Insidious Encroachment? Strengthening the "Crown Jewels": The 2018 Reauthorization of FISA Section 702

John F. Schifalacqua
University of Pennsylvania Law School

Follow this and additional works at: https://digitalcommons.wcl.american.edu/nslb

Part of the Fourth Amendment Commons, Legal History Commons, Legislation Commons, and the Privacy Law Commons

Recommended Citation
Available at: https://digitalcommons.wcl.american.edu/nslb/vol9/iss1/2

This Article is brought to you for free and open access by the Washington College of Law Journals & Law Reviews at Digital Commons @ American University Washington College of Law. It has been accepted for inclusion in American University National Security Law Brief by an authorized editor of Digital Commons @ American University Washington College of Law. For more information, please contact kclay@wcl.american.edu.
INSIDIOUS ENCROACHMENT?

STRENGTHENING THE “CROWN JEWELS”: THE 2018 REAUTHORIZATION OF FISA SECTION 702

John F. Schifalacqua*

ABSTRACT

This article seeks to turn a critical eye toward to the Reauthorization Act—both its development and future challenges—as a way to evaluate the current state of Section 702 since its recent reauthorization. To establish a historical context, Part II will lay out the general history of Section 702, its requirements, and the techniques the government has typically deployed under its authority. Part III will develop an account of the legislative history of the Reauthorization Act to highlight the keys issues of contention in public discourse over Section 702. Part IV will detail the key changes to Section 702 implemented by Congress. Part V will then describe the typical constitutional challenges to Section 702 prior to the Reauthorization Act and reassess the viability of in light of the key changes to the program. Finally, Part VI will conclude by offering positive developments and missed opportunities from the debates. Overall, this article seeks to emphasize that the responsibility to protect constitutional rights while simultaneously ensuring national security can at times feel like a herculean duty. But this balance is often best struck on the front end when members of Congress and are pressured to reform national security authorities rather than rely on Executive agencies to utilize its surveillance tools according to an often malleable, broad legal standard. Nevertheless, this Comment argues that there are presently substantial avenues for litigants to challenge the newest changes to Section 702 under the Fourth Amendment.

* John F. Schifalacqua is a May 2019 J.D. Candidate at the University of Pennsylvania Law School. He received a B.A. in History from the University of Virginia in 2014. He would like to thank David Sadoff for his guidance and valuable feedback while writing this article.
# TABLE OF CONTENTS

Abstract ......................................................................................................................................... 93
Introduction .................................................................................................................................... 95

I. Origin and Authorities of Section 702 .................................................................................. 101
   A. Background of FISA and Section 702 ............................................................................ 101
   B. Authorities Under Section 702 .................................................................................... 113
   C. Separating Theory from Practice ............................................................................... 117

II. Reauthorization Debates ...................................................................................................... 119

III. The Reauthorization Act's Reform to Section 702 ............................................................ 131

IV. Reevaluating Points of Constitutional Contention ............................................................. 133
   A. Querying and “About” Collection are Fourth Amendment Searches ......................... 135
   B. Newly Authorized Section 702 Searches are Unreasonable .......................................... 138
   C. Exceptions to the Warrant Requirement Do Not Apply ............................................ 141

V. Conclusion ............................................................................................................................ 151

“Experience should teach us to be most on our guard to protect liberty when the Government’s purposes are beneficent. . . . The greatest dangers to liberty lurk in insidious encroachment by men of zeal, well-meaning but without understanding.”

Justice Louis Brandeis

Olmstead v. United States, 277 U.S. 438, 479 (1928)

“We can’t tie the hands of our national security officials at the precise moment that our enemies are taking the gloves off around the world. Terrorists don’t plan to sunset their threats to our way of life, so why should our important counterterrorism tools sunset?”

Senator Tom Cotton, Speech before Congress, June 6, 2017
INTRODUCTION

The Federal Bureau of Investigation (FBI) was racing against an almost literal ticking time bomb when agents coordinated with New York City law enforcement to stop Najibullah Zazi as he crossed the George Washington Bridge just days before the 2009 anniversary of 9/11. A search of Zazi’s rental car was unfruitful and he grew suspicious that he was under surveillance and aborted his so-called “martyrdom operation.” The operation began with a 2008 visit to an al-Qaeda stronghold in Pakistan where he received weapons and bomb making training in hopes of fighting alongside the Taliban. Instead, the Taliban directed him to return to the United States—where he was a legal resident since emigrating from Afghanistan during high school—to devise a suicide attack in New York City. He spent most of 2009 procuring explosive chemicals and preparing two other conspirators to carry out a coordinated bombing around 9/11’s anniversary—targeting the New York City Subway, Times Square, and Grand Central Station. The plan was only days away from fruition when he drove across the George Washington Bridge with hidden bomb making materials in tow. His brief encounter with law enforcement on the bridge scared him off and he fled to Colorado where he was arrested as he tried to destroy evidence to thwart any subsequent investigation.

1 A.G. Sulzberger & William K. Rashbaum, Guilty Plea Made in Plot to Bomb New York Subway, N.Y. TIMES (Feb. 22, 2010), http://www.nytimes.com/2010/02/23/nyregion/23terror.html (describing the case against Najibullah Zazi and his thwarted terrorist plot to bomb the New York Subway on the anniversary of September 11th). See also Inside the Zazi Arrest, NEWSWEEK (Sep. 25, 2009, 8:00 PM), http://www.newsweek.com/inside-zazi-arrest-79531 (describing the investigative details leading up to the Zazi arrest, with particular emphasis on the successful coordination between law enforcement entities).

2 Sulzberger & Rashbaum, supra note 1.

3 Id.


5 See id.
Zazi’s suspicion was certainly justified; law enforcement had been keeping a close eye on him in the months before his arrest. But Zazi could not have known the full extent of the surveillance. The intelligence community (IC) had long been on his tail, deploying some of its most sophisticated surveillance methods to identify him and coordinate with the FBI. The National Security Agency (NSA) used authority granted by Section 702 of the Foreign Intelligence Surveillance Act (FISA) to monitor an email account used by an al-Qaeda operative in Pakistan. That operative had received an email from a then-unknown person in the United States “urgently seeking advice regarding how to make explosives.” The NSA passed along this information to the FBI who used a National Security Letter to rapidly identify the unknown sender as Zazi. From that point forward, the FBI began a sensitive counterterrorism investigation to thwart what was considered “one of the most serious threats to the United States since 9/11.”

In retrospect, it was clear to the Privacy and Civil Liberties Oversight Board (PCLOB)—an entity that reviews the IC—that “without the initial tip-

---

6 See Inside the Zazi Arrest, supra note 1.
8 Id.
9 Id. (explaining that National Security Letters are a type of administrative subpoena certain law enforcement agencies can issue to businesses without a court order). National security letters generally require the production of a narrow type of content-neutral records (e.g., information equivalent to a trap and trace list, not the content of the conversations) to aid in a national security investigation. Statutory provisions for these subpoenas range from §114(a)(5) of the Right to Financial Privacy to the extensively used Electronic Communications Privacy Act (18 U.S.C. §2709). See CHARLES DOYLE, Summary, CONG. RESEARCH SERV. RL33320, NATIONAL SECURITY LETTERS IN FOREIGN INTELLIGENCE INVESTIGATIONS: LEGAL BACKGROUND AND RECENT AMENDMENTS (2008), https://fas.org/sgp/crs/intel/RL33320.pdf#page=2.
10 Guide to Section 702, supra note 7.
11 Sulzberger & Rashbaum, supra note 1.
12 Intelligence Reform and Terrorism Prevention Act, Pub. L. No. 108-458, § 1061, 118 Stat. 3638, 3684 (2004) (authorizing the PCLOB to continually review “regulations, executive branch polices, and procedures . . . related to laws pertaining to efforts to protect the Nation from terrorism, and other actions by the executive branch related to
off about Zazi and his plans, which came about by monitoring an overseas foreigner under Section 702, the subway bombing might have succeeded." 13 In other words, foreign intelligence surveillance was critical in preventing the attack. Indeed, the IC has long held that the authority for surveillance granted by Section 702 is vital to national security. 14 There are many more examples of successful counterterrorism beyond the Zazi plot to support this claim. 15 Members of the IC have testified as recently as 2017 that Section 702 is such a critical tool that some "foreign intelligence cannot be practically obtained through other methods" and the authority is a major contributor to counterterrorism and counterintelligence. 16 In fact, former FBI Director James Comey went as far as to say that Section 702 authorities are the "crown jewels" of counterterrorism, without which "we will be less safe as a country." 17

Despite Section 702's track record of success and significance as a national security tool, it remains a contentious subject. The PCLOB recommended several reforms despite a glowing review of the program's effectiveness, citing efforts to protect the Nation from terrorism to ensure that privacy and civil liberties are protected.").

