BRENNAN
CENTER
FOR JUSTICE

WHAT WENT WRONG WITH THE FISA COURT

Elizabeth Goitein and Faiza Patel
Foreword by Judge James Robertson

Brennan Center for Justice *at New York University School of Law*

ABOUT THE BRENNAN CENTER FOR JUSTICE

The Brennan Center for Justice at NYU School of Law is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. We work to hold our political institutions and laws accountable to the twin American ideals of democracy and equal justice for all. The Center's work ranges from voting rights to campaign finance reform, from ending mass incarceration to preserving constitutional protection in the fight against terrorism. Part think-tank, part advocacy group, part cutting-edge communications hub, we start with rigorous research. We craft innovative policies. And we fight for them — in Congress and the states, the courts, and in the court of public opinion.

ABOUT THE BRENNAN CENTER'S LIBERTY AND NATIONAL SECURITY PROGRAM

The Brennan Center's Liberty and National Security Program works to advance effective national security policies that respect constitutional values and the rule of law, using innovative policy recommendations, litigation, and public advocacy. The program focuses on reining in excessive government secrecy; ensuring that counterterrorism authorities are narrowly targeted to the terrorist threat; and securing adequate oversight and accountability mechanisms.

ABOUT THE BRENNAN CENTER'S PUBLICATIONS

Red cover | Research reports offer in-depth empirical findings.
Blue cover | Policy proposals offer innovative, concrete reform solutions.
White cover | White papers offer a compelling analysis of a pressing legal or policy issue.

ABOUT THE AUTHORS

Elizabeth (Liza) Goitein co-directs the Brennan Center for Justice's Liberty and National Security Program. Before coming to the Brennan Center, Ms. Goitein served as counsel to Sen. Russell Feingold, Chairman of the Constitution Subcommittee of the Senate Judiciary Committee. As counsel to Sen. Feingold, Ms. Goitein handled a variety of liberty and national security matters, with a particular focus on government secrecy and privacy rights. Previously, Ms. Goitein was a trial attorney in the Federal Programs Branch of the Civil Division of the Department of Justice. Ms. Goitein graduated from the Yale Law School and clerked for the Honorable Michael Daly Hawkins on the U.S. Court of Appeals for the Ninth Circuit.

Faiza Patel serves as co-director of the Brennan Center for Justice's Liberty and National Security Program. She has testified before Congress opposing the dragnet surveillance of Muslims, organized advocacy efforts against state laws designed to incite fear of Islam, and developed legislation creating an independent Inspector General for the NYPD. Before joining the Brennan Center, Ms. Patel worked as a senior policy officer at the Organization for the Prohibition of Chemical Weapons in The Hague, and clerked for Judge Sidhwa at the International Criminal Tribunal for the former Yugoslavia. Born and raised in Pakistan, Ms. Patel is a graduate of Harvard College and the NYU School of Law.

ACKNOWLEDGEMENTS

The authors would like to thank the Brennan Center's Mike German, Seth Hoy, John Kowal, Rachel Levinson-Waldman, Jim Lyons, Michael Price, Desiree Ramos Reiner, Frederick A.O. Schwarz, Jr., and Amos Toh for their invaluable input and assistance. The authors also are grateful to Jeremy Carp, Monte Frenkel, Meghan Koushik, Brynne O'Neal, and Shannon Parker for their dedicated research assistance. In addition, the authors benefited greatly from conversations and correspondence with David Anderson, Laura Donohue, Barry Friedman, David Kris, Stephen Schulhofer, Patrick Toomey, and Stephen Vladeck.

The authors wish to express special gratitude to James Robertson for his contribution to this report as well as for his many years of service on the U.S. District Court for the District of Columbia and the FISA Court.

The Brennan Center gratefully acknowledges The Atlantic Philanthropies, The Herb Block Foundation, C.S. Fund, Democracy Alliance Partners, Ford Foundation, and Open Society Foundations for their generous support of the Liberty & National Security Program.

TABLE OF CONTENTS

FOREWORD

by James Robertson, U.S. District Judge (ret.)

Many people are surprised to learn that there is no "right to privacy" in the Constitution. Privacy is more of a cultural construct than a legal one in this country, and we are aiding and abetting its steady erosion with our dependence on the Internet, our credit cards and smartphones, our flirtation with social media, and our capitulation to commercial exploitation of Big Data. In a sense, we are all under surveillance, all the time — our whereabouts, activities, and transactions reduced to metadata and available to anyone who can break the code — and we have brought it upon ourselves.

Surveillance by the government, however, is another matter. Distrust or at least wariness of a government that collects data about us lies deep in the amygdala of our civic consciousness. *This* administration may be operating lawfully and with full regard to our rights and privileges, but what about *that* one? Have we been reading too many novels, or is there a real threat of tyranny? Here, of course, is where the Constitution comes in, with the Fourth Amendment's guarantee of "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."

And here is where concern about the Foreign Intelligence Surveillance Act comes in. Title III of the Omnibus Crime Control and Safe Streets Act of 1968 established the rules for domestic government wiretaps. FISA, enacted ten years later, focused on foreign intelligence. But it is the use (or misuse) of FISA, and FISA's potential allowance of unreasonable *domestic* searches and seizures, that the reporting of James Risen and Eric Lichtblau and the disclosures of Edward Snowden have brought into sharp focus.

I have no criticism of the FISA Court. I know and deeply respect every one of its presiding judges for the last 30 years, and I am well acquainted with many of the other FISA judges who have served. They are, every one of them, careful and scrupulous custodians of the extraordinary and sensitive power entrusted to them. The staff that supports the FISA Court, the Justice Department lawyers who appear before the FISA Court, and the FBI, CIA and NSA personnel who present applications to the FISA Court are superb, dedicated professionals.

What I do criticize is the mission creep of the statute all of those people are implementing.

This Brennan Center report makes an enormous contribution to our understanding of that mission creep. It explains clearly the history and development of FISA from its enactment following the Church Committee's exposure of uncontrolled domestic spying by the FBI, through the Patriot Act amendments in the turbulent wake of the 9/11 attacks, to its present form. It explains, with a simplicity and clarity accessible to the layman but supported by a level of detail and citation of authority that will satisfy students of the subject, why in its present form FISA is disturbing to civil libertarians and to constitutional scholars. And it distills its argument into plain, powerful recommendations for FISA's amendment.

It is time, and past time, for Congress to give serious attention to the FISA problems that are so clearly documented here, and to act. The Brennan Center's recommendations are not the only ones that have been put forth, but they are not doctrinaire, my-way-or-the-highway demands. They invite discussion, debate, and even (Heaven forfend) compromise. They need to be carefully considered.

James Robertson served on the U.S. District Court for the District of Columbia from 1994 to 2010. He also served on the Foreign Intelligence Surveillance Court from 2002 to 2005, resigning the day after The New York Times *reported that the administration of President George W. Bush was conducting warrantless surveillance of Americans' electronic communications.*

INTRODUCTION

In 2013, a former government contractor named Edward Snowden revealed that United States surveillance programs supposedly aimed at foreign threats were being used to collect unprecedented amounts of information about ordinary Americans. Documents disclosed by Snowden showed that the National Security Agency (NSA) had been collecting Americans' telephone records in bulk for years under Section 215 of the USA Patriot Act[1] — a practice seemingly at odds with the text of the law. In addition, the government was collecting a massive number of Americans' phone calls and e-mails "incidentally" or "inadvertently" under Section 702 of the FISA Amendments Act (FAA) — a statute that permits the government to target only non-citizens located overseas — and using this information in domestic criminal investigations.

In defending these activities, President Obama and top intelligence officials argued that they had been blessed by the Foreign Intelligence Surveillance Court, known as "the FISA Court." This judicial body, which until then had been familiar only to specialists in surveillance law, was suddenly at the center of debates about the proper limits on the government's authority to collect information on ordinary Americans.

The FISA Court is a unique creature within the federal judiciary. Established by Congress in 1978 as part of the Foreign Intelligence Surveillance Act (FISA),[2] the court's original mandate was to review the government's applications to collect "foreign intelligence" — information relating to foreign affairs and external threats — in individual cases. Its judges, who are drawn from among federal trial judges and selected by the Chief Justice of the United States, generally hear from just one party: the government. Proceedings are closed and the court's decisions are classified. Most targets receive no notice of the surveillance, even after investigative activity has ceased.

At the time of its creation, many lawmakers saw constitutional problems in a court that operated in total secrecy and outside the normal "adversarial" process (i.e., with both parties present). But the majority of Congress was reassured by similarities between FISA Court proceedings and the hearings that take place when the government seeks a search warrant in a criminal investigation. Moreover, the rules governing who could be targeted for "foreign intelligence" purposes were narrow enough to mitigate concerns that the FISA Court process might be used to suppress political dissent in the U.S. — or to avoid the stricter standards that apply in domestic criminal cases.

In the years since then, however, changes in technology and the law have altered the constitutional calculus. Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a few years ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.

Instead of increasing safeguards for Americans' privacy as technology advances, the law has evolved in the opposite direction since 9/11. It increasingly leaves Americans' information outside its protective shield. While surveillance involving Americans previously required individualized court orders, it now

happens through massive collection programs (known as "programmatic surveillance") involving no case-by-case judicial review. The pool of permissible targets is no longer limited to foreign powers — such as foreign governments or terrorist groups — and their agents. Furthermore, the government may invoke the FISA Court process even if its primary purpose is to gather evidence for a domestic criminal prosecution rather than to thwart foreign threats.

Much has been written about the effect of these developments on Americans' privacy, not to mention the lawfulness of the NSA's actions. But these developments also have had a profound effect on the role exercised by the FISA Court. They have caused the court to veer off course, departing from its traditional role of ensuring that the government has sufficient cause to intercept communications or obtain records in particular cases and instead authorizing broad surveillance programs. It is questionable whether the court's new role comports with Article III of the Constitution, which mandates that courts must adjudicate concrete disputes rather than issuing advisory opinions on abstract questions. The constitutional infirmity is compounded by the fact that the court generally hears only from the government, while the people whose communications are intercepted have no meaningful opportunity to challenge the surveillance, even after the fact.

Moreover, under current law, the FISA Court does not provide the check on executive action that the Fourth Amendment demands. Interception of Americans' communications generally requires the government to obtain a warrant based on probable cause of criminal activity. Although some courts have held that a traditional warrant is not needed to collect foreign intelligence, they have imposed strict limits on the scope of such surveillance and have emphasized the importance of close judicial scrutiny in policing these limits. The FISA Court's minimal involvement in overseeing programmatic surveillance does not meet these constitutional standards.

Fundamental changes are needed to fix these flaws. Following Snowden's disclosures, several bills were introduced to try to ensure that the court would hear the other side of the argument, generally from some type of public advocate. Other bills addressed the court's secrecy by requiring the executive branch to declassify significant opinions or release summaries. These proposals would make important improvements, but they do not address the full range of constitutional deficiencies resulting from the changes in law and technology detailed in this report. The problem with the FISA Court is far broader than a particular procedure or rule. The problem with the FISA Court is FISA.

The report proposes a set of key changes to FISA to help restore the court's legitimacy.

- Congress should end programmatic surveillance and require the government to obtain judicial approval whenever it seeks to obtain communications or information involving Americans. This would resolve many constitutional concerns.

- Congress should shore up the Article III soundness of the FISA Court by ensuring that the interests of those affected by surveillance are represented in court proceedings, increasing transparency, and facilitating the ability of affected individuals to challenge surveillance programs in regular federal courts.

- Finally, Congress should address additional Fourth Amendment concerns by ensuring that the collection of information under the rubric of "foreign intelligence" actually relates to our national security and does not constitute an end-run around the constitutional standards for criminal investigations.

Under today's foreign intelligence surveillance system, the government's ability to collect information about ordinary Americans' lives has increased exponentially while judicial oversight has been reduced to near-nothingness. Nothing less than a fundamental overhaul of the type proposed here is needed to restore the system to its constitutional moorings.

I. THE CREATION OF THE FISA COURT

The Foreign Intelligence Surveillance Act of 1978 established a special secret court to consider government requests to conduct the special category of "foreign intelligence" surveillance in the United States.

The FISA Court was designed to accommodate the government's need to obtain surveillance orders secretly and in a hurry. It consists of 11 federal trial judges[3] appointed by the Chief Justice of the United States for a single seven-year term.[4] These judges continue serving on their regular courts, but spend one week out of every 11 on the special court in Washington, DC, ensuring a continuous rotation.[5] Congress also created the Foreign Intelligence Court of Review ("FISA Appeals Court"), consisting of three federal trial or appellate judges also selected by the Chief Justice of the United States, to hear appeals in cases where the FISA Court has denied the government's application.[6]

Congress believed that this system of "[r]equiring the special court to sit continuously in the District of Columbia will facilitate necessary security procedures and, by ensuring that at least one judge is always available, will ensure speedy access to it by the Attorney General when timeliness is essential for intelligence purposes."[7] An additional benefit of a specialized court was that it was "likely to be able to put claims of national security in a better perspective and to have greater confidence in interpreting this bill than judges who do not have occasion to deal with the surveillances under this bill."[8]

Despite these predicted benefits, there was considerable concern in Congress that the court's consideration of surveillance applications might run afoul of Article III of the Constitution, under which federal courts are limited to deciding "cases or controversies" — real disputes, which courts are capable of resolving.[9] American courts are barred from giving what are known as "advisory opinions," in which a court examines the law in the abstract rather than in the context of an actual dispute.[10] Legislators and legal experts were particularly concerned that the FISA structure — under which the government's attorney alone would appear in secret before a specially designated judge — would eviscerate the adversarial process and force the court to apply a limited scrutiny of the government's assertions, rather than produce a resolution of contested facts.[11]

The Justice Department's Office of Legal Counsel (OLC), asked for its views by Congress, agreed that the Article III question was "difficult."[12] In ultimately concluding that the constitutional requirement was satisfied, OLC relied heavily on the fact that FISA Court judges, even though they had a limited role in reviewing surveillance applications, would still be applying the law to the facts of a particular case.[13] Moreover, even though only the government would appear before the court, OLC argued that the presence of two parties is not required in every case; instead there need only be "adversity in fact" or "possible adverse parties."[14] In support, OLC pointed out that in normal criminal cases, the government is permitted to persuade a court of the need for a warrant without the target being present.[15]

A similar reasoning underpinned later court decisions upholding FISA against Article III challenges. As explained by the District Court for the Eastern District of New York, the "case or controversy" standard was met because surveillance applications under the statute "involve concrete questions respecting the

application of the Act and are in a form such that a judge is capable of acting on them, much as he might otherwise act on an *ex parte* application for a warrant."[16] Courts also relied on the similarity to regular warrants in rejecting the argument that FISA Court proceedings violate Article III because the court hears applications solely on an *ex parte* basis (i.e., with only one party appearing before it) and never conducts adversarial proceedings (i.e., with the opposing parties present).[17]

Those opposed to the legislation during its consideration, however, emphasized that FISA Court orders were not like regular warrants because their validity could not be attacked in later proceedings. As then-Professor Laurence Silberman argued: "Although it is true that judges have traditionally issued search warrants *ex parte*, they have done so as part of a criminal investigative process which … for the most part, leads to a trial, a traditional adversary proceeding."[18] In a criminal trial, the defendant has the opportunity to challenge the means by which the government obtained its evidence, thus subjecting the search to adversarial testing.

These concerns prompted an important amendment to the legislation, intended to facilitate "collateral attacks" — challenges that take place in subsequent or parallel legal proceedings — in at least some cases. The government was required to notify the defendant when "any information obtained or derived from an electronic surveillance" of that individual was to be used in criminal prosecutions or other legal proceedings.[19] These notice provisions allowed the initial spate of challenges to warrants issued under the 1978 version of FISA.

As the above discussion makes clear, in designing the FISA Court, Congress took account of the strictures of Article III; and both Congress and the courts drew comfort from the similarities between the procedures used by the special court and those used for regular warrants.

II. THE FISA COURT'S ORIGINAL MANDATE

The Foreign Intelligence Surveillance Act detailed the types of surveillance that could be authorized by the FISA Court, as well as the standards and procedures for authorization. Absent an emergency, the statute required the government to obtain an individualized court order prior to conducting electronic surveillance to obtain foreign intelligence in the United States. The statute is a complicated one, and a short detour through the political and legal landscape of the 1970s is helpful in understanding the choices Congress made in defining the court's mandate.

A. The Legal Backdrop

From the late 1960s through the 1970s, courts wrestled with the legal status of electronic surveillance under the Fourth Amendment. Even as the Supreme Court conceded that the Fourth Amendment extended to emerging technologies and that a warrant was needed to tap telephones, it sought to develop rules for national security surveillance. These rules took account of the executive branch's interest in protecting the country, while ensuring that this interest was not an excuse for bypassing traditional Fourth Amendment constraints or for targeting the dissident voices of Americans protected by the First Amendment.

Three conclusions emerge from the cases decided during this time. First, in order to intercept an American's electronic communications, the government normally must obtain a warrant by demonstrating to a court that it has probable cause to believe that the person targeted is involved in criminal activity. Second, a warrant is required for surveillance of domestic organizations within the U.S., even if the purpose is to protect national security. Third, several courts of appeal held that a warrant is not required to obtain the special category of "foreign intelligence." But these courts imposed strict conditions to ensure that the government was truly seeking information about foreign powers or their agents, and they recognized the importance of a judicial role in scrutinizing the government's motives.

1. Extension of the Warrant Requirement to Electronic Surveillance

Until the late 1960s, when the Supreme Court decided the seminal case *Katz v. United States*,[20] the Court had held that the Fourth Amendment's requirement of a warrant did not extend to telephone conversations because wiretapping involved no intrusion into a person's physical property.[21] The *Katz* decision jettisoned this reasoning, famously declaring that the Fourth Amendment "protects people — and not simply 'areas' — against unreasonable searches and seizures."[22] Judicial review prior to wiretapping was essential, the Court explained, because otherwise law enforcement agencies themselves would decide whom to target and for how long.[23] In a footnote, however, the majority inserted a caveat: "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."[24]

The principal holding of *Katz* was enshrined into law in the 1968 Omnibus Crime Control and Safe Streets Act.[25] Title III of the law authorized surveillance of electronic communications in investigations of specified serious crimes.[26] Wiretaps had to be authorized by a judge or magistrate who would evaluate

whether there was probable cause to believe that one of these crimes had been, was being, or was about to be committed.[27] In keeping with the *Katz* footnote, however, Title III refrained from explicitly regulating national security surveillance.[28]

2. National Security Surveillance

In the 1972 case *United States v. U.S. District Court* (known as the "*Keith*" case after the district court judge), the Supreme Court partially addressed the question that *Katz* and Title III avoided: it held that surveillance of domestic organizations for national security purposes did require a warrant.[29] But the Court expressly left open — and has never ruled on — the question of whether a different rule might apply if the government were seeking intelligence about a foreign power or its agent.

Keith involved three anti-war activists charged with participating in a conspiracy to destroy government property. When the defendants sought to suppress evidence obtained through wiretaps, the government argued that it was entitled to tap their phones without a warrant because it sought to "gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."[30] The Court rejected this argument, ruling that the Fourth Amendment required a warrant for surveillance "deemed necessary to protect the nation from attempts of *domestic organizations*."[31] The opinion made clear, however, that the Court was not passing judgment "on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[32]

The *Keith* Court observed that national security cases "often reflect a convergence of First and Fourth Amendment values not present in cases of 'ordinary' crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech" because the targets of official surveillance "may be those suspected of unorthodoxy in their political beliefs."[33] Given the important separation of powers function historically served by warrants, the Court held that executive officials charged with enforcing the laws should not also decide when to employ "constitutionally sensitive means in pursuing their tasks."[34]

Although it insisted on a warrant in domestic security cases, the *Keith* Court acknowledged that the standards and procedures surrounding the warrant requirement "may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."[35] The Court thus invited Congress to create special rules for domestic security surveillance. As examples, the Court suggested that different facts might support a showing of "probable cause"; that the warrant application could, "in sensitive cases," be made to any member of a specially designated court; and that the duration and reporting requirements could be less strict.[36]

Justice Douglas: A Forceful Voice for Privacy

Justice William O. Douglas penned an influential concurring opinion in *Keith*, arguing that the privacy risks posed by domestic security wiretapping require it to remain firmly within the framework of traditional Fourth Amendment jurisprudence. To begin with, due to the clandestine nature of wiretapping, those who have been illegally bugged are unlikely to be able to obtain recourse. Thus, if no warrant were required for such taps, "the federal intelligence machine would literally enjoy unchecked discretion."[37] Moreover, once started, intelligence investigations could lead to virtually unrestrained spying. In the case before the Court, Douglas observed, "federal agents wish to rummage for months on end through every conversation, no matter how intimate or personal, carried over selected telephone lines, simply to seize those few utterances which may add to their sense of the pulse of a domestic underground."[38] The type of "dragnet techniques" favored by the government, Douglas argued, were reminiscent of the general warrants used by the British in colonial times, the excesses of which gave birth to the Fourth Amendment.[39]

3. Foreign Intelligence Surveillance

The Supreme Court's decision in *Keith* effectively turned the conversation away from national security to foreign intelligence surveillance. The Court itself has never decided whether special rules could be articulated for spying on foreign powers or other types of foreign intelligence collection in the United States. Several federal appeals courts, however, took up the question that the Supreme Court left open in *Keith*: whether a warrant is required to conduct surveillance for foreign intelligence purposes.

Four courts of appeal held that no warrant was needed in cases where the President or his delegate had certified that collecting foreign intelligence was the purpose of intercepting the communications of particular individuals.[40] The Fourth Circuit's 1980 decision in *United States v. Truong Dinh Hung* distills the reasoning presented in these cases: a warrant requirement would "unduly frustrate" the president's exercise of his foreign affairs responsibilities.[41]

The *Truong* court, however, set two important limitations on the president's authority to conduct warrantless surveillance inside the United States. First, the object of the search must be "a foreign power, its agent or collaborators," because in such cases, "the government has the greatest need for speed, stealth, and secrecy," and would likely have to make "difficult and subtle judgments about foreign and military affairs."[42] When there is no such connection, the court held, the "executive's needs become less compelling; and the surveillance more closely resembles the surveillance of suspected criminals, which must be authorized by warrant."[43]

The second condition was that the surveillance must be conducted "primarily" for foreign intelligence reasons.[44] When the government instead conducts surveillance primarily for a criminal investigation, the judiciary's competence increases, individual privacy interests "come to the fore," and government foreign policy concerns recede. The court explicitly "reject[ed] the government's assertion that, if

surveillance is *to any degree* directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment."[45]

The other courts of appeal applied a similar analysis, and underscored the need for judges to ensure that the government actually was pursuing foreign intelligence. Because the justification for foreign intelligence wiretapping generally would not be disclosed to the subject of surveillance or to the public, judges bore a special responsibility to be vigilant; they must "insure that there be no future tidal wave of warrantless wiretaps and that the floodgates controlling their use not be opened for domestic intelligence purposes."[46] A departure from the warrant requirement required caution and close judicial review (albeit after-the-fact) of each particular case in which surveillance was challenged.[47]

The Court of Appeals for the District of Columbia took a different approach, refusing to endorse warrantless foreign intelligence surveillance. In the 1975 case *Zweibon v. Mitchell*,[48] the government defended its warrantless wiretapping of the Jewish Defense League's offices by arguing that the organization's anti-Soviet activities jeopardized U.S. relations with the Soviet Union. The D.C. Circuit rejected this justification, finding that a warrant was required "before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power, even if the surveillance is installed under presidential directive in the name of foreign intelligence gathering for protection of the national security."[49]

While it did not hold that a warrant would be needed to target a foreign power, the *Zweibon* court hinted at how it might rule on the issue, observing, "[A]n analysis of the policies implicated by foreign security surveillance indicates that, absent exigent circumstances, all warrantless electronic surveillance is unreasonable and therefore unconstitutional…."[50] Its holding reinforced both the need for judicial caution in evaluating foreign intelligence claims and the Supreme Court's earlier prohibition on conducting domestic security surveillance without a warrant.

