual. Today, the FISA Court routinely engages in confidential constitutional and stat-

187. The House report stated that FISA was intended to displace "uneven and inconclusive" case law developed by courts regarding electronic surveillance and national security. H.R. REP. NO. 95-1283, pt. 1, at 21 (1978). The report continued:

> Moreover, the development of standards and restrictions by the judiciary with respect to electronic surveillance for foreign intelligence purposes accomplished through case law threatens both civil liberties and the national security because that development occurs generally in ignorance of the facts, circumstances, and techniques of foreign intelligence electronic surveillance not present in the particular case before the court.

Id.

utory interpretation. This shift not only departs from Congress's original intent in 1978 but also prevents parties from testing the government's—and FISA Court's—statutory and constitutional interpretation in a well-briefed, reasoned, and adversarial setting. Such adversarial challenges outside of FISC proceedings are particularly unlikely because parties often lack notice of surveillance (and therefore the ability to bring an as-applied challenge). More importantly, however, the vast majority of surveillance conducted under Sections 215 and 702 will never find its way into any legal proceeding, criminal or civil, where the statutory or constitutional interpretation could potentially be uncovered and vetted.[188]

Before the Snowden disclosures, the majority of FISC opinions interpreting FISA and its relationship to the First and Fourth Amendments remained sealed, precluding individuals from learning about potential "injuries" to their civil liberties and bringing lawsuits in Article III courts that challenged the NSA or FBI's investigation activities. As of 2007, FISC had only published one opinion since the court's inception in 1978, prompting legislative attorneys to describe the publication procedure as "extremely rare."[189] Although publication of FISC opinions has been somewhat more common in the wake of the Snowden disclosures, there is still no way for the public to know if FISC is engaging in novel statutory or constitutional analysis.

The FREEDOM Act tackled this impediment to effective review of the FISA Court and intelligence community. FISC opinions that "include[] a significant construction or interpretation of any provision of law," including the term "specific selection term," should be declassified "to the greatest extent practicable."[190] Additionally, if a provision is exempted from declassification due to a "national security waiver," the Attor-

188. GOITEIN & PATEL, *supra* note 71, at 33–34.

189. BAZAN ET AL., *supra* note 53, at 5.

190. FREEDOM Act, Pub. L. No. 114-23, § 602(a), 129 Stat. 268, 281 (codified at 50 U.S.C. § 1872(a) (2012)). We note that the term "significant" may be ambiguous enough to open the door to unnecessary (and harmful) secrecy. Why not require FISC to publish each opinion that includes a novel application of a statute? What is insignificant in the eyes of the Attorney General may be significant to the American citizen whose information may be impermissibly obtained under that interpretation. We hope the executive branch does not abuse this term, but notes its ambiguity, especially given the intelligence community's improper use of ambiguous terms in the past.

ney General must still provide the public with a summary of the legal interpretation.[191]

Like other FISA reforms made by the FREEDOM Act, the declassification of opinions with "significant" constructions and interpretations of laws is an improvement. But, like other reforms, the declassification option seems like putting a Band-Aid on a bullet hole. The issue was not just that FISC engaged in substantial statutory and constitutional interpretation without disclosing its opinions to the public. Rather, the issue was the role FISC played in interpreting statutes and the Constitution. Under the original regime, FISC interpreted a narrow, unambiguous statute, and applied that language to specific facts provided by the government before authorizing a search. Now, FISC interprets broad and ambiguous language, applying that language to procedures employed *after* a search, and cannot question the factual base provided by the government. The post-9/11 court is engaged in more of a legal and less of a factual inquiry. It is therefore less likely that the FISC of 1978 would have needed to engage in the types of statutory and constitutional interpretation that is commonplace after the PATRIOT Act and FAA. Like bulk adjudication and collection, and executive impunity, excessive secrecy is a result of post-9/11 changes made to FISA.

We now turn to those broader, structural issues currently affecting FISC—issues that cannot be resolved with piecemeal legislation, but instead require reconceptualizing the role of the court and its relationship to the coordinate branches of government.

III. PROTECTING LIBERTIES BY ENSURING FISC ACTS LIKE A COURT—NOT AN EXECUTIVE ADJUNCT

The FISA Court currently operates more closely to an executive adjunct than an Article III court. Rather than adjudicating individual cases or controversies, the court approves systems and procedures developed by the executive branch. Rather than determining whether there is probable cause for a given search, the court approves programmatic surveillance based on a factual certification by the government. Even in regular Article III proceedings that are subject to public scrutiny, courts are hesitant to question the executive branch's assessment of

191. *Id.* § 602(c).

national security threats.[192] But the FISA Court is even more likely to defer when it is engaging in bulk adjudication in a non-adversarial setting.[193] The court is too many steps removed from the specific searches it approves on a macro scale and, therefore, less able to question the national security interests invoked by the executive branch.

In this Part we lay out specific recommendations for reform. All recommendations are tied together by the need for ensuring civil liberties are protected and vetted through traditional Article III adjudication. If the executive branch chooses to utilize a confidential court, it must recognize that that court is still bound by the requirements of Article III of the Constitution. Section A begins by discussing the need for an "adversary" to the government in FISA Court proceedings. This is particularly important in the post-9/11 adjudications that no longer resemble the ex parte "warrant" proceedings analogized to FISC adjudications in 1978. Next, Section B recommends that the FISA Court no longer approve targeting and minimization procedures under Section 702. In those proceedings, the court is approving procedures before they arguably give rise to a cognizable injury, in effect issuing an advisory opinion prohibited by Article III of the Constitution. Finally, Section C discusses the need for greater transparency and opportunities for collateral review. Although transparency must be balanced against the realistic need for protecting intelligence information, enshrouding foreign-intelligence related proceedings in secrecy undermines public trust in the institution and our government.

A. RETURNING TO QUASI-ADVERSARIAL WARRANT PROCEEDINGS

Courts serve a limited function within our government—they must resolve cases and controversies involving real disputes between parties of genuine interest. This requirement serves to ensure that parties to a proceeding both raise and vigorously examine all aspects of a given issue, which in turn improves judicial decision-making.[194] The FISA Court's current

192. *See, e.g.*, Cent. Intelligence Agency v. Sims, 471 U.S. 159, 178–79 (1985).