13 Guide to Section 702, supra note 7.
14 Id. (opining that "Title VII of FISA is vital to keeping the nation safe. These authorities provide the government with a uniquely effective way to acquire information about the plans and identities of terrorists and terrorist organizations, including how they function and receive support. These authorities also enable collection of information about the intentions and capabilities of weapons proliferators and other foreign adversaries who threaten the U.S. and inform cybersecurity efforts.").
15 Id. (stating that Section 702 success stories include the CIA using it "to alert[] a foreign partner to the presence within its borders of an al-Qaeda sympathizer;" the NSA collecting two years of intelligence on ISIS Finance Minister Hajji Iman; the FBI exposing Shawn Parson as a "key player" and recruiter in the ISIS network; and the U.S. helping to uncover the perpetrator of the deadly December 31, 2017 Turkish nightclub attack).
16 Joint Statement for the Record Before the Senate Select Committee on Intelligence, 115th Cong. 8 (Jun. 7, 2017) (statements of Daniel Coats, DNI; Michael Rogers, NSA; Rod Rosenstein, DOJ; Andrew McCabe; FBI), https://www.intelligence.senate.gov/sites/default/files/documents/os-dcoats-060717.pdf.
"certain aspects of the Section 702 program push the program close to the line of constitutional reasonableness." Much of the concern involves incidental collection of data regarding U.S. persons that are not the target of a search at the time it is made. The broadness of Section 702's grant of authority to surveil any foreigner abroad who might possess foreign intelligence information potentially means a large swath of people can be searched, including their communications with U.S. citizens. The American Civil Liberties Union (ACLU) warns that in the process of executing a Section 702 search, the IC collects a "vast trove of data for information specifically about Americans, even though these communications were all collected without a warrant." The concern is that the government can search incidental data at a later time "to prosecute Americans for crimes" unrelated to national security, thereby doing a "backdoor" end-run around the Fourth Amendment. And there is certainly reason to believe abuse might be widespread, at least concerning the invasion of privacy. A 2015 preliminary review found that NSA analysts "running searches on emails and other digital communications

19 Id. (providing, in relevant part, "[s]uch aspects [of constitutional concern] include the unknown and potentially large scope of the incidental collection of US persons' communications, the use of 'about' collection to acquire Internet communications that are neither to nor from the target of surveillance, and the use of queries to search for the communications of specific US persons within the information that has been collected.").
20 See infra Part II.B. for details on how Section 702 operates in practice.
21 Warrantless Surveillance Under Section 702 of FISA, ACLU, https://www.aclu.org/issues/national-security/privacy-and-surveillance/warrantless-surveillance-under-section-702-fisa (last visited Feb. 26, 2019). See also Barton Gellman, In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139ad8045a-11e4-8572-4blb969b6322_story.html ("Nine of 10 account holders found in a large cache of intercepted conversations, which former NSA contractor Edward Snowden provided in full to The Post, were not the intended surveillance targets but were caught in a net the agency had cast for somebody else.").
22 ACLU, supra note 21.
vacuumed up from undersea internet cables frequently violated Americans’ privacy, albeit unintentionally.”

It is hard to overstate the sheer amount of information the IC can acquire under Section 702 authority. By collecting data as it runs through infrastructural switches that bring the Internet to the world—so-called “upstream backbone facility” collection—the IC can “continuously scan international internet traffic in bulk, looking for communications associated with tens of thousands of ‘targets.’” Such collection only requires a surface-level system of judicial oversight. The Foreign Intelligence Surveillance Court (FISC) need only approve a reasonable set of targeting procedures and minimization standards designed to reduce the potential of surveilling Americans. As such, civil libertarians fear a process ripe for abuse. Critics paint an Orwellian picture that “broad, warrantless collection of data under Section 702 creates an understandable fear that private messages may be read or used by the government.” This issue is particularly acute when activists and critics of the program feel targeted as they pursue advocacy to challenge government practices under Section 702.

---


24 ACLU, supra note 21. See also Kris, supra note 18, at 9–10.

25 50 U.S.C. §§ 1881a(d)–(e) (providing, in relevant part, “[t]he Attorney General, in consultation with the Director of National Intelligence, shall adopt minimization procedures that meet the definition of minimization procedures under section 1801(h) of this title . . . [and] ensure that any acquisition authorized under subsection (a) is limited to targeting persons reasonably believed to be located outside the United States; and prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.”).


27 ACLU, supra note 21.

28 See, e.g., Clapper v. Amnesty Int’l USA, 568 U.S. 398, 406 (2013) (stating in relevant part, “Respondents are attorneys and human rights, labor legal, and media organizations. Respondents are attorneys and human rights, labor, legal, and media organizations whose work allegedly requires them to engage in sensitive and sometimes
but law enforcement later searching data without restriction—data initially collected for intelligence purposes—is quite another. It is not unfounded to ask whether Section 702 permits the government to undermine the Constitution on the pretense of national security.

At the core of the issue is the reoccurring "tension between privacy and national security."29 No amount of Zazis captured fully mitigate the history of governmental abuse of counterterrorism tools. One court reminds us that "in the 1960s and 1970s, the public was outraged over the revelation that the government conducted domestic surveillance—in the name of national security—of Dr. Martin Luther King, Jr., Vietnam War protesters, and other domestic groups the government labeled 'subversive.'"30 And whether such a history repeats itself, as the court warns, is a specter haunting the debates over Section 702.31

Nowhere has this tension been more apparent recently than in the debates preceding the passage of the FISA Amendments Reauthorization Act of 2017 (Reauthorization Act).32 The original statutory authority for Section 702 derives from the FISA Amendments Act (FAA), which was set to expire by the end of 2017. With both its usefulness and dangers in mind, Congress debated the efficacy of Section 702. The result was a renewal of the FAA and Section 702 authority until 2023—with some key changes—that was signed into law by President Trump on January 19, 2018.33 The debates preceding the reauthorization of Section 702 and the changes to the program provide an opportunity to take a fresh look at its value and constitutionality.

privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad. . . . Respondents claim that § 1881a compromises their ability to locate witnesses, cultivate sources, obtain information, and communicate confidential information to their clients.

30 Id. (citing DAVID S. KRIS & J. DOUGLAS WILSON, 1 NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 3.1 (2d ed. 2012)).
31 Id.
This article seeks to turn a critical eye toward the Reauthorization Act—both its development and future challenges—as a way to evaluate the current state of Section 702 since its recent reauthorization. To establish a historical context, Part II will lay out the general history of Section 702, its requirements, and the techniques the government has typically deployed under its authority. Part III will develop an account of the legislative history of the Reauthorization Act to highlight the keys issues of contention in public discourse concerning Section 702. Part IV will detail the key changes to Section 702 implemented by Congress. Part V will then describe the typical constitutional challenges to Section 702 prior to the Reauthorization Act and reassess the viability of those challenges in light of the key changes to the program. Finally, Part VI will conclude by offering positive developments and missed opportunities from the debates. Overall, this article seeks to emphasize that the responsibility to protect constitutional rights while simultaneously ensuring national security can at times feel like a herculean duty. However, this balance is often best struck on the front end when members of Congress are pressured to reform national security authorities rather than rely on Executive agencies to utilize their surveillance tools according to a broad and often malleable legal standard. Nevertheless, this article argues that there are presently substantial avenues for litigants to challenge the newest changes to Section 702 under the Fourth Amendment.

I. ORIGIN AND AUTHORITIES OF SECTION 702

A. Background of FISA and Section 702

It is useful to begin by differentiating between the two statutes under which the government can conduct electronic surveillance: Title III and FISA. Generally, Title III concerns electronic surveillance the government may deploy for criminal law enforcement purposes. FISA exists within the realm of foreign intelligence operations and was enacted much later. But the clear line between the two is more an ideal than a reality.\(^3^4\) Some of the core

\(^3^4\) USA Patriot Act Amendments to Foreign Intelligence Surveillance Act Authorities: Hearing Before the S. Select Comm. on Intel., 109th Cong. (2005) (statements of U.S.
constitutional issues with Section 702 arise from the blurring of this boundary between foreign intelligence gathering and criminal investigation. Unsurprisingly then, the onus for passing FISA—and ultimately expanding it under Section 702—develops out of the interplay between the boundaries set by Fourth Amendment electronic surveillance case law and flexibility needed to protect the nation.