Despite their differences, the courts of appeals all agreed that strict limits were necessary when the government exercised its authority to collect foreign intelligence in the United States.

The Fourth Amendment Overseas

Title III, *Katz*, *Keith*, and the foreign intelligence exception cases all addressed surveillance conducted on U.S. soil. They did not consider the rules that applied to surveillance conducted overseas. In 1990, in *U.S. v. Verdugo-Urquidez*, a plurality of the Supreme Court found that the Fourth Amendment did not apply to a physical search conducted overseas by American agents where the target of the search was a foreigner who lacked sufficient connections to the United States.[51] This case has been cited widely for the proposition that foreigners overseas are not entitled to the protections of the Fourth Amendment, although a majority of the justices did not state such a broad view.[52]

B. The Political Backdrop

In the 1970s, the country was roiled by a series of spying scandals. In 1972, *The Washington Post* revealed that President Nixon's White House was spying on and sabotaging political opponents.[53] Two years later, *The New York Times* reported that the Central Intelligence Agency (CIA), on President Lyndon Johnson's orders, had conducted a massive intelligence operation against critics of the Vietnam War, other domestic dissidents, and journalists the administration considered unfriendly.[54] A series of other CIA abuses — covert operations to overthrow foreign governments, plots to assassinate foreign leaders, secret drug experiments on unsuspecting victims, and the illegal opening of mail sent by Americans — came to light.[55]

These reports triggered Congressional investigations, the best known of which was conducted by a specially convened Senate committee known as the Church Committee.[56] Over the course of its two-year long investigation, the Church Committee catalogued a host of abuses both overseas and at home. Some of its key findings included:

- The Federal Bureau of Investigation's (FBI) Counterintelligence Program (COINTELPRO) began in 1956 when President Dwight Eisenhower authorized the Bureau, run by J. Edgar Hoover, to conduct domestic covert operations, which included "disinformation, mail interception, electronic surveillance, tax surveillance, forgeries, harassment, even clandestine trash inspection."[57] Its targets included the U.S. Communist Party, anti-Vietnam War protesters, the New Left, and African American groups ranging from Rev. Martin Luther King, Jr.'s Southern Christian Leadership Conference to the Nation of Islam and the Black Panthers.[58] Most infamously, the FBI sought to blackmail King into suicide by threatening to expose his extramarital affairs.[59]

- Between 1953 and 1973, the CIA checked more than 28 million letters (mostly to and from the Soviet Union) against a watch list, and opened 200,000.[60]

- In 1967, President Lyndon Johnson instigated a program to determine whether foreign Communist agents were fomenting the unrest that was sweeping the country in the form of anti-war protests, college campus takeovers, and urban riots. A special CIA unit collected information on 7,000 Americans and 6,000 groups engaged in these activities until 1974, even though it never found any credible evidence of foreign involvement.[61]

- In a program named "Project Shamrock," which stretched from the mid-1940s to the mid-1970s, the NSA copied and analyzed international telegrams sent by American citizens.[62] At the end of the program, many estimate the NSA was analyzing 150,000 messages a month.[63]

The Church Committee: A Prescient View

Even four decades ago, the Church Committee was concerned about newly emergent electronic surveillance capabilities. Its chairman cautioned:

> In the need to develop a capacity to know what potential enemies are doing, the United States government has perfected a technological capability that enables us to monitor the messages that go through the air . . . . Now, that is necessary and important to the United States as we look abroad at enemies or potential enemies. We must know, at the same time, that capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything — telephone conversations, telegrams, it doesn't matter. There would be no place to hide.
>
> If this government ever became a tyranny, if a dictator ever took charge in this country, the technological capacity that the intelligence community has given the government could enable it to impose total tyranny, and there would be no way to fight back because the most careful effort to combine together in resistance to the government, no matter how privately it was done, is within the reach of the government to know. Such is the capability of this technology.[64]

Many reforms were enacted in the period immediately following the Church Committee's investigations, including the establishment of standing intelligence committees in both the House and the Senate, the extension of inspector general oversight to the activities of certain intelligence agencies and components, and the establishment of internal Department of Justice guidelines that restricted the FBI's authority to conduct open-ended domestic intelligence investigations.[65] The 1978 Foreign Intelligence Surveillance Act (FISA) was one of these reforms.

C. A New Statutory Scheme for Foreign Intelligence Surveillance

The political pressure generated by Watergate and the findings of the Church Committee motivated both the executive branch and Congress to come up with a scheme for regulating national security surveillance. Three crucial points emerge from the debates that led up to the enactment of the Foreign Intelligence Surveillance Act. First, Congress soundly rejected the notion that the executive had unilateral authority to collect foreign intelligence in the United States. Second, Congress declined the *Keith* Court's invitation to make special rules for warrants seeking to obtain domestic intelligence, leaving in place a regular warrant requirement.[66] Third, Congress agreed that a special scheme was necessary for foreign intelligence surveillance conducted at home, but placed strict limits on such surveillance to ensure that it would not be used to suppress domestic dissent or to evade the warrant requirement in ordinary criminal cases.

The first attempt at comprehensive legislation on foreign intelligence surveillance was a proposal by President Gerald Ford in 1976.[67] The bill never passed. Many lawmakers objected strongly to a provision conceding that the president had authority to order surveillance outside of any statutory framework passed by Congress.[68] Lawmakers also were concerned that the bill's standard for authorizing surveillance — namely, probable cause that the target was a foreign power or its agent — was too low. They argued that surveillance should be initiated against Americans only if the government showed probable cause that they had committed or were about to commit a crime.[69]

The following year, Sen. Edward Kennedy (D-Mass.) introduced a bill on electronic surveillance that was supported by the new administration of President Jimmy Carter and formed the basis of FISA as eventually enacted.[70] Responding to concerns expressed over the Ford bill, Kennedy removed the provision recognizing presidential authority to order surveillance for national defense purposes. The new bill also required some nexus to criminal activity in order for surveillance targeted at Americans to be authorized. The stringency of this requirement was hotly debated in Congress, as were the following provisions aimed at ensuring that surveillance approved by the FISA Court would truly be aimed at gathering foreign intelligence.

What Is "Electronic Surveillance"?

FISA regulates "electronic surveillance," which it defines to include four categories of activity: (1) acquisition of wire or radio communications that intentionally targets "a particular, known United States person who is in the United States"; (2) acquisition within the United States of wire communications (e.g., calls made via land lines) to or from a person in the United States; (3) intentional acquisition of radio communications (e.g., satellite communications) "if both the sender and all intended recipients are located within the United States"; and (4) electronic monitoring within the United States to obtain information other than through a wire or radio communication (e.g., planting bugs).[71]

These complex categories defy simple generalizations. For instance, while FISA is often described as regulating surveillance that occurs within the United States, the description is both under- and over-inclusive: FISA actually regulates *overseas* surveillance of radio communications if all parties to the communication are located in the United States, and it does *not* regulate surveillance within the United States of radio communications between people in the United States and foreigners overseas. Nor does FISA regulate the wiretapping within the United States of communications between foreigners overseas that transit through the United States.

1. Agent of a Foreign Power

The availability of electronic surveillance under FISA as enacted in 1978 depended on whether the government could show probable cause that the person or group being targeted was a "foreign power" or an "agent of a foreign power." The statute defines "foreign power" broadly, to include not only foreign governments, but also factions of foreign nations; entities that foreign governments control; international terrorist groups; foreign-based political organizations; and foreign entities engaged in the proliferation of weapons of mass destruction.[72]

The term "agent of a foreign power" is more narrowly defined for U.S. persons[73] than for non-U.S. persons, requiring some connection to criminal activity.[74] The legislative history shows that Congress employed this narrower definition deliberately to ensure that FISA did not ensnare ordinary Americans exercising their First Amendment rights. The Ford bill would have allowed surveillance of U.S. persons without any criminal nexus. The 1977 Kennedy bill, by contrast, proposed that an American should not be considered an agent of a foreign power unless he or she knowingly engaged in "clandestine intelligence activities" that "involve or will involve a violation of the criminal statutes of the United States."[75]

Even then, lawmakers worried that the formulation was too broad and would capture activities that "border on political activities protected by the First Amendment."[76] To safeguard against "unjustified surveillance of political activities," the wording was amended so that only "clandestine intelligence *gathering* activities" would be covered.[77] According to the legislative history, it was "anticipated that most of the persons under surveillance under this subparagraph will be violating the criminal espionage laws…."[78]

Legislators also were concerned that the second part of the formulation (which required that an American target's activities "involve or will involve" a criminal act) would permit indefinite surveillance based on a vague suspicion of an unspecified, and possibly minor future crime.[79] In the legislative history, lawmakers clarified that this provision was intended to impose a requirement that a federal crime must have already been committed or must be imminent before surveillance is justified.[80]

Finally, Congress made clear that mere association with agents of a foreign power or ideological sympathy with a foreign government would not trigger surveillance.[81] Legislators frequently cited the case of Martin Luther King, Jr., whose phone and home had been bugged by the FBI on "national security grounds" because of his association with suspected communists.[82] To ensure that such surveillance could not occur under FISA, Congress added language clarifying that aiding and abetting foreign powers must be "knowing" in order to render a U.S. person an agent of a foreign power, [83] and that a person could not receive this designation "solely upon the basis of activities protected by the first amendment to the Constitution of the United States."[84]

2. Foreign Intelligence Purpose

A second key limitation on the government's ability to obtain a FISA surveillance order was the requirement that it demonstrate that the purpose of the surveillance was to obtain "foreign intelligence information."

Senators were concerned that the definition of "foreign intelligence information" in an early draft of the bill was too broad because it went beyond national security to include information on "the conduct of the foreign affairs of the United States." One Senator wrote to the Chair of the Intelligence Committee, pointing out that the views of members of Congress could "easily be classified as information 'essential to the conduct of the foreign affairs of the United States,'"[85] suggesting that Congress itself could be surveilled under FISA.

To address such misgivings (and over the objections of the Department of Defense and other agencies),[86] the final version of FISA required that, where the government sought information "concerning a United States person," it must show that the information was not just relevant but "necessary" for the conduct of foreign affairs.[87] The accompanying House Report indicated that the use of this term precluded the executive's ability to seek a FISA order based on what is often known as the "mosaic theory":

> [I]t is often contended that a counterintelligence officer or intelligence analyst, if not the policymaker himself, must have every possible bit of information about a subject because it might provide an important piece of the larger picture. In that sense, any information relating to the specified purposes might be called 'necessary' *but such a reading is clearly not intended*.[88]

For non-Americans, however, FISA still allowed the collection of information that "relates to . . . the national defense or the security of the United States," as well as information that relates to the conduct of foreign affairs.[89]

Comparing Title III Warrants with FISA Orders

Under the statutory scheme designed by Congress in 1978, orders issued by the FISA Court share a critical feature with regular Title III warrants: both require prior judicial scrutiny of an application for an order authorizing electronic surveillance in a particular case.[90] This is not to say, however, that FISA orders are equivalent to warrants issued by regular federal courts.

Title III allows a court to enter an *ex parte* order authorizing electronic surveillance if it determines, on the basis of the facts submitted in the government's application, that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" a specified predicate offense.[91] By contrast, FISA's highest standard, which is reserved for the targeting of U.S. persons, requires a showing of probable cause that the target's activities "involve or may involve" a violation of U.S. criminal law.[92] While Congress intended for this standard to approach the threshold for criminal warrants (as discussed above),[93] the absolute secrecy surrounding the FISA procedure precludes a full understanding of how this standard operates in practice. For example, documents leaked by Edward Snowden revealed that the government had obtained FISA orders targeting prominent Muslim American community leaders with no apparent connection to criminal activity.[94]

Traditional FISA orders also require much less proof that the surveillance activities will yield the information sought. Under Title III, the government must demonstrate probable cause to believe that particular communications concerning specified crimes will be obtained through an interception.[95] Under FISA, the government instead must show probable cause that the facilities at which the surveillance is directed are used by a foreign power or its agent; it need not show probable cause that collecting on these facilities will yield the desired information.[96] A high-level government official must certify that the information sought is foreign intelligence information and designate the type of information being sought. However, the court reviews the substance of this certification only when the target is a U.S. person, and even then, the court's review is limited to determining whether the certificate is "clearly erroneous." [97] As the legislative history of the statute itself acknowledges, this "standard of review is not, of course, comparable to a probable cause finding by the judge."[98]

Like warrant applications under Title III, FISA applications are generally heard on an *ex parte* basis. However, unlike individuals monitored under Title III, those whose communications are intercepted under FISA are highly unlikely to receive notice of the intrusion. Title III requires notice to the target (and, within the discretion of the judge, to other persons whose communications were intercepted) once the surveillance order expires.[99] FISA does not require notice unless the government "intends to enter into evidence or otherwise use or disclose" such communications in a trial or other legal proceedings.[100] Moreover, recent reports suggest that the government has taken a very narrow view of when and how this notice requirement applies.[101]

III. THE BRAVE NEW WORLD OF FOREIGN INTELLIGENCE SURVEILLANCE

It is no exaggeration to say that the world of electronic surveillance looks entirely different today than it did in 1978 when the FISA Court was established to oversee foreign intelligence surveillance. Communications technology and the legal framework have fundamentally changed, vastly increasing the nature and quantity of information the government may collect — and decreasing the court's role in supervising these operations.

Although the Supreme Court in *Keith* attempted to distinguish between surveillance of domestic organizations and surveillance of foreign powers, the demarcation was never clean and has become ever more strained. Advances in technology mean that the exercise of authorities aimed at foreigners abroad inevitably picks up swaths of information about Americans who should enjoy constitutional protections. But rather than develop additional safeguards for this information, the law has developed in the opposite direction: the government's authority to collect communications pursuant to its foreign intelligence-gathering authorities has expanded significantly. At the same time, the safeguard of judicial review — already limited when FISA was first enacted in 1978 — has eroded to near-nothingness. Indeed, in some cases, the role played by the FISA Court is so different from the normal function of a court that it likely violates the Constitution's separation of powers among the legislative, executive, and judicial branches.

A. A Revolution in Communications Technology

The impact of advances in communications technology over the last decades cannot be overstated. In 1978, most domestic telephone calls were carried over copper wires,[102] while most international calls took place via satellite.[103] To listen to a domestic call, the government had to identify the wire that geographically connected the two ends of a communication and manually tap into it.[104] Capturing a satellite communication to or from a particular source required sophisticated equipment; resulting databases were subject to practical limitations on storage and analytical capability.[105] Cellular phones were not commercially available,[106] and the Internet existed only as a Department of Defense prototype.[107] Surveillance generally had to occur in real time, as electronic communications were ephemeral and unlike later forms of communication (like e-mail) were not usually stored.

Today, a large proportion of communications — including e-mails and international phone calls — are transmitted by breaking down information into digital packets and sending them via a worldwide network of fiber-optic cables and interconnected computers.[108] The government can access these communications by tapping directly into the cables or into the stations where packets of data are sorted.[109] Digital information often is stored for long periods of time on servers that are owned by private third parties, giving the government another way to obtain information, as well as access to a trove of historical data. Most cell phone calls, along with other forms of wireless communication, travel by radio signals that are easily intercepted.

These changes have weakened the relationship between the place where communications are intercepted and the location (and nationality) of the communicants. For communications that travel wholly or

in part via packets, each packet may follow a different route, and the route may be unrelated to the locations of the sender or recipient. An e-mail from a mother located in San Diego to her daughter in New York could travel through Paris, and the contents might be stored by an online service provider in Japan. But FISA, as enacted in 1978, is keyed to the location and nationality of the target and the location of acquisition. As discussed further in Part II.B.3.a, the globalization of the communications infrastructure has changed the way the law plays out in practice.[110]

Technological changes also have expanded the amount of information about Americans the government can acquire under FISA. For one thing, globalization and advances in communications technology have vastly increased the volume — and changed the nature — of international communications.

The cost and technological difficulties associated with placing international calls during the era of FISA's passage meant that such calls were relatively rare. In 1980, the average American spent less than 13 minutes a year on international calls.[111] Today, the number is closer to four and a half hours per person — a thirty-fold increase.[112] That number does not include the many hours of Skype, FaceTime, and other Internet-based voice and video communications logged by Americans communicating with family, friends, or business associates overseas. And, of course, the advent of e-mail has removed any barriers to international communication that may have remained in the telephone context, such as multi-hour time differences. Worldwide e-mail traffic has reached staggering levels: in 2013, more than 182.9 billion e-mails were sent or received *daily*.[113] As international communication has become easier and less costly, the content of communications is much more likely to encompass — and, in combination, to create a wide-ranging picture of — the intimate details of communicants' day-to-day lives.

Technology and globalization also have led to much greater mobility, which in turn has generated a greater need to communicate internationally. Foreign-born individuals comprised around 6 percent of the U.S. population when FISA was enacted but account for more than 13 percent today.[114] Immigrants often have family members and friends in their countries of origin with whom they continue to communicate. Similarly, there has been a sharp increase in Americans living, working, or traveling abroad, creating professional or personal ties that generate ongoing communication with non-citizens overseas. The number of Americans who live abroad is nearly four times higher than it was in 1978 and the number of Americans who travel abroad annually is nearly three times higher.[115] The number of American students who study abroad each year has more than tripled in the past two decades alone.[116] These trends show no signs of abating, suggesting that the volume of international communications will only continue to expand.

In addition, technological changes have made it likely that government attempts to acquire international communications will pull in significant numbers of wholly domestic communications for which Congress intended the government to obtain a regular warrant rather than proceeding under FISA. For instance, a recently declassified FISA Court decision shows that when the NSA taps into fiber-optic cables, it pulls in some bundles of data that include multiple communications — including communications that may not involve the target of surveillance. The NSA claims that it is "generally incapable" of identifying and filtering out such data bundles.[117] The result is that the agency routinely collects large numbers of communications — including "tens of thousands of wholly domestic communications" between U.S. persons — that are neither to, from, or about the actual "target."[118]

For all of these reasons, the collection of foreign intelligence surveillance today involves Americans' communications at a volume and sensitivity level Congress never imagined when it enacted FISA. If the government wished to acquire the communications of a non-citizen overseas in 1978, any collection of exchanges involving Americans could plausibly be described as "incidental." Today, with international communication being a daily fact of life for large numbers of Americans, the collection of their calls and e-mails in vast numbers is an inevitable consequence of surveillance directed at a non-citizen overseas. The volume of information collected on U.S. persons makes it difficult to characterize existing foreign intelligence programs as focused solely on foreigners and thus exempt from ordinary Fourth Amendment constraints.

B. Post-9/11: Move from Individualized to Mass Surveillance

1. Bulk Collection of Business Records

In the immediate aftermath of 9/11, Congress passed the Patriot Act to expand the tools available to the government to combat terrorism.[119] The bill was enacted as an emergency-response measure, with far less debate than such significant changes in the law usually would occasion.[120] One important provision expanded the government's ability to obtain business records from third parties for foreign intelligence purposes. While on its face, this change seemed to require the FISA Court to issue the same type of individualized court orders that it had previously done (albeit under a far more lax standard), the court secretly interpreted the law to authorize a dragnet surveillance program.

Prior to 2001, the FBI could obtain an order from the FISA Court to require third parties to turn over the business records of transport companies, hotels and motels, car and truck rental agencies, and storage rental facilities. To do so, the government had to certify that the records were sought for a foreign intelligence or international terrorism investigation being conducted by the FBI. Further, it had to present "specific and articulable facts giving reason to believe" that the subject of the records was a foreign power or agent of a foreign power.[121]

Section 215 of the Patriot Act greatly expanded this authority. It removed the limitation on the types of records the government could obtain, granting authority to obtain "any tangible thing." Connection to a foreign power or its agent was no longer required. The government need only provide a statement of facts showing that "there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities."[122]

Although this change allowed the government to obtain more material with a lesser showing, it at least appeared to preserve the safeguard of prior judicial approval on a case-by-case basis. In 2013, however, Edward Snowden's first and most dramatic disclosure revealed that the FISA Court had issued orders under Section 215 allowing the NSA to collect Americans' telephone records in bulk.[123] The records in question, known as "metadata," included the numbers dialed, the numbers of those who called, and the times and lengths of calls — information that could be used to create a detailed picture of a person's associations and activities (as discussed further below).

The so-called "bulk collection" program was not itself news. *USA Today* had uncovered it in 2006, a year after *The New York Times* revealed the NSA's warrantless surveillance of phone calls and e-mails.[124] At that time, however, both programs operated outside the FISA framework, and the Bush administration had made no attempt to secure the FISA Court's permission for them. Snowden's disclosures not only confirmed the continuing existence of the bulk collection program; it revealed that the administration, concerned about continuing its now public surveillance activities without statutory cover, had enlisted the FISA Court's help to operate this program under FISA.

The FISA Court's decision in 2006 to allow mass collection of this data was based on an expansive new interpretation of the concept of "relevance." This interpretation made its first appearance in 2004, when the court approved the NSA's bulk collection of Internet metadata under a different statutory provision that also requires relevance.[125] Although the Internet metadata program, like the phone records and warrantless wiretapping programs, originally operated outside the FISA framework, the issue ultimately came before the FISA Court because Justice Department officials believed statutory authorization was necessary.[126] The FISA Court approved the Internet metadata program (which was discontinued in 2011 for operational reasons, according to administration officials[127]) and two years later relied on a similar logic to approve the bulk collection of phone records under Section 215. The Court did not issue a written opinion on the phone records program, however, until 2013.[128]

In its 2013 decision, the FISA Court ruled that all Americans' phone records were relevant to authorized international terrorism investigations. It conceded that the vast majority of Americans have no link to international terrorism. However, it noted the obvious fact that "information concerning known and unknown affiliates of international terrorist organizations was contained within the non-content metadata the government sought to obtain."[129] It also accepted the government's argument that "it is necessary to obtain the bulk collection [sic] of a telephone company's metadata to determine . . . connections between known and unknown international terrorist operatives."[130] It concluded, in short, that because collecting irrelevant data was necessary to identify relevant data, the irrelevant data could thereby be deemed relevant.

The court prohibited the NSA from looking at any of the phone records it collected unless those records were pulled using search terms (generally telephone numbers) that met a higher bar. Specifically, the NSA must have a reasonable articulable suspicion, or "RAS," that the search term was associated with an international terrorist organization.[131] The FISA Court, however, disclaimed any role in the RAS determination, leaving that assessment to the NSA. Section 215 thus became a form of programmatic collection, with the court approving standards for searches but not the searches themselves. In early 2014, based on a policy decision by the Obama administration, the Justice Department asked the FISA Court to revise the court-issued procedures for the bulk collection program to include court review of RAS determinations.[132] However, the court's previous interpretation of "relevance" stands, which means that Section 215 may be used for programmatic collection in the future (or perhaps even currently under other, as-yet undisclosed programs).

2. Demise of the "Primary Purpose" Test

Another critical change made by the Patriot Act was accomplished by revising two words. Previously, FISA allowed the government to obtain surveillance orders if it certified that "the purpose" of surveillance was the acquisition of foreign intelligence. Under the Patriot Act, however, the government need only certify that acquiring foreign intelligence is "a significant purpose" of the surveillance.[133] In addition, the Patriot Act provided that federal officers who conduct electronic surveillance to acquire foreign intelligence information "may consult with" law enforcement officials to protect against attack or other hostile acts by foreign powers or their agents.[134]

A complex history underlies these deceptively simple changes. As discussed in Part II.A.3, the courts that recognized a foreign intelligence exception to the warrant requirement generally held that collecting foreign intelligence must be the "primary purpose" of surveillance. This condition served to ensure that foreign intelligence wasn't used as a pretext for warrantless searches in domestic criminal cases.