193. *See, e.g.*, Internet Metadata Opinion and Order, No. PR-TT [REDACTED], slip. op. at 30–31 (FISA Ct. 2006), http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf ("Such deference [to the executive branch] is particularly appropriate in this context, where the Court is not charged with making independent probable cause findings.").

194. *See* PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., WORKSHOP REGARDING SURVEILLANCE PROGRAMS OPERATED PURSUANT TO SECTION 215 OF THE

practice of engaging in broad statutory and constitutional interpretation without the benefit of an adversary to the government does not satisfy the adversity requirement memorialized in the Constitution and Supreme Court jurisprudence.[195]

During FISA's enactment, a core concern was whether the FISA Court comported with Article III's "case or controversy" requirement.[196] Could the ex parte and in camera proceedings of the court satisfy the constitutional requirement of adversarial adjudication? The Department of Justice itself conceded in 1978 that lack of adversity before the FISA Court presented a "difficult question."[197] The Justice Department justified FISA's procedures by analogizing them to warrant proceedings, which are likewise conducted ex parte, involve a particular target, and require judicial approval *prior* to the search.[198] Similar to warrant proceedings, the FISA Court would make individualized assessments based on a variant of probable cause, and apply that standard to a specific warrant relating to a specific search (whether person or place) before the search occurred.

Although FISC still engages in traditional warrant-like proceedings, many searches are approved via bulk adjudication. Whereas from 1978 to 2001, the FISA Court engaged *exclusively* in a quasi-adversarial warrant procedure, today the court is often even further removed from the discrete facts and arguments that may justify ruling against the government.[199] The court is less involved in the pre-search inquiry—it must accept the government's certification of "relevance" to a "foreign intel-

USA PATRIOT ACT AND SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 34 (July 9, 2013) [hereinafter TRANSCRIPT, PCLOB WORKSHOP] (statement of Honorable James Robertson, Retired, Dist. Court, Foreign Intelligence Surveillance Court) ("[A]nybody who has been a judge will tell you that a judge needs to hear both sides of a case before deciding. It's quite common, in fact it's the norm to read one side's brief or hear one side's argument and think, hmm, that sounds right, until we read the other side.").

195. *See* U.S. CONST. art. III, § 2 (articling the case or controversy provision); Muskrat v. United States, 219 U.S. 346 (1911) (describing the adversity requirement and dismissing a suit in which the government effectively was both the plaintiff and defendant).

196. U.S. CONST. art. III, § 2.

197. *Foreign Intelligence Electronic Surveillance Hearings*, *supra* note 132, at 26 (statement of John M. Harmon, Assistant Attorney Gen., Office of Legal Counsel).

198. *Id.* at 29.

199. Until 2004, the FISA Court considered "government applications relating to a *specific person, a specific place, or a specific communication account or device*." PCLOB REPORT, SECTION 215, *supra* note 113, at 175 (emphasis added).

ligence" purpose, and must do so without the government providing specific and articulable facts to support its certification. The court plays a more expansive role in post-search procedure, by assessing targeting and minimization criteria. FISC thus is acting less like a neutral magistrate approving an individualized warrant.

These changes place judges in an uncomfortable position. FISC judges have less ability to rule against the government for factual reasons and are left to consider abstract collection and minimization procedures. Furthermore, judges are more likely to rule in favor of the government when national security is involved, leading the FISA Court to become more of a rubber stamp on behalf of government programs than a neutral check against executive overreach. This deference is memorialized in FISC opinions, one of which states, "[T]his Court has often recognized the expertise of the government in foreign intelligence collection and counterintelligence investigations of espionage and international terrorism, and *accorded great weight* to the government's interpretation of FISA's standards."[200] The lack of adversity leads to less developed arguments being provided to the FISA Court, and therefore the possibility of less well-reasoned opinions, as borne out by the Second Circuit's decision in *ACLU v. Clapper*. The risk of missing counterarguments to the government's position—or failing to understand the depths of those counterarguments—is all the more pressing now that the FISA Court regularly engages in broad constitutional and statutory interpretation. Such risk undermines the integrity and impartiality of the court.

One potential solution to this problem is to appoint an ombudsman, or "Special Advocate," to represent the public interest before the FISA Court.[201] This solution was recommended by the Privacy and Civil Liberties Oversight Board (PCLOB), raised in Congress multiple times, and recently codified (to a limited extent) in the FREEDOM Act. FISA previously provided a mechanism for FISC judges to invite amici, or friends of the court, to comment on a case. However, the amici provision was rarely invoked, and never to provide an "assessment of the

200. *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, Nos. Multiple (FISA Ct. May 17, 2002) (emphasis added), http://fas.org/irp/agency/doj/fisa/fisc051702.html.

201. Before the FREEDOM Act, FISA did "not provide a mechanism for the FISC to invite non-governmental parties to provide views on pending government applications." PCLOB REPORT, SECTION 215, *supra* note 113, at 180.

government's legal authorization to conduct surveillance."[202] The PCLOB recommended creating a "pool of 'Special Advocates' who would be called upon to present independent views to the court in important cases."[203] The FREEDOM Act adopted a variation of the PCLOB's recommendation.[204] Now, FISC judges may appoint pre-approved "amici" to present arguments on a FISA application that, "in the opinion of the court, presents a novel or significant interpretation of the law, unless the court issues a finding that such appointment is not appropriate."[205] Like other aspects of the FREEDOM Act, this amici provision is a step in the right direction but does not remedy all of FISA's post-9/11 underlying structural wrongs.

There are a few issues with the FREEDOM Act's amici provision. First, an amicus does not need to present a view that is "adversarial" to the government. Rather, the amicus provides "(A) legal arguments that advance the protection of individual privacy and civil liberties; (B) information related to intelligence collection or communications technology; or (C) legal arguments or information regarding any other area relevant to the issue presented to the court."[206] These interests may well be quasi-adversarial to the government, but there may also be sit-

202. *Id.* at 181; *see also id.* (describing the amicus procedure before the FISA Court of Review).