The first case setting a substantive boundary was *Katz v. United States*. In that seminal case, the government introduced evidence obtained by “attach[ing] an electronic listening and recording device to the outside of the public telephone booth from which [the defendant] had placed his calls.” In a critical passage, Justice Stewart declared that “the Fourth Amendment protects people, not places” and that a physical intrusion into a protected area was not necessary to constitute a Fourth Amendment violation—privacy would be the new compass rose directing the analysis. By overruling long-standing property-based precedent established in *Olmstead v. United States,* the government could no longer conduct electronic surveillance without conforming to the privacy limits implied by the Fourth Amendment. A court

---

Attorney General Alberto R. Gonzales & Robert S. Mueller, III, Director, FBI), https://www.govinfo.gov/content/pkg/CHRG-109shrg24983/html/CHRG-109shrg24983.htm (“the USA PATRIOT Act helped to bring down this ‘wall’ separating intelligence and law enforcement officials. They erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel. They also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing”).

35 See infra Part IV.


37 *Id.* at 351.

38 *See Olmstead v. United States*, 277 U.S. 438, 475 (1928) (stating “[i]t is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offense; but it is the invasion of his indefeasible right of personal security, personal liberty and private property . . . ”).

39 Coincidentally, the Supreme Court would once again reintroduce the topic of property into its Fourth Amendment analysis with United States v. Jones, 565 U.S. 400 (2012). However, for all intents and purposes, absent a violation of an individual’s property rights, the *Katz* two-pronged test remains the main way to evaluate whether a Fourth Amendment “search” occurred. Given that most electronic surveillance
would be forced to focus on personal privacy by asking: 1) Did a person intend their effects to be private? (subjective question); and 2) Is society prepared to recognize that subjective expectation of privacy as reasonable? (objective question) If both questions can be answered in the affirmative, a constitutionally recognized "search" occurs, implicating the Fourth Amendment.

These questions were much more onerous for law enforcement to answer than whether a physical intrusion of property occurred. Consequently, Congress passed Title III of the 1968 Omnibus Crime Control and Safe Streets Act to hedge investigative misconduct by requiring more particularized judicial warrants to obtain electronic surveillance for law enforcement purposes. As such, these warrants were much more thorough than a regular search warrant would require. But it was not until 1967 that these higher standards were put to another test when the Supreme Court was presented with the question of electronic surveillance in the national security context. In United States v. U.S. District Court (Keith), the Court recognized 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." In balancing interests, the Court rejected any arguments about an exception for special circumstances.

40 See Katz, 389 U.S. at 361.
44 Id. at 313.
45 Id. at 320 (providing, in relevant part, that "[t]he Government argues that the special circumstances applicable to domestic security surveillances necessitate a further exception to the warrant requirement. . . . The circumstances described do not justify complete exemption of domestic security surveillance from prior judicial scrutiny. Official surveillance, whether its purpose be criminal investigation or ongoing intelligence gathering, risks infringement of constitutionally protected privacy of speech. Security surveillances are especially sensitive because of the
holding instead that "Fourth Amendment freedoms cannot properly be guaranteed if domestic security surveillances may be conducted solely within the discretion of the Executive."\(^{46}\) A judicial warrant would be required to electronically surveil domestic targets, even for national security purposes.

But the Court explicitly reserved judgement "on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country" (emphasis added).\(^{47}\) The Court stressed that the President had a duty under Article II, Section 1 of the Constitution "to protect our Government against those who would subvert or overthrow it by unlawful means."\(^{48}\) This passage left open the possibility that the government need not be constrained when surveilling foreign targets. In absence of any direction, a number of lower courts looked to fill out the doctrine. The Third, Fourth, Fifth, and Ninth Circuits all held that a warrant was not necessary when surveilling foreign targets so long as the Executive branch could certify that foreign intelligence was the object of the surveillance.\(^{49}\)

The Troung Dinh Hung court explained that "because of the need of the Executive branch for flexibility, its practical experience, and its constitutional competence, the courts should not require the Executive to secure a warrant each time it conducts foreign intelligence surveillance."\(^{50}\) But there were three conditions: 1) "the object of the search or surveillance [had] to be a foreign power" because in those circumstances the need for stealth and speed were so great that the judiciary would have difficulty with the "subtle judgements inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent. We recognize, as we have before, the constitutional basis of the President's domestic security role, but we think it must be exercised in a manner compatible with the Fourth Amendment. In this case we hold that this requires an appropriate prior warrant procedure."\(^{\text{50}}\).

\(^{46}\) Id. at 316.

\(^{47}\) Id. at 308.

\(^{48}\) Id.

\(^{49}\) See United States v. Troung Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Buck, 584 F.2d 871, 875 (9th Cir. 1977); United States v. Butenko, 494 F.2d 593, 604–605 (3d Cir. 1974) (en banc); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973).

\(^{50}\) Troung Dinh Hung, 629 F.2d at 914.
about foreign and military affairs”; 2) the primary purpose of the search had to be to collect foreign intelligence (as opposed to prosecution), otherwise “courts are entirely competent to make the usual probable cause determination”; and 3) the search had to be reasonable according to the facts and circumstances of the case.51 Behind this reasoning was an acknowledgement—similar to the theoretical underpinnings of the political question doctrine52—that courts are not competent to evaluate the intricacies of Executive branch policies, and in this context, the Executive branch’s needs and methods for collecting foreign intelligence. Courts could not make a judgement on a warrant in this context, even if Katz factors were implicated to protect citizens’ privacy interests.

The tension between trusting judges to make a warrant evaluation for surveillance of domestic intelligence gathering (i.e., Keith), but not trusting them in the foreign intelligence context (i.e., Troung Dinh Hung) was not lost on the D.C. Circuit in Zweibon v. Mitchell.53 One would assume that if national security concerns are implicated in both cases, a judge would be either competent or incompetent in both, even if citizen privacy concerns are arguably more significant in the former than the latter.54 The Mitchell court posited that the explanation for the incongruity originates from an argument that the “President’s preeminent power over the conduct of foreign affairs” under Article II, Section 2 permits surveillance without a warrant.55 But the

51 Id. at 915–16.
52 See Baker v. Carr, 369 U.S. 186, 211 (1962) (providing, in relevant part, “Foreign relations: There are sweeping statements to the effect that all questions touching foreign relations are political questions. Not only does resolution of such issues frequently turn on standards that defy judicial application or involve the exercise of a discretion demonstrably committed to the executive or legislature; but many such questions uniquely demand single-voiced statement of the Government’s views.”).
53 516 F.2d 594 (D.C. Cir. 1975).
54 Id. at 624 (providing, in relevant part, “‘Judicial competence’: Although the judicial competence factor arguably has more force when made in the foreign rather than the domestic security context, the response of Keith to the analogous argument is nevertheless pertinent to any claim that foreign security involves decisions and information beyond the scope of judicial expertise and experience.”).
55 Id. at 615–16 (providing, in relevant part, that “[t]o be sure, the fact that the Keith Court found the President’s powers with respect to domestic affairs insufficient to justify an exception to the warrant requirement when the domestic aspects of national
court refused to hold that this power necessarily “preordain[s] the procedures [or lack thereof] with which the President must comply in exercising that authority.”56 The court laid out the numerous arguments against judicial competence,57 rejecting them all by relying on Keith for the notion that even in the foreign intelligence context, courts so regularly deal in complex domestic matters that such surveillance issues cannot be too complicated for judges to comprehend.58 “If the threat is too subtle or complex for our senior law enforcement officers to convey its significance to a court, one may question whether there is probable cause for surveillance.”59 The court went on to discuss the possibility of security leaks, the nature of ongoing foreign surveillance, the possibility of dangerous delay in following a warrant process, and the administrative burden on the Executive branch when applying for these warrants.60 None of these were considered compelling.61

This circuit split over Title III authority in the context of foreign intelligence surveillance embodied two broad debates. First, would complying with Fourth Amendment requirements so substantially handicap the Executive as to seriously infringe on the effectiveness of Article II, Section 1 and 2 powers? This debate was the objective dispute between courts in Troung Dinh Hung and Mitchell, which disagreed over the extent to which the warrant process would lead to leaks, delays, and administrative burdens that would undercut the ability of the government to collect critical foreign intelligence.62 Second, the more subjective and theoretical issue dealt with the security are involved, yet refused to specify what procedures would be entailed if the national security threat had its origin with foreign powers, indicates that any difference in result must turn on the President’s peculiar powers in the field of foreign affairs.”).