Discerning which motive predominates in any mixed-motive case, however, is a difficult endeavor. If the NSA or FBI wiretaps someone to obtain foreign intelligence, and the Justice Department simultaneously wishes to preserve the option of a criminal prosecution against that person, which is the "primary" purpose? In *United States v. Truong*, the Fourth Circuit looked to the role that criminal prosecutors played in the foreign intelligence investigation. If it appeared that the prosecutors were excessively involved in the foreign intelligence surveillance, the court reasoned, one could conclude that the primary purpose of the surveillance was law enforcement.[135]

Following this decision, the Justice Department voluntarily adopted a set of practices designed to facilitate the sharing of information between intelligence and law enforcement components, while avoiding any appearance that prosecutors were directing the intelligence investigations. A version of these practices ultimately was formalized in a series of memoranda and procedures issued between 1995 and 2001.[136]

The procedures, taken together, encouraged consultation between prosecutors and intelligence officials in a variety of ways — for example, by requiring intelligence investigators to report indications of significant federal crimes to the Justice Department, and by requiring senior intelligence officials to provide monthly briefings to officials overseeing criminal matters.[137] At the same time, the procedures included provisions to ensure that the Criminal Division of the Justice Department would not deploy FISA surveillance as a tool to gather evidence for criminal prosecutions, thus making an end run around the traditional Fourth Amendment warrant requirement. While the Criminal Division could provide advice on intelligence investigations, it could not "direct[] or control[]" them, and it could not "instruct the FBI on the operation, continuation, or expansion of FISA electronic surveillance or physical searches."[138] Moreover, intelligence investigators needed approval from FBI headquarters and another Justice Department component to share certain portions of their investigative memoranda with law enforcement.[139]

In its first published opinion, the FISA Court in 2002 described these procedures as permitting "broad information sharing," as well as "substantial consultation and coordination."[140] Nonetheless, there was a strong perception within the government that the procedures erected a "wall" between intelligence and law enforcement that inhibited robust cooperation. This impression was echoed in the findings of a May 2000 report by the Attorney General's Review Team[141] and a July 2001 report by the General Accounting Office.[142] After 9/11, the "wall" was blamed for impeding cooperation that conceivably could have averted the attacks, and it was dismantled.[143]

To discourage any limits on coordination, Congress amended FISA to expressly permit consultation between intelligence and law enforcement officials, and to provide that foreign intelligence acquisition need only be a "significant" purpose of surveillance.[144] As a result, when obtaining a traditional FISA order, even if the primary purpose of surveillance is to build a prosecution against an American citizen, the government is empowered to collect that person's communications without making the probable cause showing required in criminal cases as long as collection of foreign intelligence is a secondary aim.

Did "The Wall" Cause 9/11?

The hypothesis that the "primary purpose" test required the establishment of a "wall" which then led to 9/11 is flawed in a number of respects. Most fundamentally, the 9/11 Commission's report showed that the "wall" did not cause the lack of coordination that contributed to intelligence failures before 9/11. It documented that CIA investigators, as well as FBI officials detailed to the CIA, had information months before the attack that two of the hijackers were potential terrorists already in the United States. There were many opportunities to share this information more broadly, and most of these opportunities were squandered because of poor judgment calls by individual analysts.[145]

Moreover, the hypothesis oversimplifies the relationship between the "primary purpose" test and "the wall." While courts signaled that they would look askance if criminal prosecutors were directing foreign intelligence surveillance, no court held that the "primary purpose" test necessitated the particular limitations that the Justice Department imposed on itself.[146] Nor is it clear that chilling coordination was the direct and inevitable result of implementing those limitations. According to the Attorney General's Review Team, the voluntary restraints that were in place between 1984 and 1993 "appear[] to have worked quite satisfactorily . . . both from the perspective of the Criminal Division and that of the FBI."[147] At least some of the impediments to coordination that subsequently emerged appear to have been a result of officials' conservative interpretation of the rules, rather than the rules themselves.[148]

3. The FISA Amendments Act

Background

Although the next major set of statutory changes took place six years after the Patriot Act, they, too, had their origins in surveillance activities that began in the immediate aftermath of 9/11. At that time, the Bush administration began intercepting communications to and from Americans without seeking any type of judicial approval. After *The New York Times* reported on these operations in 2005, President George W. Bush admitted to one aspect of the warrantless surveillance: the so-called "Terrorist Surveillance Program" (TSP), which involved the acquisition of communications between Americans in the United States and suspected members of Al Qaeda and related terrorist organizations abroad.[149]

Despite violating FISA, the government initially took the view that its actions under the TSP (and presumably other programs like it[150]) were legal on the ground that Article II of the Constitution granted the president authority to conduct surveillance in order to protect the nation.[151] Faced with public and congressional criticism, it switched gears and sought to enshrine its warrantless surveillance within the FISA paradigm. Ultimately, this would require amending the statute.[152]

In pressing for changes to FISA, the executive branch made two primary arguments, both of which rested on the premise that changes in technology had subverted the intent behind FISA. First, officials claimed that when FISA was passed in 1978, the vast majority of international communications between Americans and foreigners overseas were transmitted by satellite rather than by wire. Because the statute's definition of "electronic surveillance" does not include the acquisition of international satellite communications, officials argued, Congress did not intend to regulate the collection of international communications at all. Subsequent advances in fiber-optic technology, however, led to the majority of international communications being carried by wire, which in turn brought those communications within FISA's regulatory structure (at least in cases where acquisition took place inside the United States) — thus undercutting Congress's original intent.[153]

This argument is unconvincing. Even when Congress passed FISA, one-third to one-half of international communications were carried by wire.[154] Congress could have chosen to exempt these from FISA's reach, but did not, suggesting that it intended to regulate at least some international communications.

Furthermore, the legislative history shows that Congress intended to address international satellite communications at a later date and that the Attorney General had pledged to assist in that effort.[155] Although these efforts ultimately went nowhere, Congress made clear that the gaps in FISA's coverage of NSA's operations "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans."[156] Accordingly, the government's suggestion that Congress endorsed the government's acquisition of international communications outside the FISA scheme is unsupported by the record.

The executive branch's second argument for increasing its authority was that certain purely foreign-to-foreign communications, which Congress never intended to regulate, now travel through the United States in ways that bring them within FISA's scope.[157] In practice, this appears to be a fairly discrete (albeit thorny) problem that applies to one category of communication: e-mails between foreigners

that are stored on U.S. servers.[158] It is certainly possible that Congress would have wished to exclude such e-mails from FISA's scope if presented with that issue in 1978. Of course, it also seems likely that Congress would have wished to *include* e-mail exchanges between Americans that are stored on overseas servers, yet the executive branch did not even raise this issue, let alone seek remedial legislation. In any event, the solution that the Bush administration sought in 2007 was far broader than necessary to address the problem it identified. Rather than seek a solution specific to stored e-mails,[159] the administration sought and obtained the much broader expansions of surveillance authority discussed below.

The Statute

In response to the administration's push, Congress passed two statutes amending FISA: the Protect America Act (PAA) of 2007,[160] which expired the following year, and the FISA Amendments Act (FAA),[161] which replaced it. While the FAA walked back a handful of the PAA's most significant changes, the two statutes were fundamentally similar in that they both authorized a regime of "programmatic surveillance."

The FAA, which is still in place today, eliminated the requirement of an individual court order for acquisition, within the United States, of communications to which U.S. persons are a party. Instead, under a new section of FISA (Section 702) created by the FAA, the government may conduct a program to collect any communications "targeting" a person or entity reasonably believed to be a non-U.S. person overseas — including that person or entity's communications with Americans in the United States.[162] In other words, the government no longer needs an individualized court order to acquire Americans' international calls and e-mails, as long as the American is not the "target" of the surveillance.

There are three primary limitations on this authority. First, the government must certify that obtaining foreign intelligence information is a "significant purpose" of the collection. It need not be the only purpose or even the main purpose, as discussed above;[163] moreover, the certification of purpose applies to the program as a whole, not to each target of surveillance under the program. Second, the government must have in place targeting and minimization procedures that are approved by the FISA Court. The targeting procedures must ensure that the program's targets are indeed "reasonably believed" to be foreigners overseas, while the minimization procedures must be "reasonably designed" to minimize the collection and retention — and prohibit the sharing — of Americans' information, "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[164] Third, the law prohibits the government from engaging in "reverse targeting" — i.e., collecting the international communications of a foreigner abroad when the government's true motive is to target "a particular, known person reasonably believed to be in the United States."[165]

The existence of targeting and minimization requirements, as well as a reverse targeting prohibition, has enabled the government to portray Section 702 as a program designed to capture the communications of non-U.S. persons abroad. Any collection of calls to or from Americans is described as "incidental."[166] This characterization is highly questionable. With the exception of e-mails stored in the United States, the new law had no impact on the government's ability to collect the communications of foreigners with other foreigners. The sea change that the statute brought about was the elimination of a court order requirement for the domestic capture of foreigners' communications with Americans. The legislative history makes clear that facilitating the capture of communications to, from, or about U.S. persons was a primary purpose, if not the primary purpose, of the FAA.[167]

Section 702 and Surveillance of Americans

The administration routinely asserts that Section 702 of FISA targets only foreigners overseas.[168] These statements create a false impression that only foreigners' communications are sought or acquired. In fact, anyone who talks to or about a target is subject to surveillance.

The NSA has refused to provide any estimate of how many Americans' communications are acquired under Section 702, claiming that providing such an estimate would itself violate Americans' privacy.[169] However, a declassified 2011 opinion of the FISA Court notes that 250 million internet communications were acquired the previous year under Section 702.[170] If only ten percent of these communications involved U.S. persons, that would still add up to the collection of 25 million internet communications involving Americans for a single year.[171] This number would not include wholly domestic communications swept up in the net, which happens tens of thousands of times a year, according to the same decision.[172]

Moreover, the new law dramatically widened the pool of foreigners the government can target. Instead of being limited to targeting foreign powers or agents of a foreign power, the government is permitted to target any non-U.S. person overseas, as long as one of its goals is the acquisition of foreign intelligence. As noted above, the statute's definition of "foreign intelligence information" is exceedingly broad when a foreign person is the target, encompassing any information that "relates to" the conduct of foreign affairs or the country's security.[173] Programmatic surveillance under the FAA thus could include the international communications (including communications with Americans) of almost any non-U.S. person overseas. Of course, the greater the number of foreigners who can be targeted, the greater the number of Americans whose international communications are likely to be caught up in surveillance operations.

The court's own role in approving government surveillance changed even more fundamentally. Previously, the court determined, on a case-by-case basis, whether the government had probable cause to believe that (1) the proposed target of surveillance was a foreign power or agent of a foreign power, and (2) each of the specified facilities or places for surveillance were being used, or were about to be used, by a foreign power or an agent of a foreign power. The court also approved minimization requirements based on their sufficiency in the particular case before it. If the target was a U.S. person, the court reviewed the government's certifications — including the certification of a significant foreign intelligence purpose — to ensure that they were not "clearly erroneous."

Under Section 702, by contrast, the 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 (which gives little direction as to what is required) and with the Fourth Amendment.[174] The court is not even informed of the specific targets of surveillance or the facilities to be surveilled, let alone asked to approve them. And the court may not review the substance of the government's certifications, including its certification of a significant foreign intelligence purpose, even for "clear error."[175]

Executive Order 12333

This report focuses on FISA and the FISA Court, which regulate and oversee surveillance that takes place within the United States. Collection on foreign targets that takes place abroad generally is conducted under Executive Order 12333, which allows collection without judicial oversight and imposes even fewer limits than Section 702.[176]

At first blush, the government's longstanding ability to engage in the warrantless collection of international communications from overseas might appear to undermine the claim that Section 702 greatly expanded the government's ability to acquire such collections. However, the very fact that the executive branch pushed so hard to enact Section 702 suggests that overseas acquisition either was impossible or was deemed too costly in many cases. It is easy to imagine how that might be the case when, for instance, targets live in countries with unfriendly governments.

Moreover, the fact that the government collects information overseas under Executive Order 12333 — including, ostensibly, the "incidental" collection and retention of Americans' communications with overseas targets on an even greater scale than under Section 702[177] — does not establish the legality of the practice. Even if foreigners overseas lack Fourth Amendment protections, it is far from clear that a foreign target's communications with U.S. persons are exempt from constitutional safeguards. Because surveillance under Executive Order 12333 does not involve judicial review, courts have not had occasion to rule on whether the surveillance it authorizes is constitutional when a U.S. person's communications are involved.

IV. CONSTITUTIONAL CONCERNS

The technological and legal changes described above have fundamentally altered the role of the FISA Court, throwing the constitutionality of FISA's entire judicial oversight scheme into question. The court's move from adjudicating applications for surveillance in individual cases to approving broad programs based on vague standards arguably runs afoul of Article III of the Constitution, which limits courts to deciding concrete disputes that they are capable of resolving. At the same time, the current law's standards for court oversight of surveillance fail to pass muster under the Fourth Amendment.

A. Article III Concerns

The FISA Court's original role was to assess the sufficiency of the government's factual showing in individual cases. The court had to find probable cause that the target of the proposed electronic surveillance was a foreign power or agent of a foreign power, and that a foreign power or its agent was using the telephone or other facility to be intercepted.

While the standard applied by the court was not a particularly high bar — and falls short of what is required for a normal criminal warrant — the original law focused the court's analysis and limited the pool of cases the government could bring before the court. The pool was further cabined by the technological limitations on, and relatively low demand for, international communications.

Today, under Section 702 of the FAA, the court is no longer tasked with assessing the sufficiency of the government's factual showing in individual cases that arise within a limited pool. Instead, it reviews broad targeting and minimization procedures that the government will apply to tens of thousands of cases involving hundreds of millions of communications, if not more, each year.[178] The court then approves or rejects the procedures based on a facial analysis of whether they comport with the statute and the Fourth Amendment. Similarly, under Section 215, the FISA Court has endorsed a form of "programmatic surveillance" in which it may approve procedures for obtaining and searching telephone records without reviewing individual searches (although it currently reviews these searches pursuant to the administration's request).[179]

These developments, compounded by the secrecy and lack of adversarial process that mark the court's proceedings, have critical implications for the constitutional legitimacy of the court. Lack of adversary process in a proceeding that bears no relationship to a traditional warrant application is inconsistent with Article III. Moreover, the court's facial review of agency procedures cannot shed light on their constitutionality in specific cases.

1. Lack of Adversarial Process

Article III of the Constitution generally requires the presence in court of opposing parties, because its "case or controversy" requirement "confines the business of federal courts to questions presented in an adversary context."[180] Warrant proceedings are an exception to this rule. The FISA Court's shift from issuing individualized, warrant-like orders to approving programmatic surveillance renders the lack of an opposing party in its proceedings, which was a "difficult question" for the Department of Justice even under the original 1978 FISA procedure,[181] impossible to defend — and highly problematic.

As discussed, at the time FISA was passed, the Justice Department sought to address concerns about the lack of an opposing party in FISA Court proceedings. Even though the procedure for obtaining a surveillance order did not involve adverse parties, the Justice Department argued that there was "adversity in fact" because "the interests of the United States and the target will inevitably be adverse to each other. The United States' interest is to institute electronic surveillance of a particular target. The interest of the target would, presumably, be that the surveillance not be conducted."[182] The Department emphasized the similarity of these features to traditional warrant proceedings, and concluded: "It is obvious . . . that we rely heavily on the analogy to warrant proceedings to uphold the validity of the [FISA] proceeding."[183]

Under Section 702, that analogy disappears. There is no such thing as a criminal warrant proceeding in which a law enforcement agency seeks blanket authorization to conduct an unlimited number of searches over the coming year, on the basis of written procedures setting forth generic rules for how such searches will be conducted. While *ex parte* proceedings are a standard feature in warrant applications, they are not standard when courts review rules and procedures that affect millions of people. As stated by Judge James Robertson, who served on the FISA Court from 2002 to 2005, the FISA Court's role in programmatic surveillance "is not adjudication, it is approval."[184] The approval process, he noted, "works just fine when [the court] deals with individual applications for surveillance warrants," but when courts are asked to review policy determinations for compliance with the law, "they do so in the context . . . of adversary process."[185] By requiring the FISA Court to review and approve entire surveillance programs *ex parte*, the FAA "turned the FISA Court into something like an administrative agency which makes and approves rules for others to follow."[186]

Section 215, at first blush, appears much closer to the kind of warrant proceeding that has traditionally taken place with only one party present because it seems to preserve individualized review in which particular opposing interests are identifiable. But this apparent similarity is negated by the FISA Court's decision that the government may collect essentially all phone records to search for relevant records buried within them.[187] This program, too, now involves judicial approval, without any adversarial process, of the broad contours of a program affecting much of the American population — a situation that cannot be squared with the requirements of Article III.[188]

In addition to being constitutionally suspect, secret, non-adversarial proceedings are a bad way to make law. The shortcomings are starkly illustrated by the FISA Court's approval of bulk collection. The question the court considered in 2006 — whether collecting the phone records of millions of admittedly innocent Americans comports with the Constitution and the Patriot Act — was one of first impression and overriding legal importance. Yet all of the evidence and all of the briefs were submitted by one party: the government. Despite the gravity of the issue, the FISA Court did not exercise its authority to solicit participation by *amici curiae* — knowledgeable outside parties who serve as "friends of the court." Instead, it granted the government's request without even a written opinion (although one was produced after Edward Snowden's disclosures in 2013).[189]

The adversarial system does more than assure the due process rights of the parties. It ensures that all relevant facts and legal arguments are aired, which in turn enables the tribunal to reach an accurate decision. FISA Court judges are more likely to misinterpret the law if they hear only one side of the case. As the Supreme Court stated in a different context:

> [T]he need for adversary inquiry is increased by the complexity of the issues presented for adjudication. . . . Adversary proceedings will not magically eliminate all error, but they will substantially reduce its incidence by guarding against the possibility that the trial judge, through lack of time or unfamiliarity with the information contained in and suggested by the materials, will be unable to provide the scrutiny which the Fourth Amendment exclusionary rule demands.[190]

Of course, it is well understood that judges make mistakes; that is why the federal judicial system has two levels of appeal. Indeed, the Supreme Court often waits for multiple lower courts to address an issue before taking it up. This process of assessing, comparing, and honing decisions across jurisdictions and levels of review make it more likely that the judicial system as a whole will get to the "right" result. In the FISA context, however, there is no opportunity to appeal an erroneous grant of an application, because the government is generally the only party.

Operating in their own echo chamber, and hearing from only one party, the chances that FISA Court judges will misinterpret the law — and perpetuate that misinterpretation in subsequent decisions — is high. When such misinterpretations involve fundamental questions of constitutional law that affect all Americans, the error is anything but harmless.

2. Absence of a "Case or Controversy"

FISA Court judges approve the NSA's procedures in a vacuum, divorced from any specific application of them. This may run afoul of Article III's "case or controversy" requirement, which generally requires courts to review legal questions in the context of specific facts rather than in the abstract.[191]

The "case or controversy" requirement ensures that there is an actual dispute which is capable of being resolved by the court. It guards against courts simply providing advice to the other branches of government, an activity that would go beyond their assigned role and intrude on the other branches' prerogatives. Challenges to a law's constitutionality based on future applications of the law, involving as-yet unknown facts, are subject to dismissal because they do not establish the required "case or controversy."[192]

In its 1978 form, FISA required the court to apply law to specific, alleged facts. As the Justice Department explained at the time, the court would be deciding a "case or controversy" because "what is to be determined is the United States' authority to conduct electronic surveillance of a particular target," and "[t]he judge is required under the bill to apply standards of law to the facts of a particular case."[193] These conditions no longer apply. Instead, Congress has charged the FISA Court with determining whether general procedures, divorced from any facts about how they are applied in actual cases, "are consistent with . . . the fourth amendment."[194] The court has no information about who will be targeted, the factual circumstances that support the government's determination that the target fits the statutory

targeting criteria, the particular information to be obtained, the collection method to be applied and its impact on non-targets, or how the government will implement minimization protocols — all factors that are relevant to the constitutionality of electronic surveillance under the Fourth Amendment.

An exception to the general rule that courts adjudicate specific applications of the law is facial challenges, in which a plaintiff seeks to strike down a law in its entirety without reference to any specific application. Section 702 in theory could be viewed as asking the FISA Court to rule on a facial challenge brought by an imaginary litigant. But using such a review to establish the constitutionality of the targeting and minimization procedures raises its own set of problems.

The Supreme Court has noted that, "[a]lthough passing on the validity of a law wholesale may be efficient in the abstract, any gain is often offset by losing the lessons taught by the particular, to which common law method normally looks."[195] The Court accordingly has deemed facial challenges appropriate only where no conceivable application of the statute could pass constitutional muster.[196] In other words, the statute will stand if there is even one set of circumstances in which its application would comport with the Constitution.

Critically, however, surviving such a contest does not mean that the law's constitutionality has been established for all time and all circumstances. Rather, the door remains open to future challenges based on how the law is actually applied (called "as-applied" challenges).[197] The statute, in essence, lives to fight another day, at which time "the lessons taught by the particular" may be brought to bear. For instance, courts have upheld government programs involving warrantless searches — such as fixed sobriety checkpoints — under the so-called "special needs" doctrine (discussed at Part IV.B.1). In doing so, they have examined the procedures attending such programs to ensure that they meet the reasonableness standard of the Fourth Amendment. Yet, even where this analysis has appeared to yield judicial approval of entire programs, the courts have explicitly left open the possibility of later challenges based on the facts of a particular search.[198]

What Exactly is the FISA Court Approving Under Section 702?

The question of whether any and all applications of the NSA's procedures would be constitutional is not "capable of resolution through the judicial process" because FISA Court judges simply don't know the specific activities that the procedures may authorize in any given case.[200] An excerpt from the 2009 targeting procedures, which were blessed by the court, makes this clear:

> NSA determines whether a person is a non-United States person reasonably believed to be outside the United States in light of *the totality of the circumstances* based on the information available with respect to that person, including information concerning the facility or facilities used by that person.
>
> NSA analysts examine . . . three categories of information, *as appropriate under the circumstances*, to make the above determination . . . NSA *may* use information from any one or a combination of these categories of information in evaluating the totality of the circumstances to determine that the potential target is located outside the United States.
>
> The following are *examples* of the *types* of lead information that NSA *may* examine: . . . .[201]

When reviewing these vague and indeterminate procedures, the most the court can do — and the most any court does when it conducts a facial review — is hold that the procedures could be applied constitutionally in at least one imaginable set of circumstances.

Accordingly, even if the FISA Court may decide that Section 702 procedures are *un*constitutional on their face, it could not, consistent with Article III, proclaim that they are constitutional in all of their future applications. That legal question can be resolved only through as-applied challenges in which the relevant facts are put before the court. In the FISA context, however, an as-applied challenge to surveillance is usually impossible because notice of the surveillance is not provided to the target. Indeed, it seems likely that Congress's very purpose in requiring FISA Court approval of targeting and minimization procedures was to *substitute for* as-applied challenges.[199]

Congress's solution does not satisfy Article III. A determination that agency procedures *could* be applied constitutionally is very different from a determination that they are constitutional in every possible application. To the extent Congress was attempting to use FISA Court review of NSA procedures as approval for all activities taken under them, even though the specific activities are not before the court, any such effort would be invalid under Article III's "case or controversy" requirement.

The Barriers to FISA Challenges

In theory, there are three ways in which surveillance of particular targets may be challenged in an adversary setting: targets may file civil claims; they may contest the surveillance in the course of legal proceedings; and communications service providers who receive FISA orders may petition the FISA Court to set them aside. In practice, however, none of these options provides a meaningful opportunity to challenge surveillance.