203. *Id.* at 184. Important cases are those involving programmatic surveillance and bulk collection of data, as distinguished from the more individualized proceedings that resemble traditional warrant proceedings. *Id.* at 183–84. The PCLOB recommended that the "Special Advocate" only present arguments when invited and that the advocate need not always serve as an "adversary" to the government. Rather, the advocate would read the government's position and could agree with it. We think this distinction is not only risky, but it also misses the mark. As noted by Judge Robertson, the judicial decision-making process is improved when *adversarial* positions are presented. *See* TRANSCRIPT, PCLOB WORKSHOP, *supra* note 194. The requirement of adversity is enforced in other Article III courts. For example, when the Obama administration declined to argue on behalf of the Defense of Marriage Act, the Supreme Court and Solicitor General recognized that Congress needed its own representation. *See* Editorial, *Defense of Marriage Act: Attack the Law, Not the Lawyer*, L.A. TIMES (Apr. 21, 2011), http://articles.latimes.com/2011/apr/21/opinion/la-ed-doma-20110421. One side, even the somewhat neutral position of the "government," would not suffice. *Id*. ("[W]ith sharp-witted counsel on both sides making the strongest possible arguments, it is more likely that justice will be done. For another, a lawyer who defends an individual or a law, no matter how unpopular or distasteful, helps ensure that the outcome is viewed as fair.").

204. *See* FREEDOM Act, Pub. L. No. 114-23, § 401, 129 Stat. 268, 279 (codified as amended at 50 U.S.C. § 1803(g) (2012)).

205. *Id.*

206. *Id.*

uations where they are not. Second, an the amicus lacks the usual authority and rights of an adverse party. The amicus, as a mere "friend" of the court as opposed to a party to the action, cannot appeal any "losing" decisions to the FISA Court of Review and Supreme Court, like an adverse party could in any other individual lawsuit. The amici provision thus provides only a surface level adversity to FISC proceedings, but does not change the underlying structural issues that limit FISC's ability to provide meaningful oversight.[207]

Finally, the amici provision contains hallmark ambiguous language, which the government and judges may invoke to avoid appointing an amicus in a given case. What constitutes a "significant" interpretation of law? If significance is measured by the potential number of United States persons impacted by a practice, then an amicus should be appointed in every case regarding programmatic surveillance. Also, does "novel" mean from the time of the FREEDOM Act onward, when the FISA Court could theoretically invoke and benefit from a quasi-adversarial amicus? Or, because opinions issued before the enactment of the FREEDOM Act are binding precedent, are those issues settled (even though they were decided without the benefit of quasi-adversarial briefing)? Moreover, the FREEDOM Act contains an escape clause for the court—FISC does not need to appoint an amicus, even if the case involves novel or significant issues, if "such appointment is not appropriate."[208] What would render such appointment inappropriate? Congress provided absolutely no guidance, and this is exactly the kind of ambiguous language that can be used to further the intelligence community's preference for operating in a cloak of secrecy at the expense of personal liberties. Indeed, there is already evidence that members of the FISA Court who are hostile to the FREEDOM

207. *See* TRANSCRIPT, PCLOB WORKSHOP, *supra* note 194 (statement of Honorable James Robertson, Retired, Dist. Court, Foreign Intelligence Surveillance Court ("[T]his process needs an adversary[,] . . . an institutional adversary to challenge and take the other side of anything that is presented to the FISA Court.")); *cf.* GOITEIN & PATEL, *supra* note 71, at 46 (arguing that prior proposals of public ombudsmen provided adversity in name only but would not change the substance of FISC proceedings).

208. FREEDOM Act § 401. The public advocate proposal has received a lot of attention. But not all proposals are equal. To be effective, there must be "a more empowered public advocate—one who is authorized to appear even without invitation from the government or the court, and, still more importantly, who is entitled to full access of information relevant to her duties." Schlanger, *supra* note 5.

Act's amici provision will use the Act's ambiguity to preclude the appointment of an amicus.[209]

Given the weaknesses remaining after the FREEDOM Act, we would propose that Congress go further. So long as FISC proceedings no longer resemble traditional warrant proceedings in which the court is approving a search of a particular person, place, or thing, there must be truly adverse positions presented to the court. As mentioned before, the current proceedings likely do not satisfy Article III of the Constitution. In 1978, a significant reason Congress moved forward with FISA—despite concerns regarding compliance with Article III—was that the FISA proceedings were limited in nature and greatly resembled traditional warrant proceedings.[210] It was that similarity to warrant proceedings that justified the creation of a completely ex parte court. That fundamental premise no longer holds now that the court also engages in bulk adjudication of programmatic surveillance, which does not resemble the individualized determinations made by a judge issuing a warrant. In those proceedings, there must be an individual who presents counterarguments to the government. Those counterarguments should not be statutorily limited, as they currently are under the FREEDOM Act. And there should be no exceptions to the invocation of an adverse party representative.

We would also recommend an expansion of responsibilities, such that an amicus is more akin to an "ombudsman." Ombudsmen, or "official[s] appointed to receive, investigate, and report on private citizens' complaints about the government,"[211] have been utilized in the Nordic countries for centuries to ensure that executive agencies comply with statutes and

209. *See In re* Application of the Fed. Bureau of Investigation for Orders Requiring the Prod. of Tangible Things, Nos. 15-77, 15-78, slip op. at 3–6 (FISA Ct. June 17, 2015), http://www.fisc.uscourts.gov/sites/default/files/BR%2015-77%2015-78%20Memorandum%20Opinion.pdf (suggesting that it may be unnecessary to appoint an amicus if "the court concludes . . . the legal question is relatively simple or is capable of only a single reasonable or rational outcome," or if the appointment would result in "some degree of additional expense and delay"); *see also* Elizabeth Goitein, *The FISC's Newest Opinion: Proof of the Need for an Amicus*, JUST SECURITY (June 23, 2015, 9:43 AM), http://www.justsecurity.org/24134/fiscs-newest-opinion-proof-amicus (describing weaknesses in Judge Saylor's analysis).

210. *See supra* notes 197–98 and accompanying text.