56 Id. at 616.
57 Id. at 641 (describing security leaks, the ongoing nature of foreign surveillance, administrative burden, etc.)
58 Id. at 641–46.
59 Id. at 641 (citing United States v. United States District Court (Keith), 407 U.S. 297, 320 (1972)).
60 Id. at 641.
61 Id.
62 Compare Troung Dinh Hung, 629 F.2d at 913 (providing that, for example, “[a] warrant requirement would add a procedural hurdle that would reduce the flexibility of executive foreign intelligence initiatives, in some cases delay executive response to
possibility that even if such handicapping were to occur, civil liberties should nonetheless prevail over national security effectiveness in the foreign intelligence context, even where an exception for special circumstances to the Fourth Amendment might be present. This was the view that the Keith court refused to address. These two debates remain relevant for Section 702 today.

At the time, the Supreme Court did not have to work through these boundaries because Congress stepped to the fore.63 A series of stunning political developments indicated that pure deference to national security concerns in the foreign surveillance context might be dangerous. In 1975, the Church Committee began investigating instances where "warrantless electronic surveillance ostensibly deployed for national security had been seriously abused. For decades Executive agencies had been secretly monitoring American citizens."64 For example, President Nixon's White House spied on political opponents as part of the Watergate Scandal and the CIA conducted intelligence collection against domestic dissidents opposing the Vietnam war.65 These overt abuses were punctuated by subtler—but no less sinister—intrusions for the sake of gathering foreign intelligence.

foreign intelligence threats, and increase the chance of leaks regarding sensitive executive operations.”) with Mitchell, 516 F.2d at 641 (finding that being “mindful of the fact that the existence of presidential powers . . . does not preclude a finding that the legitimate exercise of those powers would in no way be frustrated by subjecting them to prior judicial approval,” and that of the factors that had been asserted —judicial competence, leaks, intelligence gathering not implicating the Fourth Amendment, delay that would result in substantial harm to the national security, or undue administrative burden—none were compelling).

63 "Whether Congress has considered and authorized [an action] . . . is not irrelevant to its constitutionality. The endorsement of the Legislative Branch of government provides some degree of comfort in the face of concerns about the reasonableness of the government’s assertions [about a program.]” ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir., 2015). This suggests that when Congress acts before the judiciary to permit an Executive action in the national security space, the judiciary is more likely to honor it. This is especially pertinent in the FISA context, as it is often the case that Congress responds to negative public opinion or negative dicta with legislative changes before judicial review.

64 MATHESON, supra note 42, at 109.

"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." A program called Project Shamrock, lasting 30 years, featured the NSA acquiring telegrams sent by American citizens—up to 150,000 messages a month. These revelations precipitated the passage of FISA in 1978 as a solution to the problem.

Congress seemed to reject the notion that the Executive’s Article II, Section 1 and 2 authorities gave it unilateral ability to conduct foreign surveillance. Rather, "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 cases." The procedural framework of FISA’s protections are detailed below, but it cut the difference between substantially handicapping the Executive with a full range of procedural requirements and awarding maximal flexibility to further the IC’s collection goals. Consequently, a full criminal warrant would not be required for foreign intelligence surveillance, but less onerous oversight would be imposed. Under FISA, the government needs to obtain a FISC order in an ex parte proceeding, which certifies that there is probable cause that a

66 Id.
67 Id.
68 See Matheson, supra note 42, at 109 (providing, in relevant part, that "[t]he Church Committee stressed the lack of congressional guidelines for agencies such as the NSA. Responding to the need for a statutory framework, Congress passed the FISA in 1978 to regulate electronic surveillance of foreign intelligence information in the United States.").
69 Goitein & Patel, supra note 65, at 14. The Chairman of the Church Committee cautioned that "[i]f the 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." Id. (quoting NBCUniversal Archives, The Intelligence Gathering Debate — www.NBCUniversal Archives.com, YOUTUBE (Jan. 23, 2014), https://www.youtube.com/watch?v=YAG1N4a84Dk (statement of Sen. Frank Church)).
70 See generally Part II.
target of surveillance is a "foreign power" or "agent of a foreign power" and that the specific site being electronically surveilled is equally connected to a foreign power. With this nexus to foreign powers established by such an individualized probable cause standard, the government need only demonstrate a "significant purpose" of collecting foreign intelligence to be awarded a surveillance order. Such a test does not preclude the government from seeking a surveillance order to also pursue criminal prosecution, but the framework's requirement that the government demonstrate probable cause that the target is linked to a foreign power was probable cause requirement linked to foreign powers initially enough to permit flexible use of FISA while preventing its abuse to easily prosecute American citizens. Yet with changes in technology since 1978, the boundaries broke down. Scholars note that:

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 even more strained. Advances in technology mean that the exercise of authorities aimed at foreigners abroad inevitably picks up swathes 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.

Indeed, the very act of differentiating the surveillance of foreign powers from Title III eventually exacerbated the above issue. Drawing on *Troung Dinh Hung*, FISA "allowed the government to obtain surveillance orders if it certified that the 'purpose' of surveillance was the acquisition of foreign intelligence." This primary purpose test created a "strong perception within

---

71 50 U.S.C. § 1805(a)(2)(B) (2012). FISA was amended to include physical searches, pen registers/trap and trace, and the seizure of other "tangible things" for the purpose of foreign intelligence collection, see 50 U.S.C. §§ 1821–29 (physical searches); §§ 1841–46 (pen register/trap and trace); §§ 1861 (access to business records for foreign intelligence investigations) (2008).
73 GOITEIN & PATEL, supra note 65, at 19.
74 Id. at 23.
the government that the procedures erected a ‘wall’ between intelligence and law enforcement that inhibited robust cooperation." Incidental intelligence gathered through primary purpose FISA surveillance could not be shared with law enforcement to prosecute citizens, who are guaranteed robust Fourth Amendment protections detailed in Title III. Not only did advances in technology mean the government was inadvertently (or intentionally) collecting more information about Americans—information that would otherwise be protected in a Title III search—but law enforcement could not access information under the primary purpose test that could lead to the prosecution of terrorists.

In the aftermath of 9/11, many in the government viewed this wall as unacceptable. President Bush responded by authorizing a counterterrorism program called the Terrorist Surveillance Program (TSP) in 2002. The New York Times broke the story detailing how the TSP permitted the “interception (i.e., wiretapping), without warrants, of telephone and email communications where one party to the communication is located outside the United States” and the NSA has a good reason to believe a connection to al-Qaeda existed. To many, the program completely contravened even the minimal procedures of FISA and arguably violated the Fourth Amendment because it scrapped the foreign power requirement. Instead, the government began surveilling without judicial review any U.S. person it believed was communicating with

---

75 Id. at 24.
76 See GOLTEIN & PATEL, supra note 65, at 24 (providing, in relevant part, “There was a strong perception within the government that the [FISA] procedures erected a ‘wall’ between intelligence and law enforcement that inhibited robust cooperation”). This wasn’t necessarily the impression of the 9/11 report, see THE NAT’L COMM’N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 266–72 (2004). But it was enough for the DOJ to modify its procedures to allow FISA surveillance to be conducted under the laxer standard of “significant purpose” instead of “primary purpose” for acquiring foreign intelligence. The rationale was that the lower standard would allow more cooperation between law enforcement and the IC. This standard was challenged and upheld by the FISCR. See In re Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).
a member of al-Qaeda abroad. Understandably, people feared a return to the pre-FISA days of government abuse; the public could not easily ascertain the extent any unreviewed foreign intelligence was being shared with law enforcement. And while the President reauthorized the program many times until 2007, the administration did not disclose much of the legal and operational components of the program—even to the PCLOB. It later came to light that the government was again relying on Article II (harkening back to the question reserved in *Keith*) to argue the President had the authority to conduct this program under the Executive’s responsibility to protect the country. Even after the Bush administration assented to FISC oversight of the TSP, public outcry over the administration’s specious arguments led to FISA Amendments precipitating Section 702.