The lack of notice to targets of FISA surveillance effectively negates any civil remedies, including FISA's provision allowing "aggrieved person[s] . . . who [have] been subjected to an electronic surveillance" to sue for damages if the law has been violated.[202] Plaintiffs who have attempted to file civil suits have been rebuffed by courts on the ground that they cannot establish standing without proving that they were targets of surveillance.[203]

If FISA-derived evidence is used in a criminal prosecution or other legal proceeding against a subject of surveillance, the law requires the government to notify that person of this fact and allows him to file a motion to suppress the evidence.[204] However, the vast majority of foreign intelligence collected under FISA will never find its way into a legal proceeding.[205] Moreover, in recent years the government has honored the notification requirement in the breach,[206] sometimes using "parallel construction" — that is, developing the same evidence through different means to avoid notification.[207]

Even when notification is provided, the subject of surveillance has never been permitted to view the materials comprising the surveillance application, which renders any challenge an exercise in shadow-boxing.[208] Without the informed participation of counsel, judicial review in these proceedings is in many ways a mere repetition of the *ex parte* review conducted by the FISA Court when it issued the surveillance order — even though the initiation of legal proceedings often means the consequences of error have become far greater, particularly in criminal cases where the defendant's liberty is at stake.

In 2006 and 2008, Congress amended FISA to allow telecommunications companies that are the recipients of certain FISA orders to challenge them.[209] But these companies have no obligation to act in the interest of those directly affected by the surveillance, namely, the targets. The insufficiency of this mechanism is underscored by the fact that no company has ever challenged a court order to produce phone records under the NSA's bulk collection program,[210] and only one company challenged programmatic surveillance under the predecessor to the FAA.[211]

B. Fourth Amendment Concerns

The validity of the special system for foreign intelligence surveillance created under Section 702 — and, to the degree the Fourth Amendment covers phone metadata, Section 215 as well — rests on the notion that a traditional Fourth Amendment warrant is not required when the government seeks to collect foreign intelligence. The FISA Appeals Court has endorsed this view. It is far from clear, however, that a warrant may be dispensed with in all foreign intelligence cases — and it is quite clear that the foreign intelligence exception reflected in the current version of FISA goes far beyond what cases decided by regular federal courts would support.

Does the Fourth Amendment Protect Against "Incidental" Collection?

Some have argued that the Fourth Amendment is not even implicated where the collection of U.S. persons' calls and e-mails occurs "incidentally" in the course of collecting the communications of a foreign target who has no claim to constitutional protections. They point to the fact that, in the normal criminal context, the government is not required to obtain a warrant for each individual who is in communication with the target of surveillance. In those cases, however, the *target's* protections are substantial: surveillance ordinarily may not occur without a warrant based on probable cause of the target's criminal activity. This fact affords a certain level of vicarious protection to those in contact with the target. Moreover, the minimization procedures that protect those in communication with a target are much stronger in the criminal context.[212] The constitutional validity of incidental surveillance in that setting does not support the notion that the government may collect communications between a foreign target and a U.S. person wholly outside the strictures of the Fourth Amendment.

1. The FISA Court's "Special Needs" Analysis

In a challenge to the FAA's predecessor law, the FISA Court and the FISA Appeals Court both held that the collection of foreign intelligence was a "special need" so that no warrant was required to obtain it.[213] The "special needs" doctrine originated in the 1967 case of *Camara v. Municipal Court*, in which the Supreme Court held that city inspectors searching homes and businesses for fire hazards did not need to obtain a warrant based on probable cause of criminal activity. The reason: the case presented a "special need" — preventing fires — which simply could not be met if a regular criminal warrant were required.[214]

Instead of requiring a traditional warrant, the Court considered whether the searches were "reasonable" under the Fourth Amendment. It weighed the substantial public interest in enforcing safety codes against the invasion of privacy, which it found to be minimal because the search was not directed at a particular person and inspections were not aimed at discovering a crime — factors that, in the Court's view, reduced the risks of official overreaching and abuse.

The doctrine articulated in *Camara* has evolved to cover a range of special needs cases in which the government was found to act on interests that go beyond ordinary law enforcement functions. The special needs the Court has recognized include the need for schools to maintain discipline (search of a student's handbag by school officials looking for contraband),[215] the need to maintain a probation system (search of a probationer's home),[216] and the need to ensure the safety of the traveling public (drug testing of public transportation employees).[217]

In a 2008 opinion, the FISA Appeals Court extended this doctrine to the foreign intelligence context. Although noting that the Supreme Court had never recognized foreign intelligence collection as a special need, the court decided that the doctrine applied by analogy. No warrant was required for "surveillance undertaken for national security purposes and directed at a foreign power or an agent of a foreign power reasonably believed to be located outside the United States."[218] Having concluded that no warrant was required, the FISA Appeals Court then looked at the overall reasonableness of the surveillance.[219]

Unsurprisingly, the court found that the governmental interest in national security "is of the highest order of magnitude."[220] It then looked at the privacy protections included in various agency procedures and concluded that, in light of the weighty governmental interest, they were sufficient to pass constitutional muster.[221]

The court's decision did not critically analyze the government's contentions and veered from the case law on foreign intelligence and special needs. Closer examination shows that the government interest the court identified cannot support the broad exception to the warrant requirement that the court endorsed and that is reflected in current version of FISA.

2. Would a Warrant Requirement "Unduly Frustrate" Foreign Intelligence Gathering?

The Supreme Court repeatedly has held that warrants are generally required to comply with the Fourth Amendment and that exceptions to this rule are few and carefully delineated. Whether viewed as an exercise of the president's foreign affairs authority or as a "special need," foreign intelligence collection may be exempted from the warrant requirement only if a court finds that obtaining prior judicial approval based on probable cause of criminal activity would be "impracticable"[222] or would "unduly frustrate"[223] the government's ability to carry out its legitimate functions.

The government has put forward three primary reasons why it believes a warrant requirement is untenable. As described in Part II.A.3, most of the circuit courts to consider the government's claims accepted one or more of them.[224] In *Zweibon*, however, the D.C. Circuit rigorously analyzed and rejected all three.[225] Experience with the FISA system in the years that followed has only validated the D.C. Circuit's conclusions.

First, the government argued that security leaks from a warrant hearing could threaten national security or impede surveillance. The Supreme Court had rejected this contention in the context of domestic intelligence operations (the *Keith* case).[226] The D.C. Circuit found it equally unconvincing in the foreign intelligence context.[227] Indeed, the 35-year history of the FISA Court shows that judges and their staff are well able to maintain the requisite secrecy.

Second, the government argued that obtaining a warrant in foreign intelligence cases would cause unacceptable delay.[228] It is evident, however, that not every instance of foreign intelligence surveillance involves an urgent matter. Given the enormous scope of the NSA's collection and its repeated assertion that intelligence gathering often entails gathering innocuous pieces of a mosaic to reveal a potential threat, it can hardly be argued that each piece of information involves a time sensitive operation. And in truly urgent cases, the government may rely on a separate "exigent circumstances" exception to the warrant requirement.[229]

Finally, the government argued that evaluating foreign intelligence surveillance is beyond the scope of judicial expertise, citing the risk of harm to national security if a judge does not properly understand the government's foreign intelligence interest. The *Zweibon* court described this as relegating Fourth and First Amendment interests "to the level of second-class rights," and "naively equat[ing] all foreign threats with such dangers as another Pearl Harbor."[230] The court believed it was self-evident that a judge faced with a warrant application would take into account the magnitude of the threat identified by the government so that "the probability that a judge would erroneously deny the Executive the requested warrant approaches the infinitesimal."[231]

Today, the government might well add a fourth argument: the sheer extent of foreign intelligence surveillance necessary in the post-9/11 world makes the warrant requirement unworkable. Indeed, significant additional resources would be required for the government to obtain individualized warrants for all instances in which it currently captures communications between Americans and foreign targets. On the other hand, this factor presumably would cause the government to be more judicious in selecting targets. In any event, the need for significant additional resources cannot justify dispensing with a warrant requirement. As the Supreme Court has observed, "The argument that a warrant requirement would oblige the Government to obtain warrants in a large number of cases is hardly a compelling argument against the requirement."[232]

Judicial Deference In Surveillance Cases

The D.C. Circuit's instinct in *Zweibon* that courts will err on the side of national security when deciding whether to permit surveillance is borne out by the FISA Court's record. The court almost uniformly has granted surveillance applications, although a few have been modified.[233] A similarly heavy weight is assigned to the executive's interests in the Title III context. The latest statistics published by the Administrative Office of the United States Courts on federal and state wiretap activity show that judges almost never deny wiretap applications. From 1996 to 2013, less than 0.032 percentof applications were denied, even though requests grew by more than 200 percent.[234]

3. Is the Surveillance Reasonable under the Fourth Amendment?

Even if the collection of foreign intelligence is recognized as a "special need" that justifies surveillance without a traditional warrant, the government still must meet the second prong of the Fourth Amendment: the particular surveillance scheme must be "reasonable."

In *Camara*, the Supreme Court recognized fire safety as a special need, but it did not simply give the government free rein to search buildings at will. Instead, it required inspectors to obtain court orders based on factors relevant to fire safety, such as the age and nature of the building and the condition of the general area. Individualized orders still had to be obtained before the search, but the standards were altered to match the special need.[235] A similar arrangement may be required for foreign intelligence. As Fourth Amendment expert Professor Orin Kerr has noted: "[T]here is a plausible case to be made that foreign intelligence is a special need, but that [individualized] FISA warrants are still required to conduct foreign intelligence surveillance."[236]

Limits on the discretion vested in government officials are key to establishing the reasonableness of a special needs scheme. For example, even though the Court on several occasions has authorized checkpoints to assess motorists' sobriety or examine their license and car registration, it has refused to allow *roving* stops because they allow too much discretion on the part of government officials.[237] The Court has emphasized that meeting the reasonableness standard of the Fourth Amendment requires "at a minimum, that the facts upon which an intrusion is based be capable of measurement against 'an objective standard,' whether this be probable cause or a less stringent test."[238] This focus stems from the Court's concern about the potential for abuse of discretion; limiting this potential is a fundamental purpose of requiring a warrant under the Fourth Amendment.

As explored in the text box on page 33, the Section 702 program contains few limits on the discretion of analysts in deciding whether an individual is a non-U.S. person located overseas and therefore a valid target for programmatic surveillance. The NSA's targeting procedures set forth several considerations that officials *may* consider, but ultimately allow the NSA to reach a conclusion based on "the totality of the circumstances." The government has even more discretion in deciding what information is fair game: the statutory definition of foreign intelligence information is open-ended, and, under Section 702, the court cannot review the substance of the government's certification of a foreign intelligence purpose. It is difficult to square these features of programmatic surveillance with the type of "objective standards" that the Supreme Court has insisted on in the special needs context.

Moreover, even if the NSA's targeting and collection met the reasonableness test, the entire program cannot be deemed reasonable unless the government adequately "minimizes" the retention and use of information about U.S. persons that gets pulled in along with information about the foreign target. The FISA Court explicitly recognized this point when it found that the NSA violated the Fourth Amendment by failing to mark and delete wholly domestic e-mails acquired incidentally.[239] Although the NSA remedied this violation to the court's satisfaction, its minimization regime remains notably lax. U.S. person information may be retained for 5 years, and there are multiple loopholes allowing for longer-term retention — including a provision for the indefinite retention of encrypted communications.[240] As weak as the minimization rules are, reports suggest that they nonetheless are honored in the breach, with analysts claiming that they must retain seemingly irrelevant information about U.S. persons because the information may prove relevant in the future.[241]

A particularly stark affront to the principle of minimization is the practice known as "back-door searches." To obtain an order from the FISA Court authorizing programmatic collection, the government must certify that its interest lies in foreigners overseas and not any U.S. persons with whom they may be in contact. The law prohibits "reverse targeting," in which the government targets a foreigner as a pretext to gain information about a particular, known U.S. person.[242] Consistent with these directives, the minimization procedures governing programmatic surveillance originally barred the government from using U.S. person identifiers to search the pool of communications obtained under Section 702.[243] In 2011, the FISA Court granted the government's request to lift this bar.[244] Today, officials routinely search through Section 702 data for information about the very U.S. persons the government certified it was not targeting.[245]

This practice allows the government to dispense with the much stricter substantive and procedural requirements that Congress put in place for obtaining foreign intelligence on an American target.[246] It also allows the FBI to shrug off the Fourth Amendment when conducting domestic criminal investigations. The FBI performs searches of databases containing Section 702 data whenever it opens an investigation or an "assessment"[247] — a type of investigation in which agents do not have a factual predicate to suspect criminal activity, let alone probable cause.[248] Although the FISA Court has blessed back-door searches, it is difficult to see how a program that allows domestic law enforcement officers to listen to Americans' calls and read their e-mails without any fact-based suspicion of wrongdoing can be squared with the constitutional test of "reasonableness."

4. Is Foreign Intelligence Collection the Primary and Actual Purpose of Surveillance?

Contrary to the requirements articulated by several federal courts, Congress, backed by the FISA Appeals Court, has allowed the government to conduct warrantless surveillance even when collecting foreign intelligence is not its primary purpose.

As discussed, the most influential court of appeals decision permitting warrantless collection of foreign intelligence (*Truong*) held that obtaining foreign intelligence must be the "primary purpose" of collection. Other courts took a similar position.[249] While these cases involved surveillance that targeted U.S. persons, rather than surveillance of communications between foreign targets and U.S. persons, the rationale for the requirement — to avoid an end-run around warrants in domestic criminal cases — applies in both settings.

The Patriot Act, by contrast, adopted a "significant purpose" test, under which collection may take place even if the government's primary purpose is to gather evidence for a criminal prosecution. (The link to a foreign intelligence purpose was further attenuated by Section 702 of the FISA Amendments Act, which allows the government to certify that the acquisition of foreign intelligence is a significant purpose of the program as a whole, rather than requiring such a certification for each target.) In a 2002 decision, the FISA Court held that blurring the line between foreign intelligence and criminal investigations could allow criminal prosecutors to bypass the warrant requirement by appropriating more flexible FISA tools in cases where "the government is unable to meet the substantive requirements" of a regular warrant, or where the administrative burdens of obtaining one are deemed "too onerous."[250]

The FISA Appeals Court, however, disagreed and reversed, reasoning that criminal prosecutions "can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts."[251] Even where foreign intelligence is gathered for use in a criminal prosecution, the ultimate aim is still "to counter the malign efforts of a foreign power. Punishment of the terrorist or espionage agent is really a secondary objective."[252] By contrast, the court opined, the purpose of criminal law is to punish individual wrongdoers and deter others from following in their footsteps. Accordingly, the FISA Appeals Court concluded that acquiring foreign intelligence information for the purpose of bringing a criminal prosecution is consistent with Supreme Court case law holding that "special needs" can justify warrantless searches only outside the law enforcement context.

This reasoning was a stretch at best. Without citing any authority, the court assumed that "ordinary" criminal prosecutions differ from terrorism investigations because they are intended primarily to punish or deter crime. It ignored the fact that almost all prosecutions may be framed as serving broader societal purposes. Quite aside from punishment or deterrence, prosecutions of gang violence are intended to protect community safety and vitality; prosecutions of drug offenses are intended to promote public health; prosecutions of insider trading are intended to ensure the stability and integrity of financial markets; etc. The Supreme Court has clearly held that such broader motives cease to justify warrantless searches at the moment the "immediate objective" shifts to criminal investigation or prosecution.[253] Thus, for instance, a hospital's program to test obstetrics patients for drug use in order to improve fetal health was struck down because it involved referring those who tested positive to criminal authorities for prosecution.[254]

At bottom, the FISA Appeals Court's analysis tries to have it both ways. On the one hand, the court characterized foreign intelligence investigations as fundamentally different from ordinary criminal investigations, to the point that the former may be labeled a "special need" and placed in an entirely separate category for Fourth Amendment purposes. On the other hand, the court found criminal proceedings to be such a fundamental and inextricable element of foreign intelligence investigations as to render the "primary purpose" test arbitrary and unworkable. These premises are, at a minimum, in tension.

Finally, courts have emphasized the need for close judicial scrutiny of the particular facts of each case to ensure that foreign intelligence collection is not used as a cover for domestic surveillance. The routine use of "back-door searches" by the FBI when opening any investigation or assessment strongly suggests that Section 702 has become, in substantial part, a domestic law enforcement tool. Leaving aside whether this practice undermines the constitutional reasonableness of the program as a whole, it certainly would undermine the legitimacy of any given instance of surveillance that was undertaken with the goal of obtaining information about a U.S. person through a "back-door search." Only close judicial review can discern whether that is the case.

Yet no such scrutiny takes place under the current system. As discussed, there is rarely an opportunity for after-the-fact review of the sort conducted by the courts of appeal in *Truong* and other foreign intelligence cases. Even when a traditional, individualized FISA order is used to target a U.S. citizen and the government discloses this fact in a criminal proceeding, the defendant is prohibited from seeing the materials comprising the government's application, which not only limits the defendant's ability to challenge the order but also significantly handicaps the court's ability to adjudicate its validity.[255]

Nor does any court review particular cases or targets prior to collection under either Section 702 or the Section 215 bulk collection program. Indeed, under Section 702, the FISA Court conducts no individualized inquiry whatsoever and is barred from performing any substantive review of the government's certification of a "foreign intelligence" purpose. This forced judicial passivity is a far cry from the microscopic examination courts have deemed necessary[256] to ensure that foreign intelligence surveillance does not become an end run around the Fourth Amendment's warrant requirement.

5. Is the Scope of Foreign Intelligence Surveillance Properly Limited?

The courts that have allowed foreign intelligence collection to take place outside the warrant framework have noted the narrowness of this exception. In *Truong*, the Fourth Circuit emphasized the need to carefully limit the foreign intelligence exception, allowing it only when

> the object of the search or the surveillance is a foreign power, its agent or collaborators. In such cases, the government has the greatest need for speed, stealth, and secrecy, and the surveillance in such cases is most likely to call into play difficult and subtle judgments about foreign and military affairs. When there is no foreign connection, the executive's needs become less compelling; and the surveillance more closely resembles the surveillance of suspected criminals, which must be authorized by warrant.[257]

As enacted in 1978, FISA required the government to show probable cause that the target of surveillance was a foreign power or an agent of a foreign power. The FAA eliminated this requirement for programmatic surveillance. The target of surveillance may be *any* non-U.S. person or entity located overseas, and the FISA Court has interpreted the law to allow the government to obtain any communications to, from, *or about* the target.[258] The only limitation is a requirement that the government certify that a significant purpose is the collection of "foreign intelligence."

Consider how these changes could operate in practice. As noted in Part II.C.2, "foreign intelligence information," where non-U.S. persons are concerned, is broadly defined to include information "that relates to . . . (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States."[259] This elastic concept is unlikely to impose any meaningful restraint — particularly since the FISA Court is not allowed to probe the government's foreign intelligence certification.[260] The only real limitation on surveillance, then, is the target's nationality and location.

Given the prevalence of international communication today, the government could shoehorn literally billions of communications (including communications with Americans) into a warrantless foreign intelligence collection framework, as long as there is a chance that the net will pull in some information relating to security or foreign affairs. This is plainly inconsistent with the admonition of most courts that warrantless foreign intelligence surveillance must be "carefully limited" to "those situations in which the interests of the executive are paramount."[261]

In a 2008 opinion approving Section 702 targeting and minimization procedures, the FISA Court held that limiting the foreign intelligence exception to foreign powers or their agents is unnecessary when the target is a non-citizen overseas.[262] This ruling ignores the fact that Section 702 is designed to capture

communications involving U.S. persons, and expressly contemplates that U.S. person information may be kept and shared where minimization would be inconsistent with "the need of the United States to obtain, produce, and disseminate foreign intelligence information."[263] Regardless of who is labeled the "target," Section 702 involves the acquisition and use of Americans' information for foreign intelligence purposes, in volumes that likely far exceed the collection in *Truong* and similar cases. The need to construe the exception narrowly is thus at least as important in the Section 702 context.

The Fourth Amendment and Telephone Metadata

Relying on Supreme Court precedent dating from 1979,[264] the FISA Court and some regular federal courts have held that records held by third parties, such as transactional records of telephone calls held by companies to enable them to carry out their billing functions (so-called "metadata"), do not receive Fourth Amendment protection.[265] However, there is increasing judicial recognition that modern life requires the disclosure of highly personal information to third parties, and that this forced disclosure should not eviscerate all privacy interest in the information.

As a threshold matter, the notion that telephone records are not particularly revealing of private information has been debunked. The former head of the NSA has said that the U.S. government kills people based on metadata.[266] Experts have explained that, with the help of sophisticated computer programs, government officials can use metadata to create a detailed picture of a person's associations, activities, and even beliefs.[267] Indeed, in some cases, the metadata for even a single call can be just as revealing as the content — for instance, a late-night call placed to a suicide hotline. This is the type of information in which a person should have a reasonable expectation of privacy.

As for whether disclosure to a communications service provider eviscerates that expectation, courts are becoming more skeptical. In an admittedly different context — the warrantless acquisition of the *content* of e-mails stored with a third party — the Sixth Circuit in 2010 held that "the mere ability of a third-party intermediary to access the contents of a communication cannot be sufficient to extinguish a reasonable expectation of privacy."[268] The Supreme Court's recent decision in *Riley v. California*, requiring warrants to search cell phones incident to arrest, relied heavily on the types of information stored on cell phones — including information (such as that generated by "apps") that by definition is shared with third parties — in assessing the privacy interests at stake.[269] In an influential concurring opinion in *United States v. Jones*, Justice Sonia Sotomayor signaled that it might be time for the Supreme Court to reconsider its stance on third party records.[270]

If telephone records and other such data held by third parties are protected by the Fourth Amendment, collection under Section 215 would be constitutional only if it fell within an exception to the warrant requirement — presumably the foreign intelligence exception. And in that case, in order to ensure that the exception was narrowly drawn, the records would have to pertain to a foreign power or its agent (as explained in *Truong*). This requirement was present in the 1999 version of the law, but was eliminated by the Patriot Act.

***

As this report shows, the legal and technological changes of recent years have altered fundamentally the nature of the FISA Court's endeavors. A court that once applied the law to the facts of particular cases now approves vague government procedures outside the context of any particular application. A court that once exercised jurisdiction over surveillance targeting foreign powers and their agents primarily for intelligence purposes now oversees surveillance targeting any non-citizen abroad, even where foreign intelligence collection is a decidedly secondary motive. These changes undermine the legitimacy of the court, as well as Americans' privacy. The problem with the FISA Court, it turns out, is FISA itself.

V. RECOMMENDATIONS

Major reforms are necessary to bring judicial review of foreign intelligence surveillance into compliance with the Constitution. But charting a course for reform that will address the various problems detailed in this report is no simple task. For instance, the most obvious and direct remedy when a court is performing a non-judicial function is to transfer the function to the appropriate branch. While allowing the executive branch to approve its own surveillance procedures might cure any Article III defects, however, it would exacerbate Fourth Amendment concerns. The recommendations for reform that appear below would not resolve every concern surrounding the activities of the FISA Court, but would go far toward bolstering the constitutionality, under both Article III and the Fourth Amendment, of the FISA scheme.

A. End Programmatic Surveillance

The most effective reform would be for Congress to end programmatic surveillance. This would entail expressly prohibiting bulk collection under Section 215 and similar provisions, as well as repealing Section 702 and replacing it with a regime requiring an individualized court order for the interception of communications involving U.S. persons, regardless of whether they are the identified target of the surveillance.