211. *Ombudsman*, BLACK'S LAW DICTIONARY (10th ed. 2014).

fulfill their public obligations.[212] This change in function has the potential to bring adversity to the court without undermining the legitimate needs of government to conduct confidential national security surveillance. The ombudsman would not have a limited role, raise only certain statutorily defined arguments, or serve at the discretion of FISC. Rather, the ombudsman would be generally charged with representing the public interests and ensuring that the government pursues surveillance more broadly in accordance with the Constitution and statutes of the United States. For example, we believe the ombudsman should be able to challenge the government's certification of "relevance" to a "foreign intelligence investigation."

A (preferable) alternative to appointing an ombudsman in cases involving bulk collection and programmatic surveillance, however, would be limiting the role of FISC, so that it only adjudicates individualized warrant applications, similar to pre-9/11 practices.

B. LIMITING FISC TO ADJUDICATING INDIVIDUAL CASES AND CONTROVERSIES

The approval of programmatic, as opposed to individualized, surveillance also raises questions regarding FISC's compliance with Article III's requirement that courts decide individual and real—not abstract—disputes. A fundamental premise of separation of powers principles is that courts resolve concrete cases, as opposed to merely issuing advisory opinions. The prohibition against Article III courts issuing advisory opinions has its foundation in "the earliest days of the Republic."[213] In short, federal courts cannot "decide abstract, hypothetical or contingent questions."[214] FISA Court bulk adjudication of programmatic surveillance arguably constitutes an advisory opinion in two distinct ways—the court's decisions are reviewed

212. *See The Parliamentary Ombudsman*, SIVILOMBUDSMANNEN, http://www.sivilombudsmannen.no/?lang=en_GB (last visited Apr. 11, 2016) (describing the role of the Norwegian Parliamentary Ombudsman).

213. Ronald J. Krotoszynski, Jr., *Constitutional Flares: On Judges, Legislatures, and Dialogue*, 83 MINN. L. REV. 1, 16 (1998).

214. Ala. State Fed'n of Labor v. McAdory, 325 U.S. 450, 461 (1945); *see also* Evan Tsen Lee, *Deconstitutionalizing Justiciability: The Example of Mootness*, 105 HARV. L. REV. 603, 644–45 (1992) (collecting Supreme Court characterizations of advisory opinions); Krotoszynski, *supra* note 213, at 17 ("This prohibition generally has been read to preclude federal courts, as a matter of basic Article III jurisprudence, from offering up advice on legal questions in the absence of a lawsuit brought by litigants with standing to maintain the action.").

post-judgment by the executive branch and the issues presented to the court are not yet ripe for review.[215]

We begin with ripeness, or the lack of a justiciable controversy. Under Section 702, "the [FISA] court has no role in approving individual intrusions at all. Rather, its substantive role is limited to determining whether generic sets of targeting and minimization procedures comply with the statute . . . and with the Fourth Amendment."[216] In essence, the court is ruling on the appropriateness of guidelines before they have been administered and applied to a particular person or search.[217] Even more problematic, the review is brought forward by the government itself—the party that develops the guidelines. The FISA Court acts more akin to an administrative adjunct, positing on the validity of various agency regulations before they actually go into effect. That is not a traditional Article III role and is of dubious constitutionality so long as FISC is labeled as a court over which Article III judges preside.

Second, there is the issue of post-judgment review by executive agencies. Even after the FISA Court issues its opinions on programmatic surveillance, the executive branch has a significant amount of flexibility to amend its procedures and searches. For example, after the FISA Court held that essentially *all* metadata is relevant to investigating terrorism under Section 215, the government had a blank check and could decide for itself how to sift through the collected data for potentially relevant information. Under Section 702, FISC merely approves generic targeting and minimization procedures, which contain enough flexibility that the government may then apply them in a variety of ways to specific searches and collected information. By approving programmatic surveillance, one step removed from potential infringements on individuals' rights, the court is not deciding an actual controversy—there has not even been a search or alleged violation of a statutory right.

We believe FISC should no longer engage in the approval of programmatic surveillance through bulk adjudication, which is an unanticipated evolution of FISA, following the enactment

215. Lee, *supra* note 214, at 645–52.

216. GOITEIN & PATEL, *supra* note 71, at 27.

217. Courts do engage in post-enactment review of rules issued by agencies under the Administrative Procedure Act. That review is different from FISC's, however, because an adversarial record is developed through notice and comment rulemaking, and Congress has chosen to create a cause of action for individuals. Finally, it is not the government that brings the action, but instead an individual aggrieved by the agency rules.

of the PATRIOT Act and FAA. Doing so not only contradicts the original intent of Congress in 1978 but also likely violates Article III of the Constitution. As discussed in Part II.B, FISC was supposed to be a court of limited jurisdiction, engaging in warrant-like adjudications. That is still an appropriate role for FISC, but *only* if the court is approving individual warrant applicants *ex ante* and individuals subject to surveillance are notified and able to challenge the surveillance *ex post*. However, FISC additionally approves broad searches—including one search authorized by a single court order issued under the FAA that permitted the targeting of 89,138 individuals, groups, and organizations.[218] The government cannot credibly argue that such a broad search is related to the individualized and specific facts that are the hallmark of Article III adjudications, especially when the search is premised on a factual certification by the government. By approving such broad searches, FISC lends legitimacy (and insulation) to programmatic surveillance, but not in a meaningful way that actually limits executive authority.

Even more problematic, however, FISC has become an adjunct to intelligence agencies, providing advisory opinions on the procedures that the agencies put in place. Those sorts of decisions should not be made by an Article III court, period.[219] And they certainly should not be made by an Article III court that can make broad constitutional and statutory interpretations contrary to the holdings of other, transparent and traditional, Article III courts.[220] Rather, the targeting and minimization procedures should be promulgated by an executive agency, and only considered by an Article III court if there is a cognizable injury to a party as a direct result of the application of those procedures. Pre-enforcement review of rules and regulations is limited within the confines of the Administrative Procedure Act.[221] The FISA Court should not regularly engage in such re-

218. *See* Barton Gellman et al., *The NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), http://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html.