The administration convinced a Democratically-controlled Congress in 2007 and 2008 to create the FAA’s system of “programmatic surveillance” by arguing that the rapidly digitalizing nature of communication required broader authorities for electronic communication in the war on terror. Section 702 was created as a result. Under its authority, “government may conduct a program to collect any communications ‘targeting’ a person or entity’s communications with Americans in the United States. In other words, the government no longer needs an individualized court order to acquire Americans’ international calls and emails, as long as the American is not the ‘target’ of the surveillance.” While programmatic limits exist, Section 702’s is the statutory version of the TSP and a paring back from FISA’s original procedural safeguards against government abuse by foregoing the need for individualized orders focused on surveilling agents of foreign powers. Now,

---

79 MATHESON, supra note 42, at 111.
83 Id.
communicating with a foreigner abroad is enough to be caught up in the IC’s foreign intelligence programs.

Consequently, the history of FISA embodies competing interests weighed by the case law of electronic surveillance. On the one hand, harkening back to Keith and Troung Dinh Hun, “different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of Government for intelligence information and the protected rights of our citizens.”84 But on the other hand, and in the context of uncertainty and government abuses, “FISA was essentially enacted to create a secure framework by which the Executive branch may conduct legitimate electronic surveillance for foreign intelligence while meeting our national commitment to the Fourth Amendment.”85 The issue can be distilled from the original Keith framework. There the Court believed that the Katz concerns about personal privacy were implicated much more significantly when a domestic person was the target of electronic surveillance compared to a foreign person.86 As such, Executive responsibilities to provide for the nation’s safety and direct foreign affairs were significant enough to recognize flexible oversight requirements in the foreign intelligence context. Courts and Congress were comfortable comporting them with the Fourth Amendment. However, when technology advances and massive amounts of data can be collected in the process, the line blurs to such an extent that citizen privacy concerns may be equally implicated when foreign powers are targeted. The Keith framework begins to crumble, but not concerns about giving the Executive flexibility to accomplish its Article II responsibilities. This trend is embodied by the push toward the original FISA’s restrictions designed to combat abuse (while maintain government flexibility) and the pull from the Bush administration’s TSP (that ultimately

84 United States v. United States District Court (Keith), 407 U.S. 297, 322-23 (1972).
86 See United States v. U.S. District Court (Keith), 407 U.S. 297, 308, 312 (1972) (holding that while “the instant case requires no judgment on the scope of the President’s surveillance power with respect to the activities of foreign powers, within or without this country . . . [t]here is, understandably, a deep-seated uneasiness and apprehension that this capability will be used to intrude upon cherished privacy of law-abiding citizens.”).
morphed into Section 702) to require more flexibility to adequately protect national security. This history is useful because it frames these conceptual battles ebb and flow concerning the nature of electronic intelligence surveillance for national security and its demands from competing interests. Section 702's development is therefore critical for understanding the stakes in the constitutional battles over the program's adherence to the First Amendment, Fourth Amendment, and Separation of Powers principles. And these stakes are increasingly higher as the nature of war and intelligence evolves. The core question is whether Section 702's new authorities tip the constitutional balance.

B. Authorities Under Section 702

Before addressing these new authorities, it is helpful to detail Section 702's original authorities to set a baseline for understanding its changes. Section 702 is programmatic, not individualized. Put differently, "the government no longer needs an individualized court order to acquire Americans' international calls or emails, as long as the American is not the 'target' of surveillance." Indeed, this is a major difference from typical FISA surveillance under which the government can only surveil foreign powers or agents of foreign powers (not just any foreigner abroad) for intelligence information under some semblance of probable cause. The statute authorizes electronic surveillance of non-U.S. persons "reasonably believed" to be located outside the country. The Attorney General (AG) and Director of National Intelligence (DNI) can jointly authorize such targeting for up to a year by procuring an order from the FISC (renewal is possible). If the two determine

87 GOTTEIN & PATEL, supra note 65, at 26.
88 50 U.S.C. §§ 1801(a), et seq. (requiring a traditional FISA search to render some showing of probable cause that the target is a foreign power or agent of a foreign power—including the specific facilities and/or persons to be searched. Section 702 does away with this specificity and individualized determinations. Rather, a major restriction is that the target of a Section 702 search has to be reasonably believed to be a foreigner abroad.).
90 Id.
exigent circumstances exist, then they can proceed without an order.91 This exigency is limited to those situations where “without immediate implementation of an authorization . . . intelligence important to national security of the United States may be lost or not timely acquired . . . .”92 In this case, surveillance can begin without a FISC order, but must be submitted to the FISC within no more than seven days.93 If it becomes known that a non-U.S. person enters the country, the government has 72 hours to continue surveillance under a current order if discontinuing surveillance would threaten real harm.94 In any case, when the government applies to the FISC for a Section 702 order, they are asking to implement a surveillance program, which must not intentionally target any person within the U.S.; target any U.S. person located outside the U.S.; or “acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.”95 Finally, the program must comport with the Fourth Amendment and the Constitution.96 To ensure these limits, the government must attest to certain targeting and minimization procedures that will decrease the likelihood of capturing the information of U.S. persons or those who reside in the U.S. First, the government must certify that a “significant purpose” of the surveillance is to capture foreign intelligence information.97 Second, that this intelligence is being captured with the cooperation of electronic service providers with whom the government must coordinate.98 Third, “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’

91 Id. § 1881a(c)(2).
92 Id.
93 Id. § 1881a(g)(1)(B).
95 Edward C. Liu, Cong. Research Serv., R44457, Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA) 2 (2016); § 1881a(b).
96 Id. § 1881a(b)(6).
97 Id. § 1881a(h)(2)(A)(v).
98 Id. § 1881a(h)(2)(A)(v)(i).
information." All of this is to prevent so-called "reverse targeting" whereby the government uses Section 702 to collect information about a foreigner abroad, but really wishes to target a particular known person in the U.S.\textsuperscript{100}

The tools at the disposal of the government under Section 702 are both astonishing in scale and in technological development. In 2013, a FISC report detailed that the NSA "collected 250 million Internet communications per year under Section 702."\textsuperscript{101} The government can collect this information using many methods. First, the government can tap into "upstream" facilities.\textsuperscript{102} These facilities are the infrastructural "backbone" of the Internet and telephone networks.\textsuperscript{103} They include fiber cables, switches, undersea cables, and other critical junctions.\textsuperscript{104}

As data passes through them, the NSA applies complex algorithms to determine if they contain certain targeted information (while applying minimization standards).\textsuperscript{105} For example, the NSA could filter for an email address from a foreigner abroad. It would pick up emails sent to and from that email address (i.e., To/From Collection) and emails between non-targets who mention the target (i.e., "About" Collection).\textsuperscript{106} "About" Collection is highly controversial because it can pick up the contents of U.S. person communications that are simply about or mention a target foreigner located abroad. This collection method was eventually (and perhaps only temporarily) ended by the NSA despite the government arguing for its

\textsuperscript{99} Goitein & Patel, supra note 65, at 26; §§ 1881a(d)(1)(A), 1881a(e)(1), 1801(h)(1).
\textsuperscript{100} Goitein & Patel, supra note 65, at 26.
\textsuperscript{101} Liu, supra note 95, at 1.
\textsuperscript{103} See Kris, supra note 18, at 9 (discussing "... the international switches or other backbone facilities ..." through which communications transit).
\textsuperscript{104} See Kris, supra note 18, at 9–10, 24–45 (discussing the network of cables that makes up the backbone of telecommunications networks).
\textsuperscript{105} See Kris, supra note 18, at 9–10 (discussing how the NSA finds targeted information during "upstream" collection and applies minimization standards.)
\textsuperscript{106} Kris, supra note 18, at 9.
permissibility under the Constitution. Controversy also exists as to whether the government can store and later search unminimized data (i.e., before the approved search algorithms are applied). This storage could allow the government to search incidental data for related (or unrelated) law enforcement purposes—all without adequate Fourth Amendment procedures. This technique is colloquially known as “backdoor searching.”

It is possible to conduct backdoor searches with U.S. persons data obtained using “about” collection.