Ending programmatic surveillance would return the FISA Court to its traditional role of applying the law to the facts of a particular case.[271] This would mitigate many of the Article III concerns relating to the absence of a case or controversy. If the standard for issuing a surveillance order were sufficiently strict (discussed below), ending programmatic surveillance could address Fourth Amendment objections as well.

But these changes would not fully cement the constitutional status of the FISA Court's activities. FISA orders will never look entirely like criminal warrants because they rarely culminate in criminal prosecutions, thus removing the primary vehicle for challenging their legitimacy. Concerns about the lack of adversarial process thus would remain even if programmatic surveillance were replaced with an individualized regime. To address them, the reforms listed in the next section would be needed.

B. Enact Additional Article III-Related Reforms

1. Introduce Adversarial Processes

Several existing reform proposals would address the lack of a party opposing the government in FISA Court proceedings by establishing a permanent public interest advocate (or slate of advocates) to represent the interests of people affected by government surveillance.[272] President Obama and two former judges of the court publicly support the appointment of such an attorney, commonly referred to as the "Special Advocate."[273] An alternative approach would allow the FISA Court to hear from certain individuals or interest groups as *amici curiae*.[274] The court could call upon these outside representatives to weigh in on potential privacy and civil liberties concerns raised by a government application.[275]

The latter approach would not resolve the Article III problem, particularly if participation were left to the court to decide. The FISA Court already has discretion to solicit or permit *amicus* participation, and with few exceptions, has preferred to rely on the government's submissions alone.[276] Article III would be best served by strengthening the special advocate concept to the greatest extent possible, including by ensuring that special advocates are notified of cases pending before the court, have the right to intervene in cases of their choosing, and are given access to all materials relevant to the controversy in which they are intervening.

In addition, there must be a mechanism for appeal in cases where the court rules against the special advocate. Legitimate questions arise as to whether a special advocate would have standing to bring an appeal, given the advocate's lack of a personal stake in the outcome.[277] Various solutions to this problem have been proposed: for example, the special advocate could serve as a *guardian ad litem* for third parties affected by the surveillance (such as those incidentally in communication with the target), or the court could be required to certify particular types of decisions to the FISA Appeals Court for review.[278] The standing problem, while real, is not insurmountable.

2. Increase Transparency and Facilitate Collateral Challenges

A defining feature of the FISA Court is that nearly all of its decisions are classified. This hampers democratic self-government and sound policymaking. It also has Article III implications: secret decisions cannot be challenged, and the opportunity to challenge a FISA Court order in collateral proceedings is critical to the legitimacy of the process. A number of existing proposals would introduce some transparency by requiring the executive branch to release full copies, redacted versions, or summaries of FISA Court opinions containing significant legal opinions.[279] For both constitutional and policy reasons, Congress should establish a non-waiveable requirement that the government issue public versions of FISA Court opinions or summaries containing certain minimum information — including the legal questions addressed, as well as the construction or interpretation given to any legal authority on which the decision relies.

Transparency alone cannot address the Article III defects in the FISA Court. Congress also must facilitate collateral challenges. One key step would be to prohibit the practice of "parallel construction," in which the government builds a criminal case based on FISA-derived evidence but then reconstructs the evidence using other means. This allows the government to avoid notifying defendants of the FISA surveillance and thus makes it impossible for them to challenge it. Any time the government uses the tools of FISA as part of an investigation, the subject of any resulting legal proceedings should be notified, and should be entitled to challenge any evidence that resulted either directly or indirectly from that surveillance.

The special procedures governing a defendant's access to FISA application materials, under which a defendant is almost never given any hint of their contents, should be jettisoned. Instead, the process under the Classified Information Procedures Act (CIPA)[280] — which has been used successfully in the most sensitive national security and espionage cases, and which allows the government to use summaries or admissions of fact in place of classified information — should apply.[281]

Finally, the government's attempt to shut down *every* civil lawsuit that has been brought to challenge the constitutionality of foreign intelligence surveillance must end. Even where plaintiffs have had reasonable grounds to fear that they were being surveilled[282] — indeed, even where they have had irrefutable proof[283] — the government has tried to have the lawsuit dismissed, arguing that the plaintiffs lacked evidence or that the evidence contained state secrets. Today, after Snowden's disclosures, many secret programs are public knowledge and dismissing plaintiffs' fears of surveillance as "speculative" is increasingly disingenuous. Moreover, warrantless surveillance is no longer a secret, it is the law — and, given the broad scope of collection, acknowledging that a plaintiff has standing to challenge FISA surveillance does not reveal the identity of any investigation's target. If ever the government's jurisdictional and national security defenses had merit, they no longer do.

C. Enact Additional Fourth Amendment-Related Reforms

Restoring the requirement that the government obtain individualized court orders before conducting surveillance does not end the Fourth Amendment analysis. The question of what standards the court should apply in issuing these orders remains. Even if the Supreme Court were to hold that acquiring foreign intelligence is a special need and that the government need not demonstrate probable cause of criminal activity, longstanding precedent suggests that the collection of foreign intelligence must adhere to the following standards and procedures.

1. Restore the "Foreign Power/Agent of a Foreign Power" Requirement

The government should be permitted to conduct surveillance in the United States only when it can show probable cause that the target is a foreign power or its agent. This would reinstate the standard contained in original FISA. It also would track the holding of *Truong* and other courts that sought to limit the universe of individuals whose communications may be captured under the foreign intelligence exception. The terms "foreign power" and "agent of a foreign power" are quite broadly defined, including terrorist groups and other non-state actors. They are thus expansive enough to accommodate the government's legitimate security interests, while enhancing protection for U.S. persons (and the foreigners with whom they communicate).

2. Narrow the Definition of "Foreign Intelligence Information"

The definition of "foreign intelligence information" in FISA should be narrowed. The courts of appeal have admonished that the foreign intelligence exception must be narrowly construed and reserved for matters in which the executive branch's interests are of the most compelling nature. Yet, in addition to information necessary to protect against foreign attack, terrorism, or espionage, the current definition includes information relevant to (or, in the case of a U.S. person, necessary to) "the security of the United States" and "the conduct of the foreign affairs of the United States." A general interest in obtaining any information that "relates to" these vague areas cannot justify the massive intrusion on privacy and First Amendment rights implicated by the warrantless acquisition of Americans' international communications.

The definition of "foreign intelligence information" could usefully be narrowed to information relating to external threats — including "actual or potential attacks or other grave hostile acts," "sabotage,"

"international terrorism," "the international proliferation of weapons of mass destruction," and "clandestine intelligence activities."[284] These are the specific threats currently listed in FISA's statutory definition, minus the overbroad catch-all language regarding security and foreign affairs.

Another option is to rely on the restrictions that President Obama recently placed on the permissible uses of signals intelligence information collected abroad in bulk. Presidential Policy Directive 28, issued on January 17, 2014, states that such information shall be used

> only for the purposes of detecting and countering: (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests; (2) threats to the United States and its interests from terrorism; (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction; (4) cybersecurity threats; (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel; and (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section.[285]

The surveillance activities governed by this Directive are subject to fewer domestic legal constraints than any other type of communications surveillance. The fact that the above restrictions are considered appropriate in a context where the president has maximum discretion strongly suggests that imposing the same limits in the context of Section 702 collection would not unduly restrict the government's intelligence gathering. More fundamentally, defining "foreign intelligence information" as information relating to the above-listed threats would honor the principle that any foreign intelligence exception should be limited to instances in which the government's interests are paramount.[286]

3. Restore the "Primary Purpose" Test

Congress should amend FISA to require that obtaining foreign intelligence information be the primary purpose of surveillance. Other than the FISA Appeals Court, the courts that have recognized a foreign intelligence exception have generally imposed such a "primary purpose" requirement. As these courts have recognized, surveillance that is primarily for law enforcement purposes must take place pursuant to a regular criminal warrant, lest the foreign intelligence exception drive a massive hole through the protections of the Fourth Amendment.

The FISA Court also must be empowered to review whether there are truly foreign intelligence considerations at stake, and whether acquiring foreign intelligence is the primary purpose of surveillance. Courts of appeal have emphasized the need for close scrutiny on this point, noting that "judges must microscopically examine the wiretaps in order to determine whether they had their origin in foreign intelligence," and that warrantless wiretaps should be upheld only when "the foreign and sensitive nature of the government surveillance is crystal clear."[287]

Congress should accordingly strengthen the certification requirement. It should direct the executive branch to certify, not merely that its primary purpose is to acquire foreign intelligence information, but that the requested surveillance is reasonably likely to produce such information. It also should

authorize the court to review this certification not only for proper form (as is currently the case), but for its substance as well. And it should prohibit the practice of "back door searches," which gives the government an easy end-run around the foreign intelligence purpose requirement as well as the requirement of targeting foreigners overseas.

An argument could be made that no court — not even the highly specialized FISA Court — has the expertise necessary to evaluate whether a given collection is likely to produce foreign intelligence. But under current law, the FISA Court reviews the government's certification of a "foreign intelligence" purpose for clear error when surveillance is targeted at a U.S. person. Congress thus has acknowledged the judiciary's competency to conduct at least a limited review of the executive's conclusions about the foreign intelligence value of proposed surveillance.

D. If Programmatic Surveillance Continues, Reform It

As the above discussion makes clear, the key to reforming the FISA Court is ending programmatic surveillance. If such surveillance continues, serious Article III and Fourth Amendment problems will be unavoidable. It is nonetheless worth noting that, as a policy matter, incorporating the reforms set forth in Parts V.B and V.C, above, into programmatic surveillance would enhance privacy and strengthen the judiciary's role.

Specifically, if programmatic surveillance continues, Congress should amend Section 702 to require that the target of surveillance must be a foreign power or its agent. It should narrow the definition of foreign intelligence as discussed above. It should require the executive branch to certify that the collection of foreign intelligence is both the primary purpose and the likely outcome of the programmatic activities, and empower the FISA Court to review that certification on its substance. All of these changes would nudge programmatic surveillance in the right direction on the Fourth Amendment reasonableness spectrum — even if, in our view, they would not go far enough.[288]

Moreover, additional steps should be taken that would make the court's limited role more meaningful. More specific statutory requirements for targeting and minimization procedures would enhance the FISA Court's ability to ensure that the agencies conducting surveillance are complying with the law. Currently, the criteria for these procedures are so subjective and open-ended, they provide no useful benchmark for the court to apply. They also permit a level of vagueness in the agency's own procedures that renders the court's facial review a hollow exercise.[289]

Finally, Congress should require the government, on a periodic basis, to submit to the FISA Court for its review a list of the selection terms used to acquire electronic communications under Section 702. For each selection term, the government should summarize succinctly the facts supporting its use. This would provide the FISA Court with a concrete factual basis on which to evaluate the constitutionality of foreign intelligence surveillance activities. The government's determinations should be reviewed by the court for clear error, with the government required to cease collection (and purge any already-collected information) in cases that fall below that low bar.[290]

CONCLUSION

Changes in the law and technology over the last 40 years have upended the compromise reached by Congress in 1978 when it first established the FISA Court to supervise the collection of foreign intelligence in the United States. Today, the court's activities resemble neither the granting of warrants nor the ordinary adversarial process for reviewing a challenge to the constitutionality of an agency's program. Instead, the court provides a veneer of judicial oversight for surveillance activities, blessing mammoth covert programs without hearing from those affected by them.

But this type of approval is not what the Constitution contemplates or allows. Nor does the Constitution countenance the mass collection of information about ordinary, law-abiding Americans who happen to communicate with foreigners overseas.

Revamping this system is one of the most crucial challenges of our time. It will not be accomplished by small reforms that nibble at the edges of the problem. Congress must directly tackle the foundational legal weaknesses of the FISA Court to bring it back into line with its constitutional role of providing a strong judicial check on executive branch surveillance.

ENDNOTES

1 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter Patriot Act] (codified as amended in scattered sections of 5, 8, 10, 12, 15, 18, 20, 21, 22, 28, 31, 42, 47, 49, 50 U.S.C.).

2 Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 [hereinafter Foreign Intelligence Surveillance Act of 1978] (codified in scattered sections of 8, 18, 47, 50 U.S.C.).

3 The initial number of FISA Court judges was seven. Foreign Intelligence Surveillance Act of 1978, *supra* note 2, at § 103 (current version at 50 U.S.C. § 1803). This was increased to 11 by the Patriot Act, which also added a requirement that at least three of the judges reside within 20 miles of the District of Columbia. Patriot Act, *supra* note 1, at § 208 (codified as amended at 50 U.S.C. § 1803).

4 50 U.S.C. §§ 1803(a)(1), 1803(d).

5 David S. Kris & J. Douglas Wilson, National Security Investigations & Prosecutions 2d § 5.3 n.14 (2012) [hereinafter Kris & Wilson Treatise]. To avoid the potential for "judge shopping" between members of the FISA Court, applications under FISA are heard by a single FISA Court judge, and the government may not ask a second judge to consider an application for electronic surveillance or a physical search after one FISA Court judge has denied it. 50 U.S.C. § 1803(a)(1); FISA Ct. R. P. 18(b)(2). In most cases, the only recourse for a denial is an appeal to the FISA Appeals Court. *See infra* text accompanying note 6. However, a case may be reheard by the entire slate of FISA Court judges in particular circumstances, if the majority of them agree. 50 U.S.C. § 1803(a)(2).

6 50 U.S.C. § 1803(b).

7 H.R. Rep. No. 95-1283, at 71 (1978). The Senate Intelligence Committee's report also noted that "[t]he need to preserve secrecy for sensitive counterintelligence sources and methods justifies ... consolidation of judicial authority in a special court…." S. Rep. No. 95-701, at 12 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 3980. The House version of FISA initially allowed judges to hear applications in the district where the surveillance was to take place. This was strongly opposed by Attorney General Griffin Bell, who argued that requiring intelligence officials "to travel across the country seeking a judge with jurisdiction to act in a particular locale" would make it "difficult to protect the security of … information and difficult to reach such a judge in time to act in an effective manner in urgent circumstances." 124 Cong. Rec. H12539 (daily ed. Oct. 12, 1978) (statement of Rep. Morgan Murphy quoting letter from Attorney General Bell). The directors of the CIA, NSA, and FBI also strongly argued against the House amendment, arguing that "the inability of the Government to make secure widely dispersed court facilities and numerous personnel would have made highly secret information potentially available to hostile foreign intelligence services." 124 Cong. Rec. H12534 (daily ed. Oct. 12, 1978) (statement of Rep. Robert Kastenmeier). These concerns were addressed by centralizing the work of the FISA Court in Washington, D.C. H.R. Rep. No. 95-1283, at 71 (1978).

8 H.R. Rep. No. 95-1283, at 91 (1978).

9 *See infra* Part IV.A. Although FISA doesn't explicitly state that the FISA Court is established under Article III, the court itself has taken the position that this is the case. *In re* Motion for Release of Court Records, 526 F. Supp.2d 484, 486-87 (FISA Ct. 2007). It has also been recognized as an Article III court by various courts of appeals. *See, e.g.,* United States v. Abu-Jihaad, 630 F.3d 102, 120 (2d Cir. 2010) (citing decisions of various courts of appeals in deciding that the FISA Court operates appropriately as an Article III court).

10 The "oldest and most consistent" application of the federal law of justiciability holds that federal courts may not give "advisory opinions." Flast v. Cohen 392 U.S. 83, 96 n.14 (1968) (quoting C. Wright, Federal Courts 34 (1963)) (noting that "the rule against advisory opinions was established as early as 1793").

11 *See, e.g.*, 124 Cong. Rec. H7776 (daily ed. Aug. 2, 1978) (statement of Rep. Robert Drinan) ("I do not understand why the judges assigned to these special courts would not take offense at the duties and limitations imposed on them. They are not free to examine all the evidence presented by the Attorney General as they are in the ordinary warrant application process under title III."); *Foreign Intelligence Surveillance Act: Hearing Before the Subcomm. on Courts, Civil Liberties, and the Admin. of Justice on the Comm. on the Judiciary,* 95th Cong. 115 (1978) [hereinafter *1978 Judiciary Hearing*] (statement of Rep. George Danielson, Member, H. Comm. on the Judiciary) ("Is the court itself to play the role of advocate? Who is coming in for the Soviet Union to decide whether or not this alleged espionage agent should be surveilled? I respectfully submit we have none."); 124 Cong. Rec. H9122 (daily ed. Sept. 6, 1978) (statement of Rep. Allen Ertel, Member, H. Comm. on the Judiciary) ("We are compromising our Constitution…. Decisions will be made in secret …. There will be no exposure to the public, no way to review them."); 124 Cong. Rec. E1205 (daily ed. Mar. 10, 1978) (statement of Robert H. Bork) ("The bill pretends to create a real set of courts that will bring 'law' to an area of discretion. In reality, it would set apart a group of judges who must operate largely in the dark and create rules known only to themselves.").

12 *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. 26 (1978) [hereinafter OLC Memo] (statement of John M. Harmon, Asst. Att'y. Gen., Office of Legal Counsel).

13 *Id.* at 31.

14 *Id.* at 28.

15 *Id.* at 29.

16 United States v. Megahey, 553 F. Supp. 1180, 1196-97 (E.D.N.Y. 1982) *aff'd* 729 F.2d 1444 (2nd Cir. 1983). Additional arguments based on Article III were also rejected by courts. For example, some defendants argued that FISA Court judges were not independent because they were not appointed to that particular court for life. Courts uniformly rejected this objection. FISA judges were found to be sufficiently independent because they were Article III district court judges who had life tenure and whose salary could not be diminished. Matter of Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986). Moreover, as the Ninth Circuit explained: "[T]emporary designation within the federal judicial system has never been thought to undermine the judicial independence that [A]rticle III was intended to secure." United States v. Cavanagh, 807 F.2d 787, 792 (9th Cir. 1987). Defendants also argued that two provisions of the statute unconstitutionally required FISA Court judges to resolve political questions committed to the other branches of government. First, defendants argued that where the government alleges that a FISA target is an agent of an international terrorist organization, the judge must consider the definition of "international terrorism." Courts found, however, that because that term is defined in terms of criminal activity, applying it to a FISA application was no different from the normal factual and legal judgments that courts make under criminal laws. *Megahey*, 553 F. Supp. at 1196. *See also* United States v. Hovsepian, No. CR 82-917 MRP, 1985 WL 5970, at *3 (C.D. Cal. Jan. 25, 1985); United States v. Duggan, 743 F.2d 59, 74–75 (2d Cir. 1984). Second, defendants contended that the FISA Court would be required to review the government's certification that the information it seeks is "foreign intelligence information," which includes information on "the conduct of the foreign affairs of the United States" normally thought to be within the purview of the executive branch. *Duggan*, 743 F.2d at 71 (citing 50 U.S.C. § 1801(e)(2)(B)). This argument too was rejected because the limited review conducted by the FISA Court "does not unduly inject the courts into the making of foreign policy". *Duggan*, 743 F.2d at 75.

17 *See Matter of Kevork*, 634 F. Supp. at 1014; *Megahey*, 553 F. Supp. at 1196-97; United States v. Falvey, 540 F. Supp. 1306, 1314 (E.D.N.Y. 1982).

18 *Foreign Intelligence Electronic Surveillance: Hearings on H.R. 5794, H.R. 9745, H.R. 7308, and H.R. 5632 Before the Subcomm. on Legislation. of the H. Permanent Select Comm. on Intelligence*, 95th Cong. 224 (1978) (statement of Hon. Laurence Silberman). Prof. Silberman eventually became a FISA Court of Review judge himself and apparently shed his misgivings, participating in a decision blessing a huge expansion of the government's surveillance authority. *See infra* text accompanying notes 228-34 (describing FISA Court of Review decision allowing the government to conduct warrantless surveillance even when collecting foreign intelligence is not primary purpose).

19 50 U.S.C. § 1806(c). At the time FISA was originally introduced, it provided that when the government intended to use evidence derived from FISA surveillance in a court proceeding, it must notify the relevant court, but need only disclose to the aggrieved person in question specific portions of documents where "necessary for an accurate determination of the legality of the surveillance." Foreign Intelligence Surveillance Act of 1977, S. 1566, 95th Cong. § 2526(c) (as introduced May 18, 1977). The subsequent legislative history indicates that critics of the bill testified in Congress against this provision, arguing that this framework impinged upon the adversarial process by allowing a solely *ex parte* determination of the government's assertion and a lack of notice for the aggrieved person. *See, e.g.*, *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. 128-32 (1978) (statement of Robert C. Sheehan, Bar of the City of New York) ("We find the [*ex parte* determination] provision abhorrent to basic concepts of due process, and … there is a substantial possibility that it is unconstitutional, at least with respect to criminal proceedings."); *Foreign Intelligence Surveillance Act: Hearing Before the Subcomm. on Courts, Civil Liberties, and the Administration of Justice on the Comm. on the Judiciary,* 95th Cong. 124 (1978) (statement of Rep. Allen Ertel) ("Why then do we even get the court involved … if really, the court is going to rely on affidavits from the Attorney General? He is going to say it is sufficient … so I don't understand why we even have the court putting its stamp of approval, or is it just a sham we are exercising for the American people's satisfaction?").

20 Katz v. United States, 389 U.S. 347 (1967).

21 Olmstead v. United States, 277 U.S. 438, 466 (1928).

22 *Katz*, 389 U.S. at 353.

23 *Id.* at 356 (In the scheme the Court found unconstitutional, "restraint was imposed by the [law enforcement] agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized.").

24 *Id*. at 358 n.23. Justice Douglas, in a concurring opinion joined by Justice Brennan, decried this "wholly unwarranted green light for the Executive Branch to resort to electronic eavesdropping without a warrant in cases which the Executive Branch itself labels 'national security' matters." *Id*. at 359 (Douglas, J., concurring). He noted that the president and the Attorney General are not neutral magistrates but rather interested parties in national security cases and that the Fourth Amendment does not distinguish between various types of substantive offenses based on their seriousness in a way that would suggest treating national security cases differently from other types of crime. *Id*. at 359-60.

25 Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197 (codified as amended in scattered sections of 5, 18, and 42 U.S.C.).

26 *Id.* at § 802. The Patriot Act expanded the list of criminal statues for which wiretaps can be ordered. Patriot Act, *supra* note 1, at §§ 201-202 (codified as amended at 18 U.S.C. § 2516(1)-(2)).

27 Title III contained a few exceptions to this warrant requirement. The government could conduct warrantless surveillance where one party to the communication consented; a specially designated enforcement officer was authorized to wiretap without prior judicial approval in an "emergency situation"; and employees of communications providers and the Federal Communications Commission could intercept communications in the course of their normal duties. Omnibus Crime Control and Safe Streets Act § 802 (codified as amended at 18 U.S.C. §§ 2511(2), 2518(7)).

28 Title III left untouched the President's power to take measures that he deemed 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" and "to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." Omnibus Crime Control and Safe Streets Act § 802 (codified as amended at 18 U.S.C. § 2511(3)). This language was the subject of significant controversy among lawmakers, in part because it seemed to imply that the president's national security warrantless wiretapping authority could extend to purely domestic security matters. Indeed, the Senate report that accompanied the bill stated that it was not intended to limit the president's power to obtain information to protect the United States from foreign powers and foreign intelligence activities "or any other danger to the structure or existence of the Government," citing the domestic Communist party as an example. S. Rep. No. 90-1097, at 2182 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2182. The minority report took the view that the provision left too much discretion to the executive branch, noting that: "Under Section 2511(3) a President on his own motion could declare a militant right wing political group (i.e., the Minutemen) or left wing group (i.e., Black Nationalists), a national labor dispute, a concerted tax avoidance campaign, draft protesters, the Mafia, civil rights demonstrations, a 'clear and present danger to the structure of the Government.' Such a declaration would allow unlimited unsupervised bugging to certain crimes and places such eavesdropping under judicial supervision." S. Rep. No. 90-1097, at 2235 (1968), *reprinted in* 1968 U.S.C.C.A.N. 2112, 2235. The meaning of the exception was effectively decided in the subsequent *Keith* case. United States v. U.S. Dist. Court for E. Dist. of Mich. (*Keith*), 407 U.S. 297 (1972); *see infra* Part II.A.2.