219. *See* TRANSCRIPT, PCLOB WORKSHOP, *supra* note 194, at 36 (statement of Honorable James Robertson, Dist. Court, Foreign Intelligence Surveillance Court) ("[T]hat's not the bailiwick of judges. Judges don't make policy. They review policy determinations for compliance with statutory law but they do so in the context once again of adversary process.").

220. *See supra* notes 105–11 and accompanying text.

221. 5 U.S.C. § 704 (2015) (limiting judicial review to "final agency ac-

view, especially when it is only the government that presents the "issue" (i.e., proposed procedures) to the court, as opposed to an aggrieved party with a cognizable injury.

It may be argued that FISC's role approving programmatic surveillance is a necessary evil given the evolving nature of technology, the vast amount of information government agencies need to sift through in national security investigations, and the interconnectedness of society.[222] Certainly we agree that there is more information available and that the lines between domestic and international communications are blurry. However, this is all the more reason that the procedures under which the government collects and retains information should be subject to public scrutiny, and only addressed by a court if there is a concrete and ripe dispute.[223] Public debate of targeting and minimization procedures need not threaten national security. They are general procedures (which could be redacted as necessary) that apply regardless of who/what is being searched.

By approving generalized procedures rather than individualized warrants, the FISA Court is no longer acting like an Article III court charged with making individual and concrete decisions (and is no longer acting consistently with its original 1978 design). FISC instead operates more like an Article II adjunct to the executive branch, issuing advisory opinions on procedures before they are applied to a specific individual and set of facts. The court is already in a difficult position, lacking the benefit of an adversarial presentation of issues. It is even less likely to question the government when it is engaging in premature judicial review, without the benefit of an actual injury to serve as the basis for limiting government action.

C. EXPANDING OPPORTUNITIES FOR COLLATERAL CHALLENGE AND REVIEW

The constitutional requirements described in Sections A and B serve to protect more than the rights of individual litigants—they also ensure that all relevant arguments are made,

tion[s] for which there is no other adequate remedy in a court").

222. Increased globalization does pose a problem. The distinction between foreign and domestic communications is becoming increasingly blurry. However, this is all the more reason that procedures for searches pursuant to Section 702 should be publicly discussed and debated, giving members of society warning about the scope of their communications that may fall within the purview of a Section 702 search.

223. *See supra* notes 12–14 and accompanying text (discussing the importance of the procedural requirements of approving searches).

enabling the FISA Court to make more informed and impartial decisions, and citizens to actively and accurately participate in our constitutional democracy. The statutes and orders FISC has been enforcing "require[] *actual policy analysis*: weighing the security gains against liberty costs. Ideally, that weighing should occur in public."[224] The impact public discourse can have on society and the judiciary is evidenced by the nation's response to the Snowden disclosures.[225] Public pressure following the Snowden disclosures—including via Freedom of Information Act lawsuits—led to the declassification of FISC opinions and the eventual enactment of the FREEDOM Act. Even so, almost all FISA Court opinions remain classified. Although troubling in individual cases, this is particularly troubling when a court is making more binding statutory and constitutional interpretations than in the past.

First, as recognized by the FREEDOM Act, FISC should not issue confidential statutory and constitutional interpretations. Its only original purpose was to authorize individual subpoenas in the most sensitive cases involving national security—not to create binding, but confidential, legal precedent. FISC's statutory and constitutional interpretations are even more questionable when a traditional Article III court reaches a publicized contrary conclusion. Circuit splits in our federal court system are inevitable, but usually the two courts interpreting the statute or constitutional provision stand on equal footing in the eyes of Article III—the decision is made after a particular case or controversy is adjudicated in an adversarial setting. FISC, however, is not bound by any court other than the FISA Court of Review and the Supreme Court. Therefore, only months after the Second Circuit issued its thorough and

224. Schlanger, *supra* note 5 (emphasis added). Public scrutiny is particularly important because leaving regulation to "insiders" risks "impotence" and "capture." *Id.*

225. Similar public discourse, particularly in the wake of Watergate, led to the formation of the Church Committee and the eventual enactment of FISA.

> During the last eight years, beginning with *Ramparts* magazine's exposure of CIA covert relationships with non-governmental organizations, there has been a series of allegations in the press and Congress which have provoked serious questions about the conduct of intelligence agencies at home and abroad. The Watergate disclosures raised additional questions concerning abuse of power by the executive branch, misuse of intelligence agencies, and the need to strengthen legal restraints against such abuses.

CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 10; *see* SCHWARZ, *supra* note 167, at 175–76 (providing a thorough description of the Church Committee's origins).

well-reasoned opinion in *ACLU v. Clapper*, holding that the NSA's bulk collection program violated Section 215 (and likely the Fourth Amendment), the FISA Court disregarded the Second Circuit's opinion and upheld the program.[226] FISC reached its contrary conclusion after a process significantly less adversarial than that before the Second Circuit, undermining the public credibility of FISC's legal analysis. Thus, the "split" is not as justifiable as a traditional circuit split—especially given that the Second Circuit is a court of general jurisdiction, broadly tasked with interpreting law, whereas FISC is a court of limited jurisdiction, tasked with authorizing a limited subset of searches.

Even assuming that the FISA Court can create binding statutory and constitutional analysis, those interpretations must be made public. There is no doubt that "secrecy plays an essential role in delicate intelligence work . . . [but] it cannot justify submerging in shadow entire programs, sweeping policy changes, important shifts in law, or acts that subvert the ideals of America."[227] Such a justification is particularly lacking with regard to FISC, which was established to prevent disclosure of individual national security investigations and threats—very different from the broad and open-ended statutory interpretations of Sections 702 and 215, divorced from a specific search, in which the FISA Court currently engages. Although the FREEDOM Act does put procedures in place for declassification of certain opinions, there remain significant potential loopholes and ways for the government to evade disclosure.