The government can also use Section 702 for “downstream” collection, colloquially known as PRISM collection. Here the government works with Internet Service Providers (ISPs), like Google, to retrieve data that likely contains foreign intelligence information. ISPs will either send this data along on their own fruition or respond periodically based on search algorithms the government gives them which are pre-approved by the FISC. This is especially helpful for data that passes through upstream facilities encrypted

---

107 The NSA stopped “about” collection “to resolve problems it was having complying with special rules imposed by the [FISC] in 2011 to protect Americans’ privacy. . . . The problem stemmed from certain bundled messages that internet companies sometimes packaged together and transmitted as a unit. If even one of them had a foreign target’s email address somewhere in it, all were sucked in. . . . The NSA was having technical difficulties figuring out a way to deal with bundled packages” and so stopped collection to comply with the goals set out by the FISC with regard to the bundles. See Quinta Jurecic, NSA Stops “About” Collection, Lawfare (Apr. 28, 2017, 2:14 PM), https://www.lawfareblog.com/nsa-stops-about-collection.

108 Kris, supra note 18, at 12–13.

109 See Neema Singh Guliani, Congress Just Passed a Terrible Surveillance Law. Now What? ACLU (Jan. 18 2018), https://www.aclu.org/blog/national-security/privacy-and-surveillance/congress-just-passed-terrible-surveillance-law-now (suggesting that “the NSA conducts over 30,000 of these “backdoor” searches a year and, while the FBI refuses to report their number, we know they perform these searches routinely when investigating a crime, assessing whether they should open an investigation, or even just hunting for information about foreign affairs.”).

110 Liu, supra note 95, at 1. PRISM was the program revealed by Edward Snowden’s disclosures, see supra note 107.
but becomes unencrypted upon reaching an ISP. Most Section 702 intelligence comes from this type of collection method.

C. Separating Theory from Practice

On the surface, the authority under Section 702 is designed to capture Signals Intelligence (SIGINT) communications from foreigners abroad. It echoes the original differentiation focus in *Keith*: by only concentrating on foreigners abroad, American constitutional privacy concerns are not heavily implicated, and the government is afforded maximum flexibility. As such, the government does not need an individualized court order every time it chooses to surveil a foreigner abroad, even if such surveillance incidentally picks up on a U.S. person’s communications. Rather, the FISC need only approve of the programmatic design of a SIGINT program—it does not need to know who

---


112 LIU, supra note 95, at 1 (“The NSA collected 250 million Internet communications per year under 702. Of these communications, 91% were acquired ‘directly from Internet Service Providers,’ using a mechanism referred to as PRISM collection. The other 9% were acquired through what the NSA calls ‘upstream collection,’ meaning acquisition while Internet traffic is in transit from one unspecified location to another.”). Note how staggering this number is—if only 1% of the 250 million included communications with Americans, that would be 2.5 million Americans indirectly surveilled.

113 LIU, supra note 95, at 2 (“Acquisitions under Section 702 are also geared towards electronic communications or electronically stored information. This is because the certification supporting acquisition . . . requires the AG and DNI to attest that, among other things, the acquisition involves obtaining information from or with the assistance of an electronic communication service provider.”).
or what specifically the government plans to surveil. At its framing, this design was viewed as sufficient to prevent the government from abusing its foreign surveillance authorities to spy on Americans as they did in the pre-FISA era. Theoretically, the balancing seems correct. There should be a lot of flexibility for a type of surveillance that does not per se pose much harm to American privacy interests.

In practice, collection of electronic communications to or from Americans is increasingly beyond incidental. Section 702 represents such a stark change from original FISA authority because it “eliminates [an individualized] court order requirement for the domestic capture of foreigners’ communications with Americans.” So long as the surveillance has a significant purpose (how big is “significant”?), of acquiring foreign intelligence from a foreigner abroad, it would seem that any communications to or from a U.S. person is fair game to be collected without an individualized warrant typical of the Title III process. For any particular SIGINT program, the government might have another “significant purpose” of prosecuting terrorists. Under this framework, the warrantless intelligence collected under Section 702 could theoretically be used to prosecute an American whose communications were “incidentally” collected. Indeed, some argue that “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.” The potential for these end-runs around the Fourth Amendment are only exacerbated by the fact that unlike previous iterations of

114 Goitein & Patel, supra note 65, at 27 (“Under Section 702 . . . the court has no role in approving individual instructions at all.”).

115 Id. at 26 (“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 . . . . With the exception of e-mails stored in the United States, [Section 702] 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 the court order requirement for the domestic capture of foreigners’ communications with Americans.”).

116 Id.

117 Id.
FISA, the government can surveil any non-U.S. person overseas, not just those reasonably believed to be an agent of a foreign power. 118

With the sheer amount of information collectable under the program, the efficacy of 702 was certainly on the mind of Congress as Section 702 was set to expire in 2017 without reauthorization.

II. Reauthorization Debates

The debates to reauthorize and amend Section 702 embodied a fundamental question. Representative Barbara Lee (D-CA) framed it by quoting Alexander de Tocqueville, saying "the reason democracies invariably prevail in military conflict is because democracy is the governmental form that best rewards and encourages those traits that are indispensable to success: initiative, innovation, courage, and love of justice." 119 The extent that Section 702 could be improved to forward these ends was the conceptual dispute at the heart of the reauthorization debates. Indeed, the opportunity for disagreement on this front was varied—at least four different bills and various individual amendments were proposed. 120 All sought to provide its own theory. Is a more flexible, extensive Section 702 the answer to promoting the innovation and initiative of the IC to keep our country safe? Or should the country have the courage and love of justice to handicap the useful tools of foreign surveillance to ensure our liberties were preserved? How would Congress strike a balance “between our cherished liberties and smart security”? 121 The

118 Id. at 27 ("["The court’s] substantive role is limited to determining whether generic sets of targeting and minimizations procedures comply with the statute . . . and with the Fourth Amendment. 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.’"). This review should be compared with the more robust Title III and regular FISA authorities.


answers were far from clear. The reauthorization debates were so pivotal because it was not evident that Section 702 would be reauthorized—let alone expanded—given the above privacy concerns. A focus on the legislative history illuminates the critical considerations at play.

Debates over reauthorizing Section 702 began to foment with the 2017 nomination of then-Congressman Mike Pompeo (R-KS) to be the CIA Director. Congress was already acutely aware that the 2012 reauthorization for Section 702 was set to sunset at the end of the year. Additionally, Section 702 had been “the focus of ceaseless criticism from a politically diverse group of opponents who insist[ed] that it transcends constitutional bounds and represents the harbinger of an Orwellian surveillance state: charges that reached a crescendo in the aftermath of the disclosures by Edward Snowden in 2013.” 122 With this context in mind, Congress took the nomination as an opportunity to have “an open discussion about the future of the CIA,” which included the IC’s intelligence collection capabilities, even though Section 702 has much more to do with the NSA’s collection methods than the CIA. 123 In a long speech, Senator Ron Wyden (D-OR), who would later introduce The USA Rights Act, criticized the Pompeo nomination—detailing his support for wide ranging metadata and “about” collection programs. 124 Troubled by Representative Pompeo’s belief in a “broader and more flexible [standard of surveillance] than the standard that currently applies to Section 702,” Senator Wyden keyed up his issue with Section 702 as one concerned with the primary purpose standard and backdoor searches. 125 Other senators who opposed Representative Pompeo did so on similar grounds. Senators Tom Udall (D-NM), Jon Tester (D-MT), and Chris Van Hollen (D-MD) all spoke out, using the nomination debates as a proxy to voice their concern about backdoor searches and how “the Constitution limits how much intelligence agencies

124 Id at S373–76 (statement of Sen. Wyden).
125 Id.
and the government can intrude into the lives of Americans.” 126 Senator Bernie Sanders (D-VT) even described Section 702 as a tool for “Big Brother” to abuse, and called for amending the program to keep its effectiveness, but “without invading the privacy rights of the American people.” 127 Those who supported Representative Pompeo did so on typical grounds—citing his background and accomplishments. 128 Others chose to engage with their colleagues’ concerns. Notably, Senator James Lankford (R-OK) reminded his colleagues that the “CIA has strict prohibitions from gathering data on U.S. persons”—implying that the issue lies with the information sharing of warrantless intelligence between the IC and law enforcement, not on the scope by which the IC can collect intelligence. 129 Narrowing the issue on backdoor searches seemed pervasive across the aisle.