29 *Keith*, 407 U.S. at 323-24.

30 *Id.* at 300.

31 *Id*. at 309 (emphasis added). A domestic organization was defined as "a group or organization (whether formally or informally constituted) composed of citizens of the United States and which has no significant connection with a foreign power, its agents or agencies." *Id*. at 309 n.8.

32 *Id*. at 308.

33 *Id.* at 313.

34 *Id*. at 317.

35 *Id.* at 323.

36 *Id.* at 322-23.

37 *Id.* at 325 (Douglas, J., concurring).

38 *Id*.

39 *Id.* at 327-28.

40 United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 604-05 (3rd Cir. 1974) (en banc); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977).

41 *Truong*, 629 F.2d at 913.

42 *Id.* at 915.

43 *Id.*

44 *Id.*

45 *Id.* (emphasis added). The court concluded its discussion "by underscoring the limited nature of this foreign intelligence exception to the warrant requirement which we recognize in the instant case. The exception applies only to foreign powers, their agents, and their collaborators. Moreover, even these actors receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution. Thus, the executive can proceed without a warrant only if it is attempting primarily to obtain foreign intelligence from foreign powers or their assistants." *Id.* at 916.

46 United States v. Brown, 484 F.2d 418, 427 (5th Cir. 1973) (Goldberg, J., specially concurring) ("The judiciary must not be astigmatic in the presence of warrantless surveillance; rather judges must microscopically examine the wiretaps in order to determine whether they had their origin in foreign intelligence or were merely camouflaged domestic intrusions. The serious step of recognizing the legality of a warrantless wiretap can be justified only when, as in the case before us, the foreign and sensitive nature of the government surveillance is crystal clear.").

47 United States v. Butenko, 494 F.2d 593, 606 (3d Cir. 1974) (en banc) ("Since the primary purpose of these searches is to secure foreign intelligence information, a judge, when reviewing a particular search must, above all, be assured that this was in fact its primary purpose and that the accumulation of evidence of criminal activity was incidental. If the court, for example, finds that members of a domestic political organization were the subjects of wiretaps or that the agents were looking for evidence of criminal conduct unrelated to the foreign affairs needs of a President, then he would undoubtedly hold the surveillances to be illegal and take appropriate measures.").

48 Zweibon v. Mitchell, 516 F.2d 594 (1975).

49 *Id*. at 600.

50 *Id.* at 613-14.

51 United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

52 *Id.* at 275-78 (Kennedy, J., concurring) (opining that the Constitution applies overseas as well as domestically, but that requiring a warrant for an overseas search would be "impracticable and anomalous" and therefore not constitutionally required); *id.* at 279 (Stevens, J., concurring) (opining that the Fourth Amendment applies when the government searches the overseas property of a foreigner who has been arrested and brought to the U.S., but that no warrant is required "because American magistrates have no power to authorize such searches"); *id.* at 279-97 (Brennan & Marshall, JJ., dissenting) (opining that the Fourth Amendment requires the government to obtain a warrant to conduct a search of a foreign criminal suspect's property overseas); *id.* at 297-98 (Blackmun, J., dissenting) (opining that the Fourth Amendment applies when the government searches a foreign criminal suspect's property abroad; that a warrant is not required because American magistrates lack the authority to issue a warrant for an overseas search; but that the "reasonableness" requirement of the Fourth Amendment demands that probable cause for the search exist).

53 Carl Bernstein & Bob Woodward, *FBI Finds Nixon Aides Sabotaged Democrats*, Wash. Post, Oct. 10, 1972, at A01, *available at* http://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/101072-1.htm.

54 Seymour M. Hersh, *Huge C.I.A. Operation Reported In U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. Times, Dec. 22, 1974, at A1,
available at http://s3.documentcloud.org/documents/238963/huge-c-i-a-operation-reported-in-u-s-against.pdf.

55 *See* David Rudgers, *The Church Committee on Intelligence Activities Investigation, 1975-76, in* Congress Investigates: A Critical and Documentary History 930 (Roger A. Bruns, David L. Hostetter & Raymond W. Smock eds., Facts on File Inc. 2011) [hereinafter *Rudgers: The Church Committee*]; Seymour M. Hersh, *C.I.A. Is Linked to Strikes in Chile That Beset Allende,* N.Y. Times, Sept. 20, 1974, at 1, *available at* http://jfk.hood.edu/Collection/Weisberg%20Subject%20Index%20Files/C%20Disk/CIA%20Chile/Item%20015.pdf (detailing CIA involvement in overthrow of Chilean government); Troy Hooper, *Operation Midnight Climax: How the CIA Dosed S.F. Citizens With LSD,* S.F. Weekly (Mar. 14, 2012), http://www.sfweekly.com/sanfrancisco/operation-midnight-climax-how-the-cia-dosed-sf-citizens-with-lsd/Content?oid=2184385 (detailing the MK-ULTRA program's impact in San Francisco, wherein a CIA covert operation illicitly dosed lysergic acid diethylamide (LSD) on unwitting Americans between 1953-1964, and its public exposure in the 1970s).

56 The eleven-member "Select Committee to Study Government Operations with Respect to Intelligence Activities" was referred to as the "Church Committee" after its chairman, Sen. Frank Church (D-ID). *Rudgers*: *The Church Committee*, *supra* note 55, at 932.

57 *Id*. at 942.

58 *Id*.

59 *See* Nicholas M. Horrock, *Ex-Officials Say F.B.I. Harassed Dr. King to Stop His Criticism,* N.Y.Times, Mar. 9, 1975, at 40, *available at* http://timesmachine.nytimes.com/timesmachine/1975/03/09/84996266.html?pageNumber=40; Beverly Gage, *What an Uncensored Letter to M.L.K. Reveals,* N.Y. Times (Nov. 11, 2014), http://www.nytimes.com/2014/11/16/magazine/what-an-uncensored-letter-to-mlk-reveals.html.

60 The watch list included a Democratic senator, the author John Steinbeck, the Ford and Rockefeller Foundations, and Harvard University. *Rudgers: The Church Committee*, *supra* note 55, at 940.

61 *Id*.

62 The NSA was created by President Truman in 1952 as a continuation of surveillance efforts instituted by the Army Security Agency during World War II. Project Shamrock actually predated the NSA, but was continued by the agency. James Bamford, The Puzzle Palace: Inside the National Security Agency, America's Most Secret Intelligence Organization 302-315 (1st ed., 1983).

63 *Id.* at 459.

64 *Meet the Press: U.S. Senator Frank Church* (NBC News television broadcast Aug. 17, 1975), *available at* https://www.youtube.com/watch?v=YAG1N4a84Dk.

65 Congress also was considering establishing a statutory charter for the FBI. In an effort to stave off these efforts, Attorney General Edward Levi issued guidelines to govern the FBI's domestic intelligence activities based on recommendations from the Church Committee's investigations. The guidelines required a clear criminal nexus as a premise for domestic security investigations, and demanded progressively higher standards and levels of review for more intrusive investigative techniques. The guidelines issued by Levi led to a dramatic reduction in the number of domestic security investigations. However, their strictures have been diluted over time, as successive sets of guidelines have loosened restrictions on FBI operations. *See* Emily Berman, Brennan Ctr. for Justice, Domestic Intelligence: New Powers, New Risks, 10-16 (2011), *available at* https://www.brennancenter.org/sites/default/files/legacy/AGGReportFINALed.pdf .

66 Indeed, lawmakers were so intent on ensuring that FISA Court orders could not be used to spy on purely domestic groups that virtually every committee report on authorization for surveillance of agents of foreign powers included statements that these orders did "not authorize electronic surveillance under any circumstances for the class of individuals included by the Supreme Court within the scope of the *Keith* decision requiring judicial warrants for alleged threats to security of a domestic nature." S. Rep. No. 94-1035, at 22 (1976). *See also* S. Rep. 94-1161, at 18 (1976).

67 S. 3197, 94th Cong. (1976). *See generally* The President's Letter to the Speaker of the House and to the President of the Senate Transmitting Proposed Legislation Concerning the Use of Electronic Surveillance in Obtaining Foreign Intelligence Information, 1 Pub. Papers 793 (Mar. 23, 1976) (supporting introduction of S. 3197); 121 Cong. Rec. S2069 (daily ed. Feb. 19, 1975) (statement of Sen. Gaylord Nelson) (introducing S. 3197 to Senate).

68 S. Rep. 94-1035, at 78 (1976) ("At most *Curtiss-Wright, Waterman* and similar cases merely underline the broad nature of the President's powers to protect the national interest from foreign threats … including the implied power to gather foreign intelligence. But the existence of such powers does not establish "inherent" authority to exercise them in disregard of the fourth amendment."). The Church Committee had also rejected the notion of an inherent authority on the part of the president or intelligence agencies to "break the law" by engaging in activities such as warrantless surveillance. S. Rep. No. 94-755, bk. 2, at 5 (1976).

69 122 Cong. Rec. S3987 (daily ed. Mar. 23, 1976) (statement of Sen. Edward Kennedy) ("…the extent to which surveillance will be authorized to investigate conduct which does not rise to the level of a Federal crime, is a matter of great concern to me and others…"); *Foreign Intelligence Surveillance Act of 1976: Hearing on S. 743, S. 1888, and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary,* 94th Cong. 72 (1976) (statement of Sen. Gaylord Nelson) ("The Government cannot invade an American citizen's privacy without first obtaining a judicial warrant based on probable cause … the 'probable cause' requirement must relate to the commission of a crime."). Sen. Joseph Biden expressed the views of several of his colleagues: "This bill is an attempt to regularize national security electronic surveillance through a statutory warrant procedure. Unfortunately the emphasis in drafting this procedure has been upon the first part of the Fourth Amendment, that is the warrant procedure, and not the second, that there be probable cause that the search will seize particular evidence of specific crimes.… To my mind both parts of the Fourth Amendment are of equal importance. After all it was the abuse of so-called 'General warrants' and 'Writs of assistance' in colonial America and 18th century England which led to the Fourth Amendment." S. Rep. No. 94-1161, at 71-72 (1976).

70 Foreign Intelligence Surveillance Act of 1977, S. 1566, 95th Cong. (1976) (enacted).

71 50 U.S.C. § 1801(f).

72 50 U.S.C. § 1801(a).

73 "U.S. persons" means citizens or legal permanent residents of the United States. 50 U.S.C. § 1801(i).

74 Specifically, U.S. persons qualify as agents of foreign powers if they (i) knowingly engage in clandestine intelligence gathering for a foreign power, which involves or may involve a violation of U.S. criminal statutes; (ii) knowingly engage in "any other clandestine intelligence activities" at the direction of a foreign intelligence service, if the activities involve or are about to involve a violation of U.S. criminal statutes; (iii) knowingly engage in sabotage or terrorism (or preparatory activities) for a foreign power; or (iv) knowingly aid, abet, or conspire with a person to do any of the above. 50 U.S.C. § 1801(b)(2). A fifth category, "knowingly enter the U.S. using a false identity on behalf of a foreign power" was added to this list in 1999. Intelligence Authorization Act for Fiscal Year 2000, Pub. L. No. 106-120, § 601 (codified as amended at 50 U.S.C. § 1801(b)(2)(D)).

75 Foreign Intelligence Surveillance Act of 1977, S. 1566, 95th Cong. § 2521(b)(2)(B) (as introduced May 18, 1977).

76 *Foreign Intelligence Surveillance Act of 1978: Hearing on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence,* 95th Cong. 191 (1978) [hereinafter *1978 FISA Hearing*] (statement of Sen. Birch Bayh, Chairman, S. Select Comm. on Intelligence).

77 Foreign Intelligence Surveillance Act of 1977, S. 1566, 95th Cong. § 2521(b)(2)(B)(i) (emphasis added) (as introduced Mar. 14, 1978). A Senate Intelligence Report from 1978 defines "clandestine intelligence gathering activities" as the "collection or transmission of information or material that is not generally available to the public, or covert contacts with an intelligence service or network by means of 'drops' or other methods characteristic of foreign intelligence operations." It encompasses "activities that fall within the substantive statutory definition of spying," as well as "activities directly related to spying that may constitute violations of laws proscribing the aiding and abetting of spying, such as maintaining a 'safehouse' for secret meetings, servicing 'letter drops' to facilitate covert transmission of instructions or information, recruiting new agents, or infiltrating and exfiltrating agents under deep cover to and from the United States." S. Rep. No. 95-701, at 21-22 (1978) *reprinted in* 1978 U.S.C.C.A.N. 3973, 3990-91. The Senate also clarified that "[l]obbying Congress or seeking to influence public opinion does not become clandestine intelligence activity merely because the agent has failed to comply fully with the Foreign Agents Registration Act." *Id.* at 29. Though these definitions did not carry into the language of the 1978 bill, this remains one of the few existing definitions that attempt to parse the term "clandestine intelligence activities" as it is used in FISA.

78 S. Rep. No. 95-701, at 21 (1978).

79 *1978 FISA Hearing*, *supra* note 76, at 36-37 (statement of Sen. Birch Bayh) ("One of the things that makes me nervous … we use the phrase … 'will involve a criminal violation'. There is no requirement that the violation is about to occur or that it will soon occur…. It seems to me if we say 'will involve' that is sort of some nebulous time length there that could reasonably be interpreted to be will involve crime maybe 10 years from now."); *id.* at 94 (statement of Christopher H. Pyle) ("…The 'will involve' clause permits highly speculative judgments. The predicted violation of the criminal laws that the government suspects 'will' occur may be no more than a technical violation of the extremely vague Foreign Agents Registration Acts … or of the equally vague criminal provisions of the Export Administration Act.").

80 S. Rep. No. 95-604, pt. 1, at 23-24 (1978) ("[T]he word 'involve' … is intended to encompass a violation of federal law which is an integral part of the clandestine intelligence activity even though the clandestine intelligence activity itself might fall between the cracks of the espionage laws…. The phrase 'will involve'… is likewise in no way intended to diminish or dilute the nature of the criminal activity to be established. Its only purpose is to permit electronic surveillance at some point prior to the time when the actual crime sought to be prevented … actually occurs."). This understanding remained even after "will involve" was changed in the legislative drafting process to "may involve." S. 1566, 95th Cong. § 2521(b)(2)(B) (1978) (enacted). The change was meant to address situations where the government did not have sufficient knowledge to establish that a crime was involved or what specific crime was being committed. An example of such a situation is when federal agents witnessed meetings between a foreign intelligence officer and an American who might have access to classified information but were unable to determine what information was transmitted. In contrast, the Committee made clear that in a case where an informant claimed a target was under "deep cover" for several years before commencing espionage activities, this would not have provided the requisite justification under "may involve" to warrant surveillance for the period of "deep cover." Legislators recognized that the formulation could be interpreted as allowing long-term surveillance, but made clear that this was not the intention. S. Rep. No. 95-701, at 23 (1978) ("The committee recognizes that an argument can be made that a person could be surveilled for an inordinate period of time. That is clearly not the intention.").

81 S. Rep. No. 94-1161, at 18 (1976) ("In no event may mere sympathy for, or identity of interest with, the goals of a foreign group or government be sufficient.").

82 S. Rep. No. 95-604, pt. 1, at 29 (1977) ("An illustration of the 'knowing' requirement is provided by the case of Dr. Martin Luther King. Dr. King was subjected to electronic surveillance on 'national security grounds' when he continued to associate with two advisers whom the Government had apprised him were suspected of being American Communist party members and, by implication, agents of a foreign power. Dr. King's mere continued association and consultation with those advisers … would clearly not have been a sufficient basis under this bill to target Dr. King as the subject of electronic surveillance."); S. Rep. No. 95-701, at 28 (1978) (also discussing the unwarranted surveillance of Dr. King).

83 S. Rep. No. 95-701, at 27-28 (1978) ("This (knowing) standard requires the Government to establish probable cause that the prospective target knows both that the person with whom he is conspiring or whom he is aiding or abetting is engaged in the described activities as an agent of a foreign power and that his own conduct is assisting or furthering such activities. The innocent dupe who unwittingly aids a foreign intelligence officer cannot be targeted under this provision.").

84 *Id*. at 28. The Senate Committee report explained as follows: "For example, the advocacy of violence falling short of incitement is protected by the first amendment, under the Supreme Court's decision in *Brandenburg* v. *Ohio*, 395 U.S. 444 (1969). Therefore, the pure advocacy of the commission of terrorist acts would not, in and of itself, be sufficient to estabilsh [sic] probable cause that an individual may be preparing for the commission of such acts." *Id*.

85 *Foreign Intelligence Surveillance Act of 1976: Hearing on S. 743, S. 1888 and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary,* 94th Cong. 77 (1976) (statement of Sen. Gaylord Nelson).

86 For example, in a January 1978 hearing before a House Intelligence Subcommittee, the Department of Defense's Deputy Under Secretary for Policy testified against the use of either "essential" or "necessary" in the definition of foreign intelligence, arguing that "frequently what you are going after is a very small piece which in itself, certainly isn't essential or necessary to national security, but in the context of other intelligence, or with the history of that same kind of a surveillance, can well be essential or necessary." *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. 63 (1978) (statement of Adm. Daniel J. Murphy, Deputy Under Secretary for Policy, Dep't of Def.).

87 The Senate Committee (which had proposed tightening the definition by using "essential" instead of "relevant") took the view that the revised definition "would therefore not include information about the views or planned statements or activities of Members of Congress, executive branch officials, or private citizens concerning the foreign affairs of the United States." S. Rep. No. 95-604, pt. 1, at 30-31 (1977). The formulation was intended to "require a showing that the information is both important and required," not simply "useful or convenient." H.R. Rep. No. 95-1283, at 47 (1978).

88 H.R. Rep. No. 95-1283, at 47 (1978) (emphasis added).

89 Foreign Intelligence Surveillance Act of 1978, *supra* note 2, at § 101(e)(2) (codified at 50 U.S.C. § 1801(e)(2)).

90 *Compare* 50 U.S.C. § 1805 (FISA Court orders) *with* 18 U.S.C. § 2518 (Title III orders).

91 18 U.S.C. § 2518(3)(a).

92 50 U.S.C. § 1805(a)(2)(A) (relying on the definition of "agent of a foreign power" detailed in 50 U.S.C. §1801(2)(A)).

93 *See supra* text accompanying notes 16-19.

94 Glenn Greenwald & Murtaza Hussein, *Meet the Muslim-American Leaders the FBI and NSA Have Been Spying On*, The Intercept (July 9, 2014), https://firstlook.org/theintercept/2014/07/09/under-surveillance/.

95 18 U.S.C. § 2518(3)(b).

96 50 U.S.C. § 1804(a)(3)(B).

97 50 U.S.C. § 1805(a)(4).

98 H. R. Rep. No. 95-1283, at 80 (1978).

99 18 U.S.C. § 2518(8)(d).

100 50 U.S.C. § 1806(c).

101 *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. Times (July 15, 2013), http://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html?pagewanted=all; Charlie Savage, *Door May Open for Challenge to Secret Wiretaps,* N.Y. Times (Oct. 16, 2013), http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?pagewanted=all.

102 *How Phones Work: The Basic Science Behind Telephony,* Telecomm. Hist. Grp., Inc. (last visited Jan. 21, 2015), http://www.telcomhistory.org/vm/sciencePhonesWork.shtml ("From the beginning (or nearly the beginning) [of telephony], copper wire has been the carrier of choice.").

103 U.S. Office of Tech. Assessment, OTA-ISC-239, International Cooperation and Competition in Civilian Space Activities 147 (1985), *available at* http://govinfo.library.unt.edu/ota/Ota_4/DATA/1985/8513.PDF ("Approximately two-thirds of trans-oceanic international telecommunications now [in 1985] pass through satellites; the remainder is carried via undersea cables.").

104 Tom Harris, *How Wiretapping Works,* How Stuff Works (May 8, 2001), http://people.howstuffworks.com/wiretapping.htm.

105 *See generally* Whitfield Diffie & Susan Landau, Privacy on the Line 95-103 (updated and expanded ed. 2007); Eur. Parl. Doc. (COM 264) 30-35 (2001), *available at* http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&language=EN&format=PDF.

106 Chenda Ngak, *Cell Phone Turns 40: Martin Cooper's First Call on the DynaTAC,* C.B.S. News (Apr. 4, 2013, 5:02 PM), http://www.cbsnews.com/news/cell-phone-turns-40-martin-coopers-first-call-on-the-dynatac/.

107 *Exhibits Online: Internet History 1962 to 1992,* Computer History Museum (last visited Dec. 15, 2014), http://www.computerhistory.org/internet_history/index.html.

108 Preston Gralla, How the Internet Works 13-14 (8th ed. 1999); Thomas B. Allen, *The Future Is Calling*, 200 Nat'l Geographic 76 (2001).

109 *See, e.g.*, Craig Timberg & Ellen Nakashima, *Agreements with Private Companies Protect U.S. Access to Cables' Data for Surveillance,* Wash. Post (July 6, 2013), http://wapo.st/180jsn9.

110 *See* Orin S. Kerr, *Updating the Foreign Intelligence Surveillance Act*, 75 U. Chi. L. Rev. 225, 234-35 (2008); David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 4 (Brookings Inst., Working Paper, 2007) [hereinafter *Kris Working Paper*], *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.pdf.

111 Linda Blake & Jim Lande, FCC, Trends in the U.S. International Telecommunications Industry tbl. 4 (1998) (showing 2,732,000,000 total international call minutes in the U.S. in 1980).

112 FCC, 2011 International Telecommunications Data tbl. A4 (2013) (showing 89,591,887,346 total international call minutes in the U.S. in 2011).

113 Justin Levenstein, The Radicati Grp., Email Statistics Report, 2013-2017 4 (2014), *available at* http://www.radicati.com/wp/wp-content/uploads/2013/04/Email-Statistics-Report-2013-2017-Executive-Summary.pdf.

114 Audrey Singer, *Contemporary Immigrant Gateways in Historical Perspective*, Daedalus, Summer 2013, at 79, *available at* http://www.brookings.edu/~/media/research/files/articles/2013/09/05%20immigrant%20gateways%20singer/singer%20immigration%20article%209513.pdf.

115 A 1978 Boston Globe article estimated 1.5 million Americans living abroad and 23 million American tourists traveling overseas annually. Raymond M. Lane, *The Problem No One Likes to Think About,* Bos. Globe, Aug. 27, 1978, at B11. A 2013 State Department estimate puts those numbers at 6.8 million American citizens living abroad and over 65 million Americans traveling abroad annually. Bureau of Consular Affairs, U.S. Dept. of State, Who We Are and What We Do: Consular Affairs by the Numbers (2013), *available at* http://travel.state.gov/content/dam/ca_fact_sheet.pdf.

116 Press Release, Instit. of Int'l Educ., Open Doors 2013: International Students in the United States and Study Abroad by American Students Are at All-Time High (Nov. 11, 2013), *available at* http://www.iie.org/Who-We-Are/News-and-Events/Press-Center/Press-Releases/2013/2013-11-11-Open-Doors-Data.

117 [REDACTED], 2011 WL 10945618, at *10 (FISA Ct. Oct. 3, 2011) [hereinafter 2011Bates Decision].

118 *Id.* at *11.

119 Patriot Act, *supra* note 1.

120 Congress included a sunset for the bill's major surveillance provisions to ensure that the legislation would be revisited in less chaotic times. *Id.* § 224.

121 Intelligence Authorization Act for 1999, § 602, Pub. L. No. 105-272, 112 Stat. 2411 (1998) (current version at 50 U.S.C. § 1861).