A second related recommended reform is that there must be more opportunity for collateral review of the government's interpretation of national security laws. Society is demanding greater "transparency and accountability" mechanisms to ensure the government, with FISC's approval, does not subvert privacy to nominal security interests.[228] The publishing of redacted FISC opinions serves this goal because it may provide a basis for litigant standing to challenge a given collection prac-

226. *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things, No. BR 15-75, slip op. at 9–15 (FISA Ct. June 29, 2015) ("Second Circuit rulings are not binding on the FISC, and this Court respectfully disagrees with that Court's analysis . . . .").

227. SCHWARZ & HUQ, *supra* note 9, at 46.

228. *See* Letter from Advocacy for Principled Action in Gov't et al., to President Barack Obama et al. (Mar. 25, 2015), http://www.openthegovernment.org/sites/default/files/NSA_coalition_letter_032515.pdf (putting forth recommendations for legislation reauthorizing the PATRIOT Act).

tice. But traditional Article III courts can also further this goal by inquiring into the basis of the government's invocation of the state secrets privilege. Senator Leahy has introduced multiple bills with bipartisan support that would codify the state secrets privilege and courts' obligation to actually review the allegedly secret evidence.[229] Those proposed bills do not undermine the government's ability to assert the privilege and keep national security-related documents classified. "Rather, the bill[s] would allow judges to look at the actual evidence the Government submits so that they, neutral judges, rather than self-interested executive branch officials, would render the ultimate decision whether the State secrets privilege should apply."[230] Similarly, courts should not permit the government to completely dismiss suits that challenge the constitutionality of foreign surveillance under the state secrets doctrine. There is no reason that applying an *evidentiary privilege* should "permit the removal of *entire allegations* resulting in out-and-out dismissal of the entire suit"[231]—especially when courts have expertise reviewing classified information and FISC has procedures in place for in camera review of government submissions in adversarial FISC proceedings.[232] By blindly accepting the government's invocation of the state secrets privilege, courts abdicate their responsibility under *Marbury* to ensure that coordinate branches of government act in accordance with the Constitution.[233]

Both the publishing of redacted opinions and expanding of avenues for third party litigant challenges to FISC's statutory and constitutional interpretations reflect the same underlying value—there must be a certain amount of transparency and accountability in the operation of the intelligence community. This is important not only to reduce the current culture of impunity but also because "it is critical to the integrity of the process that the public have confidence in its impartiality and rigor."[234] Currently, there remains in our society "fundamental

229. *See* S. 417, 111th Cong. (2009); S. 2533, 110th Cong. (2008).

230. 155 CONG. REC. 3553, 3620 (2009) (statement of Sen. Patrick Leahy introducing S. 417).

231. Mohamed v. Jeppesen Dataplan, Inc., 614 F.3d 1070, 1098 (9th Cir. 2010) (en banc) (Hawkins, J., dissenting).

232. FISC R.P. 7.

233. Even the *Reynolds* court recognized that "[j]udicial control over the evidence in a case cannot be abdicated to the caprice of executive officers." Reynolds v. United States, 345 U.S. 1, 9–10 (1953).

234. PCLOB REPORT, SECTION 215, *supra* note 113, at 182.

distrust" of the intelligence agencies and systems put into place by FISA.[235] Some secrets must be protected in the name of national security.[236] But we must not permit a system in which the government can claim privilege without a coordinate branch of government confirming the validity of the invocation of that privilege. The Church Committee recommended that the "burden of proof should be on those who ask that a secret program or policy be kept secret."[237] That recommendation rings true today. The default must be transparency.

IV. PREVENTING A RELAPSE DURING THE NEXT NATIONAL EMERGENCY

Our "democratic system" must "effectively govern[] in the crucial area of secret intelligence."[238] Recently, Snowden's disclosures put pressure on the United States government to establish systems within the intelligence community that limit the power of intelligence agencies—not necessarily the power to conduct intelligence operations, but the power to conduct such operations at the cost of civil liberties. Congress responded to those pressures with the FREEDOM Act, which is an admirable step in the right direction. But given the continuous use of ambiguous statutory language and the lack of sufficient congressional oversight, the risk remains that "mission creep" will once again erode civil liberties as the nature of our enemies and foreign powers shift.

The Church Committee found that the subtle erosion of personal liberties occurred because Congress failed to issue clear laws and provide adequate oversight, and the courts thus could more easily avoid making clear rulings on the relationship between the executive and legislative branches when it came to national security.[239] In sum, the Committee found that

235. *Id.* at 15.

236. For example, the Church Committee suggested that "details about military activities, technology, sources of information and particular intelligence methods are secrets that should be carefully protected." CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 12–13. But the executive should not be able to shield embarrassing or controversial programs under the guise of security.

237. *Id.* at 8.

238. *Id.* at 15.

239. *See* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 185 ("The standards governing the use of these [surveillance] techniques have been imprecise and susceptible to expansive interpretation and in the absence of any judicial check on the application of these vague standards to particular cases, it was relatively easy for intelligence agencies and their superiors to extend

"intelligence activities have undermined the constitutional rights of citizens and that they have done so primarily because checks and balances designed by the framers of the Constitution to assure accountability have not been applied."[240] This fundamental lesson of constitutional law has once again been ignored in the wake of 9/11. The systems of checks and balances recommended by the Church Committee must be modified given the growth of the intelligence community, technological advances, and increased globalization.[241]

We use this final Part to return to the first principles of the Church Committee and bring foundational principles of separation of powers back to the discourse regarding security and individual liberties. We must reestablish a permanent system of external checks—via congressional committees, public disclosures (of general principles and systems, not specific information that could undermine intelligence operations), and traditional Article III review, informed by statutes with cogent and limiting language. Without "[c]lear legal standards and effective oversight," the abuses which led to the formation of the Church Committee and the Snowden disclosures may once again creep into intelligence practices, and "domestic intelligence activity . . . [will] undermine the democratic nation it is intended to protect."[242]

There must be robust congressional oversight, and that oversight must be embraced, not eschewed, by the intelligence community. The Church Committee found that intelligence overreach occurred in part because "Congress ha[d] not effectively fulfilled its constitutional role [as a check on the executive branch] in the area of domestic intelligence."[243] The Committee noted that although the "problem of how Congress can effectively use secret knowledge in its legislative process remains to be resolved . . . a strong and effective oversight committee is an *essential first step*" to addressing that challenge.[244] We need "empowered [] insiders who are attuned to

the[] [surveillance techniques] to many cases where they were clearly inappropriate.").