Although Representative Pompeo was confirmed relatively easily, 130 the surveillance issues through which many opposed his nomination were just beginning to brew. By March 1, 2017 the full Judiciary Committee was hearing testimony on Section 702 from various IC agencies. 131 Again, Senator Wyden led the floor discussion, this time highlighting concerns about “targeting mistakes,” “about” collection, and the implications of upstream/downstream collection—namely “you don’t even have to be communicating with one of the government’s targets to be swept up . . . law abiding Americans who have done absolutely nothing wrong, both overseas and in the United States can have their communications collected.” 132 Ultimately, Senator Wyden called for more information to assess the privacy impact of Section 702 and whether “liberty and security are not mutually exclusive”. 133

Should there be safeguards against reverse targeting? Should Congress legislate on “upstream” collection and collection of

126 Id. at S379–81.
127 Id. at S382–83 (statement of Sen. Sanders).
128 Id. at S385 (statement of Sen. Wyden).
129 Id. at S383 (statement of Sen. Lankford).
133 Id. at S1817.
communications about targets which raises unique concerns about the collection of the communications of law-abiding Americans? Are the rules related to dissemination, use, and retention of these communications adequate? Should there be limits on the use of these communications by the FBI for non-intelligence purposes? \(^\text{134}\)

With the debate keyed up along these lines, Congress began to experiment. In the House, Representative Tulsi Gabbard (D-HI) introduced legislation to amend FISA to “codify the prohibition on the acquisition of ‘about’ communications under Section 702.” \(^\text{135}\) Her bill, H.R. 2588, never made it out of committee. \(^\text{136}\) Conversely, Senator Tom Cotton (R-AR)—long a supporter of FISA—introduced a bill “that would reauthorize Section 702 permanently, as it is, with no changes.” \(^\text{137}\) In his view, concerns about Section 702 were exaggerated: “we can’t tie the hands of our national security officials at the precise moment that our enemies are taking the gloves off,” suggesting that “if you are concerned about protecting Americans’ privacy rights, then you should support extending 702 [given its host] of privacy protections.” \(^\text{138}\) His bill, S. 1297, also never made it out of committee. \(^\text{139}\) Clearly, neither a band-aid fix nor the status quo would do, even though AG Jeff Sessions and DNI Daniel Coats requested reauthorization “without amendment beyond removing the sunset provision.” \(^\text{140}\) In the months preceding reauthorization, a flurry of proposals flooded Congress.

**The USA Liberty Act (H.R. 3989)** was first introduced by the House Judiciary Committee. The bill “proposed a new framework of protections and transparency requirements to ensure that the government’s use of Section 702

---

\(^{134}\) Id.

\(^{135}\) 164 CONG. REC. H4423 (daily ed. May 22, 2017).


\(^{138}\) Id.


accords with principles of privacy and due process." Among many reforms, the bill would require: a national security purpose to query data collected; law enforcement to receive individualized court orders based on probable cause to view the content of communications collected on a Section 702 program (excluding metadata), logging queries, and strengthening oversight. The bill would also ban “about” collection programs, improve the PCLOB and whistleblowing protections, and encourage the IC to share information among themselves and foreign allies.

The FISA Amendments Reauthorization Act of 2017 (S. 2010) was introduced in the Senate within weeks of the USA Liberty Act. It took the opposite approach to scaling back Section 702. It would give permission to the IC to conduct “about” collection, pending a review of a formal DNI report and FISC certification for any resumed programs. Nevertheless, the bill would prohibit the use of Section 702 intelligence for law enforcement purposes, except for certain serious enumerated offenses, mainly related to terrorism. Perhaps most importantly, it would extend the ability to temporarily surveil U.S. citizens abroad without a FISC order in emergency situations if there was related exigency to surveil a connected non-U.S. person.

The USA Rights Act (S. 1997) was Senator Wyden’s proposed solution (a companion legislation was introduced in the House by Representative Zoe Lofgren (D-CA)) and featured perhaps the most radical paring back of Section 702. The bill would end backdoor searches by requiring a warrant for law enforcement to search for Section 702 intelligence. Moreover, it would ban

---

142 Id.
144 Id. § 5.
145 Id. § 6.
"about" collections in non-terrorism investigations and clarify that "reverse targeting" is prohibited (i.e., using Section 702 to target a foreigner, but really with the intention to access communications with a U.S. person). The bill sought to "place stronger statutory limits on the use of unlawfully collected information" and require the FISC to have an appointed Constitutional Advocate to argue against the government.

The FISA Amendments Reauthorization Act of 2017 (H.R. 4478) tracked closely with Senate version of the same name. In addition, it would require annual approval of querying procedures, publication of minimization procedures, "new procedures for unmasking Americans' names in intelligence reports," additional reporting requirements to Congress, and the temporary suspension of "about" collection pending Congressional review. But it differed in its approach to querying procedures. Whereas the Senate bill would require the FBI to inform the FISC of any query hitting on U.S. persons as a way to guarantee consistency with the Fourth Amendment, the House bill would not require such an individualized approval but would provide the FBI with the opportunity to receive a FISC order based on standard probable cause. Despite these differences, commentators were surprised that the bill also mirrored The USA Liberty Act in its minimization declassification

702 to deliberately conduct warrantless searches for the communications of specific Americans.

147 Id.
148 Id.
150 See George W. Croner, The Gun Lap: FISA Renewal in the Homestretch FOREIGN POLICY RESEARCH INSTITUTE (Dec. 6, 2017), https://www.fpri.org/article/2017/12/gun-lap-fisa-renewal-homestretch/ ("The SSCI bill, for example, includes a provision requiring that the FBI inform the FISC (within one business day) of any query that "returns information that concerns a known United States person . . .. The HPSCI bill takes a somewhat different route. There is no requirement that any form of individual query be cleared by the FISC; however, in those instances where a query of the Section 702 database is not designed to extract foreign intelligence information (i.e., is undertaken for law enforcement inquiries), the HPSCI bill furnishes the FBI with the option of applying for an order from the FISC . . ..")

124
procedures and mandating "specific procedures regulating the ‘unmasking’ of U.S. person identities [caught up in Section 702 surveillance] as part of a broadening of existing statutory minimization requirements." 151

Between these four proposals, Congress had plenty of options for reforming Section 702 before its expiration date. Many other floor amendments were proposed, 152 but conceptually the USA Liberty and the USA Rights Act stood for a paring back of Section 702 authority whereas the dually named FISA Reauthorization Act bills arguably stood for the opposite. 153 Ultimately, the bill that became law was the product of reconciliation of the two FISA Reauthorization Act bills by the House and Senate Judiciary and Intelligence Committees. But given the Congresspersons' concerns about Fourth Amendment violations from "about," backdoor, and reverse targeting collection, what accounts for the ratcheting up of Section 702?

The legislative history suggests a complex story and hardly a partisan one. 154 The possibility for reform was most possible in the House where 58 Republicans and 125 Democrats voted for the USA Rights Act, whereas 65 Democrats joined 178 Republicans to vote for the bill (S. 139) that would become law. 155 Republicans who supported S. 139 believed that the USA Rights Act "would begin resurrecting the information-sharing walls between national security and law enforcement that the 9/11 Commission identified as a major factor in the failure to identify and thwart the 9/11 plot." 156 They believed S. 139 was "drafted in the spirit of the USA Liberty Act" and,

151 Id.


154 Indeed, the bill that became law, S. 139, began as the Rapid DNA Act—"a bill to expand the use of DNA in law enforcement." See GovTrack Summary of S. 139 (Jan. 14, 2018), https://www.govtrack.us/congress/bills/115/s139/summary (supporting that legislation evolves in complex ways).