122 50 U.S.C. § 1861(b)(2)(A). In addition, if directed at a U.S. person, the investigation could not be based solely on that person's First Amendment activities. 50 U.S.C. § 1861(a)(1).

123 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.

124 Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls,* USA Today (May 11, 2006, 10:38 AM), http://usatoday30.usatoday.com/news/washington/2006-05-10-nsa_x.htm; James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts,* N.Y. Times (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=1&.

125 [REDACTED], No. PR/TT [REDACTED], at (FISA Ct. REDACTED), *available at* http://www.dni.gov/files/documents/1118/CLEANEDPRTT%201.pdf.

126 Justice Department officials' discomfort with the original version of the program led to the infamous show-down between White House officials and James Comey, who was serving as Acting Attorney General while Attorney General John Ashcroft was suffering from pancreatitis, in Ashcroft's hospital room. Barton W. Gellman, Angler: The Cheney Vice-Presidency 294-97 (1st ed. 2008).

127 Office of the Director of National Intelligence, *DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act,* IC on the Record (Nov. 18, 2013), http://icontherecord.tumblr.com/post/67419963949/dni-clapper-declassifies-additional-intelligence.

128 *In re* Application of the Fed. Bureau of Investigation for an Order Requiring the Production of Tangible Things from [REDACTED], No. BR 13-109, at 18-23 (FISA Ct. 2013) [hereinafter 2013 FISA Ct. Opinion], *available at* http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

129 *Id.* at 20.

130 *Id.* at 22.

131 *Id.* at 5.

132 *In re* Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, No. BR 14-01 6-9 (FISA Ct. Feb. 5, 2014), *available at* http://www.uscourts.gov/uscourts/courts/fisc/br14-01-order.pdf; Joint Statement by Attorney General Eric Holder and Director of National Intelligence James Clapper on the Declassification of Additional Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Feb. 12, 2014), *available at* http://www.justice.gov/opa/pr/joint-statement-attorney-general-eric-holder-and-director-national-intelligence-james-clapp-0.

133 Patriot Act, *supra* note 1, at § 218 (codified as amended at 50 U.S.C §§ 1804(a)(6)(B), 1823(a)(6)(B)).

134 *Id.* § 504, 50 U.S.C. § 1806(k)(1).

135 United States v. Truong Dinh Hung, 629 F.2d 908, 915-16 (4th Cir. 1980).

136 Memorandum Re: Instructions on Separation of Certain Foreign Counterintelligence and Criminal Investigations, from Jamie S. Gorelick, Deputy Att'y Gen., to Mary Jo White, U.S. Att'y, S.D.N.Y., Louis Freeh, Dir., FBI., & Richard Scruggs, Counsel, Office of Intelligence Policy and Review (1995), *available at* http://fas.org/irp/agency/doj/1995_wall.pdf; Memorandum Re: Procedures for Contracts Between the FBI and the Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations, from Janet Reno, Att'y Gen., to Asst. Att'y Gen., Criminal Div., Dir. FBI., Counsel for Intelligence Police, U.S. Att'ys (July 19, 1995) [hereinafter Reno Memo], *available at* http://fas.org/irp/agency/doj/fisa/1995procs.html; Memorandum to Recommend that the Att'y Gen. Authorize Certain Measures Regarding Intelligence Matters in Response to Recommendations provided by Special Litigation Counsel Randy Bellows, from Gary G. Grindler, Principal Assoc. Deputy Att'y Gen. & Jonathan D. Schwartz, Assoc. Deputy Att'y Gen., to Att'y Gen. (Jan. 18, 2000), *available at* http://fas.org/irp/agency/doj/fisa/ag012100.html; Memorandum Re: Intelligence Sharing, from Larry D. Thompson, U.S. Dept. of Justice, to Criminal Division, Office of Intelligence Policy and Review, and FBI. (August 6, 2001), *available at* http://fas.org/irp/agency/doj/fisa/dag080601.html.

137 *In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp.2d 611, 619 (FISA Ct. 2002) [hereinafter 2002 FISA Ct. Opinion], *rev'd, In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002). The procedures also allowed the Criminal Division to give guidance to intelligence investigators aimed at preserving the option of criminal prosecution and required the FBI to provide certain reports on FISA investigations to the Criminal Division. *Id.*

138 Reno Memo, *supra* note 136. To ensure compliance with these requirements, attorneys from the Justice Department's Office of Intelligence Policy and Review (OIPR) were invited to meetings between intelligence and law enforcement officials — what the government called the "chaperone" requirement. *In re* Sealed Case, 310 F.3d 717, 720 (FISA Ct. Rev. 2002).

139 2002 FISA Ct. Opinion, *supra* note 137, at 619.

140 *Id.*

141 Randy L. Bellows, U.S. Dept. of Justice, Attorney General's Review Team On The Handling Of The Los Alamos National Laboratory Investigation 721-34 (2000) [hereinafter Bellows Report], *available at* http://www.justice.gov/ag/attorney-generals-foia-reading-room-records-bellows-report.

142 U.S. Gen. Accounting Office, GAO-01-780, FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited 3 (2001).

143 *See generally* Jerome P. Bjelopera, Cong. Research Serv., R41780, The Federal Bureau of Investigation and Terrorism Investigations (2013).

144 Patriot Act, *supra* note 1, at § 218, 504 (codified as amended at 50 U.S.C §§ 1804(a)(6)(B), 1806(k)(1), 1823(a)(6)(B)).

145 *See* Nat'l Comm'n on Terrorist Attacks Upon the U.S., The 9/11 Commission Report 266-72 (2004). On the few occasions in which an analyst believed "the wall" prevented her from sharing information, the 9/11 Commission concluded that "she appears to have misunderstood the complex rules that could apply to this situation," and that no actual such barrier existed. *Id.* at 271. *See also* James Bamford, The Shadow Factory 18-20 (First Anchor Books 2009) (2008) (describing one instance in which the CIA failed to share critical information about the hijackers with the FBI because of a turf battle between the two organizations).

146 The FISA Court held that some of these limitations were required, not by the "primary purpose" test, but by FISA's minimization procedures; the FISA Court of Appeals reversed. *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp.2d 611, 623 (FISA Ct. 2002), *rev'd, In re* Sealed Case, 310 F. 3d 717, 731 (FISA Ct. Rev. 2002).

147 Bellows Report, *supra* note 141, at 712.

148 Nat'l Comm'n on Terrorist Attacks Upon the U.S., *supra* note 145, at 79 (noting that the use of the term "the wall" to describe the Justice Department's procedures is "misleading," and that lack of coordination occurred because these procedures "were almost immediately misunderstood and misapplied"); Kris & Wilson Treatise, *supra* note 5, at § 10.8 (describing the development of Department of Justice FISA coordination procedures in 1995 and how interpretations of these procedures limited coordination).

149 Offices of the Inspectors Gen. of the Dep't of Defense, Dep't of Justice, Cent. Intelligence Agency, Nat'l Sec. Agency & Office of the Director of Nat'l Intelligence, No. 2009-0013-AS, Unclassified Report on the President's Surveillance Program 1, 6 (2009), *available at* http://www.justice.gov/oig/special/s0907.pdf.

150 The 2009 report issued by several Inspectors General makes clear that the TSP was only one of many special surveillance programs initiated under a claim of presidential authority. *Id.* at 6. It is unknown how many of these other programs remain classified and/or undisclosed; accordingly, the extent of warrantless surveillance undertaken after 9/11 is still unknown.

151 Dep't of Justice, Legal Authorities Supporting the Activities of the National Security Agency Described by the President 7-10 (2006), *available at* https://www.epic.org/privacy/terrorism/fisa/doj11906wp.pdf.

152 For a brief period, the FISA Court agreed to authorize the surveillance under existing authorities, *In re* Various Known and Unkown Agents of [REDACTED] Presumed United States Persons, at 7 (FISA Ct. Jan. 10, 2007), *available at* http://www.dni.gov/files/documents/1212/FISC%20Order%2001%2010%2007%20-%2012-11%20-%20Redacted.pdf, but in 2007, a judge refused to renew this authorization. *In Re* [REDACTED], at 20 (FISA Ct. Apr. 3, 2007), *available at* http://www.dni.gov/files/documents/1212/CERTIFIED%20COPY%20-%20Order%20and%20Memorandum%20Opinion%2004%2003%2007%2012-11%20Redacted.pdf

153 *See, e.g.*, *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary*, 110th Cong. 8 (2007) (statement of Michael J. McConnell, Director, Office of National Intelligence); *FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 18 (2012) (statement of Kenneth Wainstein, Partner, Cadwalder, Wickersham & Taft LLP).

154 *Kris Working Paper*, *supra* note 110, at 4.

155 In 1976, Attorney General Edward Levi, testifying in favor of a predecessor bill, hinted that there was a "sweeping" NSA operation to intercept international radio communications. *Foreign Intelligence Surveillance Act of 1976: Hearings on S. 743, S. 1888 and S. 3197 Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary,* 94th Cong. 15 (1976). *See also Foreign Intelligence Surveillance Act: Hearings Before the Subcomm. on Courts, Civil Liberties, & the Admin. of Justice of the H. Comm. on the Judiciary,* 94th Cong. 98-99 (1976). Developing legislation to regulate this program, he noted, would be a complex and difficult undertaking. *Electronic Surveillance Within the United States for Foreign Intelligence Purposes: Hearing on S. 3197 Before the Subcomm. on Intelligence and the Rights of Ams. of the S. Comm. on Intelligence,* 94th Cong. 80 (1976). Congress ultimately chose to leave the resolution of these complexities to another day, rather than hold the rest of FISA hostage. The committee reports on the final legislation, however, indicated that Congress was "concerned" about the matter and thought it would be "desirable" to develop further legislation. S. Rep. No. 95-701, at 34 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4003; S. Rep. No. 95-604, pt. 1, at 34 (1978). The Attorney General pledged to assist. *Foreign Intelligence Surveillance Act of 1978: Hearing on S. 1566 Before the Subcomm. on Intelligence and the Rights of Ams. of the S. Select Comm. on Intelligence*, 95th Cong. 16 (1977); *Foreign Intelligence Surveillance Act: 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. 12 (1978).

156 S. Rep. No. 95-701, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004.

157 *FISA Amendments Act of 2008: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Sec. of the H. Comm. on the Judiciary*, 112th Cong. 1 (2012) (statement of Rep. F. James Sensenbrenner, Jr., Chairman, Subcomm. on Crime, Terrorism, and Homeland Sec.).

158 As discussed previously, FISA regulates three basic types of surveillance: wiretapping, the interception of radio communications, and the "monitoring" of information through other electronic means — which, in 1978, referred primarily to bugging. Although e-mails may be captured in transit by wiretapping or (for e-mails sent wirelessly) interception of radio signals, once they are stored on a server, their acquisition is considered "monitoring." Because FISA regulates "monitoring" within the U.S. regardless of the nationality of the target, stored foreign-to-foreign e-mails come within its ambit. Kris & Wilson Treatise, *supra* note 5, at §§ 7.27, 16.6.

159 The government has argued that there is no perfectly tailored way to accomplish such a solution, as it lacks any reliable way to sort foreign-to-foreign e-mails from other types of e-mails. *Strengthening FISA: Does the Protect America Act Protect Americans' Civil Liberties and Enhance Security?: Hearing Before the S. Comm. on the Judiciary,* 110th Cong. (2007) (written statement of James Baker, former Counsel for Intelligence Policy, Dep't of Justice), *available at* http://www.judiciary.senate.gov/imo/media/doc/Baker%20Testimony%20092507.pdf. Even so, the solution that the government sought in 2007 was far broader than necessary. Rather than dispensing with a warrant requirement for any type of surveillance targeting non-U.S. persons, the government could have proposed allowing programmatic collection of stored e-mails using the best procedures available to try to target foreign-to-foreign communications, coupled with strict minimization requirements for the incidentally-collected international and wholly domestic e-mails.

160 Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (2007) (expired 2008).

161 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2435 (2008) [hereinafter FAA].

162 *Id.* at § 101(a)(2) (codified as amended at 50 U.S.C. § 1881a) (creating Section 702 of FISA).

163 *See supra* Part III.B.2.

164 50 U.S.C. §§ 1881a(d)(1)(A), 1881a(e)(1), 1801(h)(1).

165 50 U.S.C. § 1881a(b)(2).

166 *See, e.g.*, *FISA Amendments Act Reauthorization: Hearing Before the H. Permanent Select Comm. on Intelligence,* 112th Cong. 8 (2011), *available at* http://www.dni.gov/files/documents/Joint%20Statement%20FAA%20Reauthorization%20Hearing%20-%20December%202011.pdf (joint statement of Lisa O. Monaco, Ass't Att'y Gen., Nat'l Sec. Div., Dep't of Justice, et al.); Privacy and Civil Liberties Oversight Bd., Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act 11 (2014) [hereinafter PCLOB 702 Report], *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/1211947/pclob-section-702-report-pre-release.pdf; Barack Obama, President, Address at the U.S. Department of Justice (Jan. 17, 2014), *available at* http://wapo.st/1mgJ3wk.

167 *See, e.g., FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary,* 109th Cong. 9 (2006), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-109shrg43453/pdf/CHRG-109shrg43453.pdf (statement of Michael Hayden, Director, Nat'l Sec. Agency) ("[W]hy should our laws make it more difficult to target the al Qaeda communications that are most important to us—those entering or leaving this country."); *see also* Transcript of Privacy and Civil Liberties Oversight Board Public Workshop, Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act 109 (July 9, 2013), *available at* http://www.pclob.gov/library/20130709-Transcript.pdf (statement of Steven G. Bradbury, Former Principal Deputy Ass't Att'y Gen., Dep't of Justice Office) ("But it is particularly focused on communications in and out of the United States because . . . those are the most important communications you want to know about if you're talking about a foreign terrorist suspect communicating to somebody you don't know inside the United States."). Indeed, when seeking these authorities from the FISA Court — unsuccessfully, which is why the executive branch turned to Congress — officials described the purpose of the program as "establishing an early warning system . . . to alert the U.S. Government to the presence of members and agents of these foreign powers and to aid in tracking such individuals *within the United States*." Memorandum of Law in Support of Application for Authority to Conduct Electronic Surveillance of [REDACTED] at 2, *In Re* [REDACTED], No. [REDACTED] (FISA Ct. Dec 13, 2006) (emphasis added), *available at* http://www.dni.gov/files/documents/1212/Memo%20of%20Law%20as%20filed%2012%2013%202006%20-%2012-11%20Redacted.pdf.

168 *See, e.g.,* Statement of James R. Clapper, Director of National Intelligence, DNI Statement on Activities Authorized Under Section 702 of FISA (June 6, 2013), *available at* http://www.dni.gov/index.php/newsroom/press-releases/191-press-releases-2013/869-dni-statement-on-activities-authorized-under-section-702-of-fisa ("Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States. It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States."); Interview by Charlie Rose with President Barack Obama (June 16, 2013), *available at* http://www.charlierose.com/watch/60230424 (President Barack Obama stated: "if you are a U.S. person, the NSA cannot listen to your telephone calls, and the NSA cannot target your emails … and have [sic] not").

169 Letter from I. Charles McCullough, III, Inspector Gen., U.S. Intelligence Cmty., to Sen. Ron Wyden & Sen. Mark Udall 1 (June 15, 2012), *available at* http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

170 2011 Bates Decision, *supra* note 117, at *9.

171 *See generally* Barton Gellman et al., *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, Wash. Post (July 5, 2014), http://wapo.st/1xyyGZF.

172 2011 Bates Decision, *supra* note 117, at *11.

173 *See supra* Part II.C.2.

174 50 U.S.C. § 1881a(i)(3)(A). After submitting proposed procedures to the court, the government need not wait for the court's approval before moving forward with surveillance, and if the court ultimately finds the procedures to be legally deficient, the government may keep all the information it improperly collected in the interim period. An amendment offered by Senator Feingold to impose certain limits on the use of such improperly collected information was defeated by a vote of 40-56. *The U.S. Congress Votes Database: S 2248,* Wash. Post (Feb. 7, 2008), http://projects.washingtonpost.com/congress/110/senate/2/votes/11/.

175 50 U.S.C. § 1881a(g)(2)(A).

176 Exec. Order No. 12,333, 3 C.F.R. 200 (1981).

177 An ACLU Freedom of Information Act request brought to light an internal surveillance manual from 2007, which describes EO 12333 as "the primary source of NSA's foreign intelligence-gathering authority." Nat'l Sec. Agency, Overview of Signals Intelligence Lessons 1-4 4 (Jan. 8, 2007) (released to ACLU in FOIA Case #70809), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Overview%20of%20Signals%20Intelligence%20Authorities.pdf; *see generally* Nat'l Sec. Agency, Legal Fact Sheet: Executive Order 12333 (Jun. 19, 2013) (released to ACLU in FOIA Case #70809), *available at* https://www.aclu.org/files/assets/eo12333/NSA/Legal%20Fact%20Sheet%20Executive%20Order%2012333.pdf.

178 Office of the Director of National Intelligence, *2013 Transparency Report: Statistical Transparency Report Regarding Use of National Security Authorities - Annual Statistics for Calendar Year 2013*, IC on the Record (June 26, 2014), http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2013 [hereinafter *2013 Transparency Report*] (estimating that 89,138 "targets" were affected by section 702 in 2013); 2011 Bates Decision, *supra* note 117, at *9 (noting that more than 250 million internet communications are obtained by the NSA under section 702 each year).

179 2013 FISA Ct. Opinion, *supra* note 128, at 2-3.

180 Massachusetts v. E.P.A., 549 U.S. 497, 516 (2007) (quoting Flast v. Cohen, 392 U.S. 83, 95 (1968)) (internal quotation marks omitted).

181 OLC Memo, *supra* note 12, at 26. *See also supra* text accompanying notes 18-19.

182 OLC Memo, *supra* note 12, at 28.

183 *Id.* at 29.

184 Transcript of Privacy and Civil Liberties Oversight Board Public Workshop, *supra* note 167, at 35 (statement of James Robertson, former U.S. D. J. who served on the FISA Ct.).

185 *Id*. at 36.

186 *Id.*

187 2013 FISA Ct. Opinion, *supra* note 128, at 4.

188 The Patriot Act's changes to business records collection undermined the adversarial process in another way. Until then, the government's applications to obtain business records had to identify the subject of the records and demonstrate that the subject was a foreign power or its agent. The Patriot Act dispensed with these requirements, replacing them with a requirement that the records be relevant to an authorized investigation. By untethering the government's request from a particular subject or target, this change arguably eviscerated the "adversity in fact" — the existence of specific parties with adverse interests — that Article III requires. For more on this aspect of the Article III adversity requirement, see Marty Lederman & Steve Vladeck, *The Constitutionality of a FISA "Special Advocate"*, Just Security (Nov. 4, 2013, 1:34 PM), http://justsecurity.org/2873/fisa-special-advocate-constitution/ and Steve Vladeck, *Why a "Drone Court" Won't Work—But (Nominal) Damages Might…*, Lawfare (Feb. 10, 2013, 5:12 PM), http://www.lawfareblog.com/2013/02/why-a-drone-court-wont-work/.

189 2013 FISA Ct. Opinion, *supra* note 128. Similarly, it was not until December 2008 — two years after the FISA Court approved bulk collection under Section 215 — that the court considered the fundamental question of whether the program could be squared with the limitations contained in the Stored Communications Act. *See In Re* Production of Tangible Things from [REDACTED], No. BR 08-13 (FISA Ct. Dec 12, 2008), *available at* http://www.fas.org/irp/agency/doj/fisa/fisc-121208.pdf.

190 Alderman v. United States, 394 U.S. 165, 184 (1969).

191 *See* United Pub. Workers of Am. v. Mitchell, 330 U.S. 75, 89 (1947) ("For adjudication of constitutional issues 'concrete legal issues, presented in actual cases, not abstractions' are requisite."); *see also* Colon v. Howard, 215 F. 3d 227, 235 (2d Cir. 2000) (Walker, J., concurring) (noting that the judiciary "is entitled to decide constitutional issues only when the facts of a particular case require their resolution for a just adjudication on the merits") (quoting Desist v. United States, 394 U.S. 244, 258 (1969) (Harlan, J., dissenting)).

192 For instance, pre-enforcement challenges — which contest an application of the law that has not yet occurred — are often deemed non-justiciable because courts "possess no factual record of an actual or imminent application of [the law] sufficient to present the constitutional issues in 'clean-cut and concrete form.'" Renne v. Geary, 501 U.S. 313, 321-22 (1991) (quoting Rescue Army v. City of Los Angeles, 331 U.S. 549, 584 (1947)). The Supreme Court has recognized that judicial review "is likely to stand on a much surer footing in the context of a specific application of [the challenged] regulation than could be the case in the framework of the generalized challenge" made in a pre-enforcement context. Toilet Goods Ass'n v. Gardner, 387 U.S. 158, 164 (1967). Similarly, when potential defendants seek a declaratory judgment to clarify their rights or obligations under the law before taking action, courts must take care to ensure that they are not engaging in a "determination of abstract questions." Ashwander v. Tenn. Valley Auth., 297 U.S. 288, 324 (1936). The Supreme Court thus deemed it inappropriate to adjudicate the constitutionality of a law prohibiting executive branch employees from taking part in political campaigns, when the court could "only speculate as to the kinds of political activity the appellants desire to engage in or as to the contents of their proposed public statements or the circumstances of their publication." United Pub. Workers of Am. v. Mitchell, 330 U.S. 75, 89 (1947). The Second Circuit cited *Mitchell* in refusing to issue a declaratory judgment on whether an obscenity law could constitutionally be applied against a theater that hosted nude dance exhibitions. Noting that the dances could vary from performance to performance, the court reasoned that the First Amendment values asserted could not be "properly balance[d] … without further factual specificity and concreteness." F.X. Maltz, Ltd. v. Morgenthau, 556 F.2d 123, 125 (2d Cir. 1977).

193 OLC Memo, *supra* note 12, at 28. Courts similarly upheld the constitutionality of the FISA procedure against Article III challenges on the ground that FISA applications "involve concrete questions respecting the application of the Act" and thus may be analogized to warrants. United States v. Megahey, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982). *See also* United States v. Duggan, 743 F.2d 59, 70-71 (2d Cir. 1984).

194 50 U.S.C. § 1881a(i)(3)(A).

195 Sabri v. United States, 541 U.S. 600, 608-09 (2004); *see also* United States v. Raines, 362 U.S. 17, 22 (1960) (arguing that exercising judicial restraint in a facial challenge "frees the Court . . . from premature interpretations of statutes in areas where constitutional application might be cloudy").

196 United States v. Salerno, 481 U.S. 739, 745 (1987).

197 *See, e.g.*, Washington State Grange v. Washington State Republican Party, 552 U.S. 442, 457-458 (2008); Gonzales v. Carhart, 550 U.S. 124, 167-168 (2007).

198 *See, e..g.,* United States v. Martinez-Fuerte, 428 U.S. 543, 559 (1976) (observing, in upholding checkpoints near the border to check for immigration papers, that "a claim that a particular exercise of discretion in locating or operating a checkpoint is unreasonable is subject to post-stop judicial review").

199 After all, ordinary criminal wiretaps under Title III, like electronic surveillance activities under FISA, require the government to "minimize" the interception of communications not otherwise subject to interception. 18 U.S.C. § 2518(5). In the Title III context, however, there is no generalized court review of minimization procedures analogous to the FISA Court's review — presumably because such review may occur on a case-by-case basis. *See, e.g.*, United States v. Hoffman, 832 F.2d 1299, 1307 (1st Cir. 1987); United States v. Lopez, 300 F.3d 46, 57 (1st Cir. 2002); United States v. Bennett, 219 F.3d 1117, 1123-24 (9th Cir. 2000).