240. *Id.* at 289.

241. BRENNAN CTR. FOR JUSTICE, STRENGTHENING INTELLIGENCE OVERSIGHT 5–8 (Michael German ed., 2015) [hereinafter INTELLIGENCE OVERSIGHT].

242. *See* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 20.

243. *Id.* at 280.

244. CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 5 (emphasis added). For example, only a "few members" of Congress knew of the "secret charter for

civil liberties" because otherwise, when making intelligence decisions, civil liberties "receive[] not just less attention, but no consideration at all."[245] Moreover, given the inevitable need to classify some practices related to national security intelligence, it falls on Congress to ensure "that the authorities as they are publicly presented are consistent with the manner in which they are being exercised."[246]

Oversight today is undermined not only by structural changes—such as a larger intelligence community and technological advances—but also by institutional changes, particularly excessive congressional secrecy. For example, Congress was not "adequately informed about the NSA's post-9/11 collection activities" in the Terrorist Surveillance Program because "the Bush administration limited notifications regarding the NSA program to . . . the chairs and ranking members of each intelligence committee."[247] There may be some instances where, due to extraordinary circumstances regarding a covert action, limited notification may be appropriate. But "intelligence collection programs," such as those exposed by Edward Snowden, do not fall within that narrow category.[248]

Congressional oversight does not mean the executive branch will be constantly at odds with congressional committees. Instead, congressional oversight provides both an important check on executive authority by ensuring the executive branch is not misleading Congress and the public, and provides public legitimacy to "secret" operations.[249] Take, for example, the recent experience of Senator Diane Feinstein, Chair of the Senate Intelligence Committee, and the release of the torture

intelligence activities," and those that did had no means of discussing that information with other members of Congress. *Id.*

245. Schlanger, *supra* note 5.

246. *See* Donohue, *Section 702*, *supra* note 62, at 159.

247. INTELLIGENCE OVERSIGHT, *supra* note 241, at 10.

248. *See id.* at 10–11. Indeed, in February 2016 Congress held a hearing on Section 702 of the FAA but closed the hearing to the public, despite calls by civil rights organizations for opening the hearing, at least in part. *See* 162 CONG. REC. 5453 (daily ed. Feb. 2, 2016); Letter from Access Now et al., to Robert W. Goodlatte and John Conyers, Members, House Judiciary Comm. (Jan. 27, 2016), http://www.openthegovernment.org/sites/default/files/Letter%20for%20the%20Judiciary%20Committee%20on%20Section%20702%20Hearing.pdf.

249. *See* SCHWARZ, *supra* note 167, at 81 (noting that "the Bush-Cheney administration never permitted the public to 'be exposed to' a 'clear, sustained and principled debate on the merits,' [of post-9/11 detention and interrogation tactics] without 'excessive secrecy'").

report. Feinstein is one of the "bigge[st] booster[s] of the C.I.A.," but she also requires honesty and transparency from intelligence agencies.[250] As she has said, "Oversight can't just be going to a hearing and listening to what somebody says, when you don't know whether they're telling you the truth or not."[251] She was challenged by both the CIA and the White House when she began investigating allegations of torture and, even more so, when she decided to make some such information public. She was told that releasing the torture report would incite violence around the globe. But, despite the executive branch's dire predictions, the skies did not fall. Instead, both the executive branch and society were assured that the intelligence committee provided actual oversight.

Oversight goes hand-in-hand with providing clear statutory directives. Feinstein's primary recommendation to President Obama after the issuance of the report was closing legal "loopholes" that made the torture possible.[252] Such loopholes, often provided by fuzzy language, also exist in FISA, as amended by the PATRIOT Act, FAA, and FREEDOM Act. Take, for example, the use of the term "foreign intelligence" in Section 702—one of the terms identified by the Church Committee as providing "ambiguous" and "fuzzy instructions."[253] In 1978, FISA limited search authority to "foreign powers" and their "agents," not only narrowly defined terms but also terms that functionally served the needs of the intelligence community. The FAA, however, brought with it the return of the ambiguous term "foreign intelligence." Moreover, the FISA Court cannot question the executive branch's "foreign intelligence" determination, leaving the meaning of that term completely within the executive branch's discretion.[254] The use of such broad language is not good for a variety of reasons. First, it provides fodder to agencies that are prone to mission creep and prioritizing "security" over personal liberties.[255] Second, and perhaps more important-

250. Connie Bruck, *The Inside War*, NEW YORKER (June 22, 2015), http://www.newyorker.com/magazine/2015/06/22/the-inside-war.

251. *Id.*

252. *Id.*

253. *See supra* notes 31–44 and accompanying text.

254. Justice Douglas stated in *Katz v. United States* that the "[e]xecutive branch is not supposed to be neutral and disinterested" in cases involving national security. 389 U.S. 347, 359–60 (1967). We think that is an accurate statement, particularly when Congress opens the door by placing malleable phrases at the heart of the executive's authority.

255. As noted by civil rights scholar Margo Schlanger, "[P]ro-civil-liberties

ly, it provides minimal guidance to the FISA Court, which is already in a difficult position, serving as the only "adverse" party, or check, on the government's use of intelligence for security purposes.

The FAA provides a prime example of the interconnection between congressional oversight and clear statutory directives for an additional reason. At the time the FAA was enacted, Congress had limited information about the Terrorist Surveillance Program and, thus, the scope of programmatic surveillance.[256] So when Congress was "updating" FISA at the executive branch's request, it lacked complete information on the scope of programs to which it was giving statutory credence.[257] Therefore, most members of Congress did not "contemplate[] [the] broad, programmatic collection" Section 702 purportedly authorized.[258] If Congress had been operating with full knowledge of the scope of the Terrorist Surveillance Program, it is very likely it would have chosen different language when structuring Section 702, guaranteeing greater civil liberty protection to United States persons. And the lack of more artful draftsmanship by Congress opened the door for FISC to broadly interpret the statute in the government's favor via its traditional deference to the executive branch on issues of national security.[259]

Constitutional structural protections—such as robust congressional oversight and a comprehensive (and clear) statutory framework—are even more essential given the evolution of both technology and increased globalization. From 1978 to the present, as technology evolved, the intelligence community minimized the scope of those evolutions, attempting to acquire more

views have received all too little respect [in the intelligence community], unless transformed by a court or congress into authoritative law." Schlanger, *supra* note 5.

256. *See* Donohue, *Section 702*, *supra* note 62, at 158–59.

257. *See* INTELLIGENCE OVERSIGHT, *supra* note 241, at 11 (arguing that "the public, Congress, and the courts . . . [could not] meaningfully participate in the debate" regarding the Patriot Act and FAA because "most Americans (and even some members of Congress) did not know the scale of collection taking place under these authorities").

258. Donohue, *Section 702*, *supra* note 62, at 158–59. Notably, the few members of Congress that explicitly acknowledged concern that Section 702 would be used to engage in broad, programmatic surveillance, did not support the bill. *Id.* at 174.

259. *Id.* at 159 ("Congress similarly neglected to uphold the limit placed on the intelligence community to not knowingly collect domestic conversations. Instead, it relied on FISC to do so—a task that the Court failed to do.").

information through outdated modes of statutory and constitutional analysis. One Bush official recently stated that it was inaccurate to call the Terrorist Surveillance Program's collection of metadata "surveillance," because surveillance requires the acquisition of "content."[260] That may have been a convenient position for someone in the Department of Justice's Office of Legal Counsel, but it is contrary to public opinion and Article III court opinions issued through traditional, public, adversarial adjudication.[261] The next technological frontier is the scope of encrypted information the government should be able to access with a FISC order.[262] If the decisions are made behind closed doors, history has shown that the intelligence community is likely to broadly construe its searching authority and minimize technological incursions on privacy, unless some external authority questions the agency's application of former laws to new technology.[263]

In short, we are more likely to find the appropriate balance between security and liberty if intelligence agencies operate within the usual confines of the Constitution. No one—and no entity—is above the law. This fundamental premise of our constitutional democracy does not undermine our national security—it enhances it. Clear laws guiding intelligence agencies and courts interpreting the actions of those agencies will clarify the roles of both the executive and judicial branch. And strong congressional oversight will also serve to limit executive overreach. Each coequal branch must play its role, utilizing its unique competencies, if we are to find the right balance between security and liberty.

260. TRANSCRIPT, PCLOB WORKSHOP, *supra* note 194, at 16–21 (statements of Steven Bradbury, Retired, Office of Legal Counsel, U.S. Dep't of Justice).

261. *See, e.g.*, Riley v. California, 134 S. Ct. 2473 (2014) (holding that the Fourth Amendment extended to searches of cell phones).

262. Nicole Perlroth, *Tech Giants Urge Obama To Reject Policies that Weaken Encryption*, N.Y. TIMES (May 19, 2015), http://www.nytimes.com/2015/05/20/technology/tech-giants-urge-obama-to-reject-policies-that-weaken-encryption-technology.html.

263. *See generally* CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 281–84 (describing a pattern of intelligence agencies undertaking programs "without authorization, with insufficient authorization, or in defiance of express orders").

CONCLUSION

In the wake of 9/11, our country, for the second time in half a century, lost sight of the fact "that to ignore the dangers posed by secret government action is to invite the further weakening of our democracy."[264] A sense of urgency, similar to that catalyzed by the Church Committee's findings, returned in the wake of Edward Snowden's disclosures. Once again, "secrets" were unveiled, and the nation—and world—lost faith in our nation's ability to protect itself without invading individual liberties. Through the FREEDOM Act, Congress attempted to repair some of that lost faith. However, as we have shown, the FREEDOM Act does not remedy the structural and procedural wrongs currently plaguing the FISA Court and that court's relationship to coordinate branches of government.

The FISA Court no longer fulfills its intended limited role in adjudicating sensitive matters of national security. When the executive branch seeks a warrant to search a specific target or place, it is akin to a traditional warrant application and understandable that such a proceeding would need to be ex parte and confidential.[265] However, when the executive branch comes to a confidential court, asking it to approve procedures divorced from a specific search or controversy, asking it to approve the collection of myriad communications that may implicate United States persons, the executive branch is asking the court to exceed its original design and, more importantly, its constitutional role. To the extent the government needs approval of surveillance procedures and bulk collection unrelated to a specific investigative subpoena, those requests must be made through traditional mechanisms—whether administrative (via regulations) or judicial (via judicial review in traditional Article III courts). It cannot be that the only way to effectively further national security interests is to create a court that violates Article III of the Constitution.

There is undoubtedly an "inherent conflict between the government's *perceived* need to conduct surveillance and the citizens' constitutionally protected rights of privacy and dis-

264. CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 8.

265. *See, e.g.*, TRANSCRIPT, PCLOB WORKSHOP, *supra* note 194, at 35 (statement of Judge James Robertson) ("The FISA approval process works just fine when it deals with individual applications for surveillance warrants because approving search warrants and wiretap orders and trap and trace orders and foreign intelligence surveillance warrants *one at a time* is familiar ground for judges." (emphasis added)).

sent."[266] However, history has also taught us that the erosion of liberties for the sake of security is a risky prospect, and one that does more harm than good for our nation over the long run.[267] This is especially true given the "tragic conceit" of secrecy—"[i]nevitably, the truth prevails and policies pursued on the premise that they could be plausibly denied, in the end damage America's reputation and the faith of her people in their government."[268] As recognized by the Church Committee's domestic task force: "Knowledge is the key to control. Secrecy should no longer be allowed to shield the existence of the constitutional, legal and moral problems from the scrutiny of government or from the American people themselves."[269] It would be better for personal liberties, and the development of statutory and constitutional law, if FISC operated less as a shield to broad secret intelligence policies, and more like an Article III court.

266. CHURCH COMM. REPORT, BOOK I, *supra* note 1, at 6.
267. *See id.* at 6–7.
268. *Id.* at 16.
269. CHURCH COMM. REPORT, BOOK II, *supra* note 8, at 292.