200 Massachusetts v. E.P.A., 549 U.S. 497, 516 (2007) (quoting Flast v. Cohen, 392 U.S. 83, 95 (1968)).

201 Eric. H. Holder, Jr., U.S Dep't of Justice, Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended 1-2 (2009) (emphasis added), *available at* https://s3.amazonaws.com/s3.documentcloud.org/documents/716633/exhibit-a.pdf.

202 50 U.S.C. § 1810.

203 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1140 (2013); ACLU v. NSA, 493 F.3d 644, 648 (6th Cir. 2007). Moreover, the Ninth Circuit Court of Appeals has held that this provision is not a waiver of sovereign immunity and thus authorizes lawsuits against private parties but not the government. Al-Haramain Islamic Found., Inc. v. Obama, 705 F.3d 845, 848 (9th Cir. 2012).

204 50 U.S.C. §§ 1806(c), 1806(e), 1881e(a).

205 *See* Brief for Appellant at Argument II.3, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (quoting H.R Rep. 95-1283, at 24 n.14 (1978)), *available at* http://www2.gwu.edu/~nsarchiv/NSAEBB/NSAEBB178/surv23.pdf ("[T]he 1978 legislative history [of FISA] correctly predicts that 'prosecution is rarely the objective or the result' of FISA surveillance . . ..").

206 Charlie Savage, *Door May Open for Challenge to Secret Wiretaps,* N.Y. Times (Oct. 16, 2013), *available at* http://www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html?_r=2&.

207 *See, e.g.,* John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover up Program Used to Investigate Americans*, Reuters (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/2013/08/05/us-dea-sod-idUSBRE97409R20130805.

208 50 U.S.C. § 1806(f); *see also* United States v. Daoud, 761 F.3d 678, 678 (7th Cir. 2014) (reversing district court's decision ordering the government to provide defense counsel with the materials on which the FISA application was based).

209 50 U.S.C. §§ 1803(e), 1881a(h)(4).

210 Spencer Ackerman, *FISA Court: No Telecoms Company Has Ever Challenged Phone Records Orders*, Guardian (Sept 17, 2013, 6:29 PM), http://www.theguardian.com/law/2013/sep/17/fisa-court-bulk-phone-records-collection. In 2010, Sprint threatened to bring a challenge if the government did not share its legal rationale for the program, but after the government shared the documents, Sprint agreed to provide the records. *See* Ellen Nakashima, *U.S. Revealed Secret Legal Basis for NSA Program to Sprint, Declassified Files Show,* Wash. Post (May 14, 2014), http://wapo.st/1sOPUj4. After the bulk collection program was revealed and one district court judge ruled it unconstitutional, Verizon, having received its periodic production order issued by the FISA Court, filed a motion with the FISA Court asking whether it had considered the district court opinion. Verizon did not challenge the order, however (although some reports described its motion as a "challenge"). *See* Evan Hill, *Telecom Firm Fails in First Known FISA Court Surveillance Challenge,* Al Jazeera Am. (Apr. 25, 2014, 6:30 PM), http://america.aljazeera.com/articles/2014/4/25/only-telecom-to-challengesurveillancefailsinfisacourt.html.

211 Conor Friedersdorf, *FISA Court Orders Are Rarely Challenged, Presiding Judge Says*, Atlantic (July 30, 2013, 8:09 AM), http://www.theatlantic.com/politics/archive/2013/07/fisa-court-orders-are-rarely-challenged-presiding-judge-says/278200/.

212 *See* Jennifer Granick, *FISA Amendments Act Is Way Worse for Privacy than Title III*, Center for Internet and Society (Nov 13, 2012, 2:35 PM), http://cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-way-worse-privacy-title-iii (comparing minimization requirements); Brief for Appellant at Argument I, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (noting that "FISA's minimization standards are more generous than those in Title III").

213 *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008). The challenge was brought by a communications service provider.

214 Camara v. Municipal Court of S.F., 387 U.S. 523, 534-37 (1967).

215 New Jersey v. T.L.O., 469 U.S. 325, 326 (1985).

216 Griffin v. Wisconsin, 483 U.S. 868, 868 (1987).

217 Skinner v. Railway Labor Executives' Assoc., 489 U.S. 602, 602 (1989); *see also* National Treasury Employees Union v. Von Rabb, 489 U.S. 656, 671 (1989).

218 *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1011 (FISA Ct. Rev. 2008).

219 The FISA Appeals Court used the "totality of circumstances" test articulated by the Supreme Court for cases in which warrants are not required. *Id.* at 1012.

220 *Id.*

221 *Id.* at 1016.

222 New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring) (noting that a warrant may not be required when "special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable").

223 United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980) (quoting United States v. United States District Court, 407 U.S. 297, 315 (1972)) (holding that a warrant requirement would "unduly frustrate" the president's exercise of his foreign affairs authority).

224 *See supra* text accompanying note 40.

225 Zweibon v. Mitchell, 516 F.2d 594, 642 (1975). Two other arguments put forward by the government were not directly relevant to the issue of whether a warrant was impracticable. First, the argument that foreign security wiretaps were likely to be aimed at collecting and maintaining "strategic" intelligence information, making criminal prosecutions less likely and Fourth Amendment protections less essential, relates to the harm caused by surveillance rather than the effect of requiring a warrant. *Id.* at 648. As Justice Douglas explained in his opinion in the Keith case, however, open-ended and unfocused national security investigations risk becoming the type of general warrants that are forbidden by the Fourth Amendment. *See supra* text accompanying notes 37-39. Second, the argument that a warrant requirement would place an enormous administrative burden on the executive branch and courts is "grounded in expediency," not the ability of the government to carry out surveillance, and, in any event, could not serve as a basis for resolving a constitutional inquiry. *Zweibon*, 516 F.2d at 651.

226 United States v. U.S. Dist. Court for E. Dist. of Mich. (*Keith*), 407 U.S. 297 (1972).

227 *Zweibon,* 516 F.2d at 647 (noting that "[s]ince the warrant proceeding is conducted ex parte, disclosure of information can be restricted to the judge; administrative personnel can be provided by the Government should he require clerical or other assistance").

228 This argument was also rejected by the D.C. Circuit. *Id.* at 649-50. In *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, 551 F.3d 1004, 1010 (FISA Ct. Rev. 2008), however, the FISA Appeals Court accepted that this delay would "materially interfere" with the collection of foreign intelligence.

229 *Zweibon*, 516 F.2d at 649-50.

230 *Id*. at 646.

231 *Id.*

232 United States v. Karo, 468 U.S. 705, 718 (1984); *see also Zweibon*, 516 F.2d at 636.

233 *See Foreign Intelligence Surveillance Act Court Orders 1979-2014*, Elec. Privacy Info. Ctr. (May 1, 2014), https://epic.org/privacy/wiretap/stats/fisa_stats.html.

234 Calculated from the Administrative Office of the U.S. Courts' Wiretap Reports from the years 2013 and 2002, showing 35,200 total intercept applications requested and 35,189 authorized from 1996 - 2013. Admin. Office of the U.S. Courts, Wiretap Report 2013 tbl. 7 (2013), *available at* http://www.uscourts.gov/Statistics/WiretapReports/wiretap-report-2013.aspx#sa1; Admin. Office of the U.S. Courts, Wiretap Report 2002 tbl. 7 (2002), *available at* http://www.uscourts.gov/Statistics/WiretapReports/WiretapReport2002.aspx.

235 Camara v. Municipal Court of S.F., 387 U.S. 523, 538 (1967).

236 Orin Kerr, *"Special Needs" and the NSA Surveillance Program*, Volokh Conspiracy (Feb. 13, 2006, 2:54 PM), http://volokh.com/2006/02/13/special-needs-and-the-nsa-surveillance-program/.

237 In *United States v. Brignoni-Ponce*, the Court invalidated roving patrols near the international border that were justified as necessary to interdict illegal aliens and prevent smuggling. 422 U.S. 873, 881 (1975). In *Delaware v. Prouse*, the Court struck down discretionary spot checks for driver's licenses and registration that were justified as part of the state's effort to promote public safety on the road. 440 U.S. 648, 648 (1979); *see also* MacWade v. Kelly, 460 F.3d 260, 265 (2d Cir. 2006) (noting, in upholding random searches of backpacks and other containers on the New York subway system, that "[o]fficers exercise virtually no discretion in determining whom to search").

238 Delaware v. Prouse, 440 U.S. 648, 654 (1979) (quoting Terry v. Ohio, 392 U.S. 1, 21 (1968)).

239 *See* 2011 Bates Decision, *supra* note 117, at *27 ("The [FISA Appeals Court] and this Court have recognized that the procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information.").

240 Eric H. Holder, Jr. U.S. Dep't of Justice, Minimization Procedures Used by the National Security Agency In Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended 7, 9 (2011), *available at* http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

241 *See* Gellman et al., *supra* note 171.

242 50 U.S.C. §§ 1881a(b)(2), 1881a(g)(2)(A)(vii).

243 Eric H. Holder, Jr. U.S. Dep't of Justice, Minimization Procedures Used by the National Security Agency In Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended § 3(b) (2009), *available at* http://www.theguardian.com/world/interactive/2013/jun/20/exhibit-b-nsa-procedures-document.

244 2011 Bates Decision, *supra* note 117, at *13 (FISA Ct. Oct. 3, 2011).

245 PCLOB 702 Report, *supra* note 166, at 55-60.

246 50 U.S.C. § 1804.

247 PCLOB 702 Report, *supra* note 166, at 59.

248 Michael B. Mukasey, U.S. Dep't Of Justice, The Attorney General's Guidelines For Domestic FBI Operations § II(B)(4)(a)(i) (Sept. 29, 2008), *available at* http://www.justice.gov/sites/default/files/ag/legacy/2008/10/03/guidelines.pdf.

249 *See, e.g.,* United States v. Duggan, 743 F.2d 59, 78 (2d Cir. 1984); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987).

250 *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp.2d 611, 623 (FISA Ct. 2002), *rev'd, In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

251 *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002).

252 *Id.* at 744-45.

253 Ferguson v. City of Charleston, 532 U.S. 67, 68 (2001).

254 *Id.*

255 Even if a court may ascertain, on its own, that the facts set forth in an application for a FISA order support the necessary finding of probable cause, there remains the possibility that those facts are untrue. In many cases, only the defendant will have information necessary to disprove an application's veracity. The Fourth Amendment's Warrant Clause requires that a defendant have the opportunity to seek an evidentiary hearing on this point, known as a "Franks hearing." Franks v. Delaware, 438 U.S. 154, 164-65, 168 (1978). As one federal appellate judge recently noted, however, barring a defendant from seeing the FISA application effectively prevents him from making the showing necessary to trigger a Franks hearing — which means the court never even hears the relevant evidence. United States v. Daoud, 755 F.3d 479, 486 (7th Circ. 2014) (Rovner, J., concurring).

256 United States v. Brown, 484 F.2d 418, 427 (5th Cir. 1973) (Goldberg, J., concurring) ("The judiciary must not be astigmatic in the presence of warrantless surveillance; rather judges must microscopically examine the wiretaps in order to determine whether they had their origin in foreign intelligence or were merely camouflaged domestic intrusions.").

257 United States v. Truong Dinh Hung, 629 F.2d 908, 915 (4th Cir. 1980) (citation omitted).

258 PCLOB 702 Report, *supra* note 166, at 7.

259 50 U.S.C. § 1801(e).

260 *See supra* text accompanying note 175.

261 *Truong,* 629 F.2d at 915.

262 *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01, at 40-41 (FISA Ct. Sept. 4, 2008), *available at* https://www.eff.org/files/2015/03/02/fisc_opinion_and_order_september_4_2008.pdf.

263 50 U.S.C. § 1801(h)(1).

264 Smith v. Maryland, 442 U.S. 735, 735 (1979).

265 *See, e.g.,* 2013 FISC Opinion, *supra* note 128, at 6-9; United States v. Reed, 575 F.3d 900, 914 (9th Cir. 2009); U.S. Telecom Ass'n v. FCC, 227 F.3d 450, 454 (D.C. Cir. 2000).

266 Lee Ferran, *Ex-NSA Chief: 'We Kill People Based on Metadata,'* ABC News (May 12, 2014, 12:59 PM), http://abcnews.go.com/blogs/headlines/2014/05/ex-nsa-chief-we-kill-people-based-on-metadata/.

267 *See, e.g.,* Declaration of Prof. Edward W. Felten at 13-22, ACLU v. Clapper, 133 S.Ct. 1138 (2013) (No. 13-cv-03994).

268 United States v. Warshak, 631 F.3d 266, 286-87 (6th Cir. 2010).

269 Riley v. California, 134 S.Ct. 2473, 2490 (2014).

270 United States v. Jones, 132 S.Ct. 945, 957 (2012) (Sotomayer, J., concurring).

271 This regime should not look identical to FISA as it stood before 2007, however. Outdated aspects of FISA — including its reliance on geography as a proxy for nationality and its differential treatment of wire and satellite communications — should be jettisoned. A court order should be required to obtain communications involving U.S. persons, regardless of where or how the person is communicating or the means by which the communication is intercepted. Wiretapping of communications involving Americans that takes place abroad, for instance, should not be exempt from FISA's reach; nor should domestically intercepted radio transmissions (e.g., from cell phone calls) be exempt simply because one party to the call is overseas.

272 *See* FISA Court Reform Act of 2013, S. 1467, 113th Cong. § 3 (2013); U.S.A. FREEDOM Act, H.R. 3361, 113th Cong. § 401 (2013); Privacy and 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 184 (2014) [hereinafter PCLOB 215 Report], *available at* http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf; President's Review Grp. on Intelligence and Communications Technologies, Liberty and Security in a Changing World 203-04 (2013) [hereinafter Review Group Report], *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

273 Barack Obama, President, Address at the U.S. Department of Justice, *supra* note 166; James G. Carr, Op-Ed., *A Better Secret Court*, N.Y Times, July 22, 2013, at A21, *available at* http://www.nytimes.com/2013/07/23/opinion/a-better-secret-court.html?_r=1&; Stephen Braun, *Former Judge Admits Flaws in Secret Court*, Yahoo News (July 9, 2013, 3:25 PM), http://news.yahoo.com/former-judge-admits-flaws-secret-court-145541583.html. *But see* Comments of the Judiciary on Proposals Regarding the Foreign Intelligence Surveillance Act (Jan. 10, 2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/1-10-2014-Enclosure-re-FISA.pdf (presenting one former FISA Court judge's view that the participation of a privacy advocate in FISA proceedings would be unnecessary and counterproductive).

274 *See* FISA Improvements Act of 2013, S. 1631, 113th Cong. § 4 (2013); Ensuring Adversarial Process in the FISA Court Act, H.R. 3159, 113th Cong. § 2(b)(5) (2013).

275 *See* Andrew Nolan & Richard M. Thompson, Cong. Research Serv., R43362, Reform of the Foreign Intelligence Surveillance Courts: Procedural and Operational Challenges 9-10 (2014), *available at* http://www.fas.org/sgp/crs/intel/R43362.pdf; PCLOB 215 Report, *supra* note 272, at 184.

276 The known instances of *amicus* participation occurred in the rare instances in which FISA matters were proceeding publicly and outside parties requested permission to file briefs. *See, e.g.*, Order Granting Leave for Center for National Security Studies to File Brief of Amicus Curiae Not Exceeding 7000 Words, *In re* Application of the FBI for an Order Requiring the Production of Tangible Things, No. BR 14-01 (FISA Ct. Mar. 20, 2014), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2014-01%20Order-1.pdf; Motion of the Reporters Committee for Freedom of the Press, ABC, Inc., the Associated Press, Bloomberg L.P., Dow Jones & Company, Inc., Gannett Co., Inc., Los Angeles Times, the Mcclatchy Company, National Public Radio, Inc., the New York Times Company, the New Yorker, the Newsweek/Daily Beast Company LLC, Reuters America LLC, Tribune Company, and the Washington Post for Leave to File Brief as Amici Curiae in Support of the Motion for the Release of Court Records and the Motions for Declaratory Judgment, *In re* Orders of this Court Interpreting Section 215 of the PATRIOT Act, No. Misc. 13-02 (FISA Ct. Aug. 7, 2014), *available at* http://www.fisc.uscourts.gov/sites/default/files/Misc%2013-02%20Motion-4.pdf; Brief for National Association of Criminal Defense Lawyers as Amici Curiae in Support of Affirmance, *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002), *available at* http://www.nacdl.org/WorkArea/linkit.aspx?LinkIdentifier=id&ItemID=16211&libID=16181. If the ability of an outside party to request *amicus* participation were to become routine rather than exceptional, there is little reason to expect that the FISA Court would grant such requests liberally.

277 *See* Jared P. Cole & Andrew Nolan, Cong. Research Serv., R43451, Reform of the Foreign Intelligence Surveillance Courts: A Brief Overview 5-8 (2014), *available at* http://fas.org/sgp/crs/intel/R43451.pdf.

278 *See* Lederman & Vladeck, *supra* note 188.

279 *See* Ending Secret Law Act, S. 1130, 113th Cong. (2013); U.S.A. FREEDOM Act, H.R. 3361, 113th Cong. (2013); USA FREEDOM Act of 2014, S. 2685, 113th Cong. (2014); Intelligence Oversight and Surveillance Reform Act, S. 1551, 113th Cong. (2013); FISA Court Reform Act of 2013, S. 1467, 113th Cong. (2013); LIBERT-E Act, H.R. 2399, 113th Cong. (2013); FISA Court in the Sunshine Act of 2013, H.R. 2440, 113th Cong. (2013); Ending Secret Law Act, H.R. 2475, 113th Cong. (2013).

280 Classified Information Procedures Act of 1980, 18 U.S.C. app. § 3.

281 For more on this argument, see Beryl A. Howell & Dana J. Lesemann, *FISA's Fruits in Criminal Cases: An Opportunity for Improved Accountability,* 12 UCLA J. Int'l L. & Foreign Aff. 145, 155-62 (2007).

282 *See* Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1145 (2013).

283 *See* Al-Haramain Islamic Found., Inc. v. Obama, 705 F.3d 845, 848 (9th Cir. 2012).

284 50 U.S.C. § 1801(e)(1).

285 Exec. Office of the president, Presidential Policy Directive/PPD-28, at 4 (2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf.

286 If these criteria were adopted, it would be critical to define "cybersecurity threats" in a manner that does not sweep too broadly. Recent cybersecurity legislation contains an overbroad definition that would encompass various types of online mischief that in no way constitute national security threats, and may even encompass the activities of whistleblowers in disclosing government fraud, waste, or abuse. *See* Cybersecurity Information Sharing Act of 2014, S. 2588, 113th Cong. (2014); Letter from ACLU et al. to Sen. Harry Reid, Sen. Mitch McConnell, Sen. Dianne Feinstein, Sen. Saxby Chambliss 1 (June 26, 2014), *available at* https://www.aclu.org/sites/default/files/assets/6-26-14_--_cisa_sign-on_letter_final.pdf (citing "the discussion draft authored by Senate Select Intelligence Committee ("SSCI") Chairman Dianne Feinstein (D-CA) and Vice Chairman Saxby Chambliss (R-GA) and released earlier [in June 2014]"). Other terms within these six criteria could conceivably benefit from a more detailed definition as well, and much would depend on how the government and the FISA Court interpreted them. Ensuring a level of transparency in FISA Court rulings should allow lawmakers and the public to assess whether further definition-tightening is necessary.

287 United States v. Brown, 484 F.2d 418, 427 (5th Cir. 1973) (Goldberg, J., concurring).

288 It is less likely that programmatic collection of Americans' telephone records will continue, given the clear tension between the program and the text of Section 215, as well as President Obama's stated intent to end the program. In the event that bulk collection does continue, however, Congress should codify the current practice of requiring the FISA Court to pre-approve any searches of the data.

289 To the extent targeting procedures could, in some of their particulars, reveal specific capabilities that depend on secrecy for their effectiveness, they cannot be spelled out by Congress. However, many of the targeting procedures contained in the now-public 2009 document clearly did not require classification. For instance, whether any doubt about a target's nationality or location should be resolved in the government's favor is a question that can be openly debated and answered by Congress. *See* Holder, *supra* note 201, at 4. Congress also could specify that the government *must* undertake many of the inquiries that the government *may* take under the current procedures — such as identifying the country code of a telephone number it plans to surveil, or comparing phone numbers or e-mail accounts against information in NSA's existing databases. *See* Holder, *supra* note 201, at 2-3. As for minimization procedures, there is simply no justification for concealing the steps that the government takes to effectuate Congress's command to "minimize" the acquisition, retention, and dissemination of U.S. person information. There is no manner in which a target could use this information to avoid collection, as minimization — in practice, even if not in theory — imposes no limits at the collection stage. Moreover, a target by definition must be a non-U.S. person, and minimization requirements apply only to U.S. person information. The specifics of how minimization is accomplished thus offer no hints to a target about how his own information may be acquired, retained, or disseminated.

290 Advocates for greater oversight might argue that a clear error review — on a matter in which the judiciary already is inclined to be deferential to the executive's judgments — would accomplish little. In fact, however, the requirement would serve an important checking function. By forcing the government to articulate the factual basis for choosing selectors, it would create an incentive for self-restraint at the front end of the process. While it is unlikely that the FISA Court would reject any of the selectors that the government submitted to it, it is quite likely that the list of selectors presented to the court would be smaller and better justified than would otherwise be the case. On the flip side, the government would no doubt argue that this proposal represents an unworkable burden on the executive branch and the FISA Court. If the government's scope of collection remained as broad as it is now, that argument might hold some weight. However, the burden stemming from this proposal should be greatly diminished by the reinstatement of the "agent of a foreign power" and "primary purpose" criteria, as well as the narrowing of the definition of "foreign intelligence information." Following these changes, the number of targets for whom selection terms must be presented to the court — while no doubt large — should be nowhere near the reported 89,000 targets today. *2013 Transparency Report*, *supra* note 178 (estimating that 89,138 targets were affected by Section 702 in 2013).

STAY CONNECTED TO THE BRENNAN CENTER

Visit our website at **www.brennancenter.org.**
Sign up for our electronic newsletters at **www.brennancenter.org/signup.**

Latest News | Up-to-the-minute info on our work, publications, events, and more.

Voting Newsletter | Latest developments, state updates, new research, and media roundup.

Justice Update | Snapshot of our justice work and latest developments in the field.

Fair Courts | Comprehensive news roundup spotlighting judges and the courts.

Money in Politics | Latest state & national developments, orginal analysis, and more.

Redistricting Round-Up | Analysis of current legal battles and legislative efforts.

Liberty & National Security | Updates on privacy, government oversight, and accountability.

Twitter | www.twitter.com/BrennanCenter
Facebook | www.facebook.com/BrennanCenter
Instagram | www.instagram.com/brennancenter

NEW AND FORTHCOMING BRENNAN CENTER PUBLICATIONS

Strengthening Congressional Oversight
Edited by Michael German

National Security and Local Police
Michael Price

What the Government Does with Americans' Data
Rachel Levinson-Waldman

What Caused the Crime Decline?
Oliver Roeder, Lauren-Brooke Eisen, Julia Bowling

Election Spending 2014: Outside Spending in Senate Races Since Citizens United
Ian Vandewalker

Political Opportunity: A New Framework for Democratic Reform
Mark Schmitt

The Impact of Judicial Vacancies on Federal Trial Courts
Alicia Bannon

Democracy & Justice: Collected Writings, Vol. VIII
Brennan Center for Justice

For more information, please visit www.brennancenter.org

BRENNAN
CENTER
FOR JUSTICE

at New York University School of Law

161 Avenue of the Americas
12th Floor
New York, NY 10013
646-292-8310
www.brennancenter.org