155 Croner, supra note 122.

consequently, was a bipartisan solution that allayed privacy concerns.\(^{157}\) For example, one Congressman thought the bill struck the right balance—"rather than ending 'abouts' [sic] collection . . . if NSA wants to reestablish 'abouts [sic] communication' collection, [the] NSA would first need to go back to court, [and] convince the judge that it has satisfied the court’s concern."\(^{158}\) Most Democrats did not agree. They argued that:

S. 139 fails to address the core concerns of Members of Congress and the American public—the government’s use of Section 702 information against United States citizens investigations that have nothing to do with national security. The warrant “requirement” contained in the bill is riddled with loopholes and applies only to fully predicated, official FBI investigations, not to the hundreds of thousands searches the FBI runs every day to run down a lead or check out a tip. S. 139 exacerbates existing problems with Section 702 by codifying so-called “about collection,” a type of surveillance that was shut down after it twice failed to meet Fourth Amendment scrutiny. S. 139 is universally opposed by technology companies, privacy, and civil liberties groups across the political spectrum from the ACLU to FreedomWorks.\(^{159}\)

A significant number of Republicans were apt to agree. Libertarian conservatives, some part of the House Freedom Caucus, were equally concerned about backdoor searches and “about” collections, urging their colleagues to force the government “to get a warrant [and] stay out of the house of communications.”\(^{160}\) Nevertheless, some Democrats believed “[they had] to come down in favor of honoring our Constitution and our civil liberties, but [could not] do that completely at the expense [of national security].”\(^{161}\) “They believed the USA Rights act “would disable 702.”\(^{162}\)

Despite a last minute effort by Representatives Justin Amash (R-MI) and Zoe

\(^{157}\) Id. at H1145 (statement of Rep. Goodlatte).

\(^{158}\) Id. at H1143 (statement of Rep. Conaway).

\(^{159}\) Id. at H1146 (statement of Rep. Lee).

\(^{160}\) Id. at H1145 (statement of Rep. Poe).

\(^{161}\) Id. at H1148 (statement of Rep. Pelosi).

\(^{162}\) Id. at H1154 (statement of Rep. Goodlatte).
Lofgren (D-CA) to save the USA Rights Act, S. 139 prevailed to preserve most of the status quo and reject the best chance of Section 702 reform.\textsuperscript{163}

Proceedings in the Senate followed in a similar fashion despite initial uncertainty resulting from a tweet by President Trump as to whether he supported S. 139.\textsuperscript{164} Overall, the failure of major reform efforts is likely the result of a few trends. First, leadership in both the House and Senate opposed FISA reform. Notably, House Speaker Paul Ryan (R-WI) and Minority Leader Nancy Pelosi (D-CA) opposed the USA Rights Act, which likely helped whip up support for S. 139.\textsuperscript{165} Second, of the 28 freshman Republicans elected to the House in the 2016 Trump wave, 24 voted for S. 139 in line with the White House’s direction, which now seemed to give credence to the belief that the current Executive branch embraced Section 702 as a critical tool rather than

\begin{footnotesize}
\begin{enumerate}
\item Id. at H160 (recording failure to pass the Amash-Lofgren amendment).
\item Martin Matishak, Trump Undercuts White House Stance Hours before Critical Surveillance Vote, POLITICO (Jan. 11, 2018, 9:21 AM EST; updated Jan. 11, 2018, 1:43 PM EST), https://www.politico.com/story/2018/01/11/trump-surveillance-fisa-vote-279321 (detailing how Trump made two contradictory tweets before the reauthorization vote, one indicating his desire for reforms to Section 702 and the other indicating he would like to proceed with the status quo. The confusions almost completely derailed the reauthorization vote.). In the Senate, 43 Republicans and 23 Democrats voted for S. 139. Despite discussion of potential filibuster, the Senate vote was far less contentious, see Ashley Killough & Ted Barrett, After Unexpected Scare, Senate Overcomes Filibuster and Advances FISA Extension Bill, CNN (Jan. 16, 2018), https://www.cnn.com/2018/01/16/politics/senate-fisa-bill/index.html.
\item Gopal Ratnam, With House Passage of FISA Measure, Action Moves to Senate, ROLLCall (Jan. 11, 2018, 3:11 PM), https://www.rollcall.com/news/politics/house-passage-fisa-measure-action-moves-senate ("In an unusual alignment, House Speaker Paul D. Ryan and Minority Leader Nancy Pelosi opposed the Amash-Lofgren amendment, saying that it would weaken intelligence agencies' ability to stop terror plots in a timely fashion.").
\end{enumerate}
\end{footnotesize}
something to be feared. 166 Of the 27 freshman Democrats, 14 voted for S. 139. 167
Clearly, the 2016 elections ushered in new Congresspersons across the aisle who were sympathetic to a robust Section 702. Whereas the old guard, particularly Tea Party Republicans, were more sympathetic to the USA Rights Act. These new views might not have been dispositive to the result, but they certainly made the margin greater, perhaps to an extent that mounting a realistic reform effort was out of the question. Third, and relatedly, there is reason to believe that the last-minute vote on the USA Rights Act was engineered by Speaker Ryan as part of a compromise with more conservative Republicans. By allowing "one amendment with the changes the bill’s opponents wanted to get a vote," but knowing full well the vote would fail, Speaker Ryan likely converted some Congresspersons on the fence to approve S. 139 "by at least giv[ing] these members the chance to say they got something," (i.e., floor time to speak their grievances to constituents and bemoan the failure of their preferred reform plan, while still letting them support national security with an affirmative vote on S. 139). 168 It does seem that members were flipped in this way when the roll-call votes for the USA Rights Act and S. 139 are compared. 169 At least in the Senate, members

166 See White House Statement of Administration Policy – House Amendment to S. 139 (Jan. 9, 2018), https://www.whitehouse.gov/wp-content/uploads/2017/11/saps139hr_20180109.pdf (stating that “[i]f the House Amendment to S. 139 were presented to the President in its current form, his advisors would recommend that he sign the bill into law.”). Compare Newly elected members to the 115th Congress, BALLOTPEDIA, https://ballotpedia.org/Newly_elected_members_to_the_115th_Congress with S. 139 Roll Call Vote (Jan. 11, 2018), http://clerk.house.gov/evs/2018/roll016.xml (showing the number of new members of Congress and comparing that to the roll call for votes on S. 139).


169 Fifty-eight Republicans voted for the USA Rights Act when it was introduced. Only 45 voted against S. 139. This reduction suggests that 13 members both voted for The USA Rights Act and then voted for S. 139 after the USA Rights Act failed, or at least abstained in the S. 139 vote. Compare S. 139 Roll Call Vote, http://clerk.house.gov/evs/2018/roll016.xml, with The USA Rights Act Roll Call Vote, http://clerk.house.gov/evs/2018/roll014.xml.
switched positions on Section 702 easily, with Senator Feinstein being a notable example.\textsuperscript{170}

Politics certainly matters. And the political currents of the 2016 election undoubtedly shaped Section 702’s ultimate fate. But conceptually, the failure of major reform efforts can be placed into the historical push and pull of electronic surveillance described above. Not unlike the rhetoric deployed at the time the TSP was instituted, Congress was thinking about reforming Section 702 at a specific moment when terroristic threats seemed to be evolving. Frequently, Congresspersons reminded the public that the bombing “attacks like that in London are the new normal, [and] we have to be proactive ... one way to be proactive and keep our country safe is to reauthorize section 702.”\textsuperscript{171} Indeed, the democracy destroying purpose of ISIS featured prominently in the legislative debates—the example of Hajii Iman and Shawn Parsons’s threat to civilian lives were highly relevant cases studies featuring the efficacy of robust Section 702.\textsuperscript{172} And against a threat which seeks to eliminate the very existence of democracy, not the typical foreign state actor, the reauthorization debates implicitly place a robust foreign surveillance tool like Section 702 as necessary, \textit{a priori}, to ensuring a state even exists to create forum for civil liberties.\textsuperscript{173} But this view is one that is historically influenced.

\textsuperscript{170} Evan Halper, \textit{After Calling for Surveillance Reform, Democrats Help Kill It}, L.A. TIMES (Jan. 17, 2018, 11:40 AM PST), http://www.latimes.com/politics/la-na-pol-fisa-democrats-20180117-story.html (“Feinstein broke with privacy advocates from the right and left to cast a crucial vote in favor of leaving the program largely unchanged for the next six years. Feinstein’s retreat back to a hawkish posture on Section 702 of the Foreign Intelligence Surveillance Act (FISA) gave supporters of the status quo the vote they needed to quell a growing movement in the Senate for more privacy protections.”).


\textsuperscript{173} Indeed, this was a consideration of the \textit{Keith} court when contemplating the efficacy of warrantless surveillance for domestic national security purposes: “Unless the Government safeguards its own capacity to function and preserve the security of its people, society itself could become so disordered that all rights and liberties might be endangered.” \textit{Keith}, 407 U.S. at 312; \textit{see also} Cox v. New Hampshire, 312 U.S. 569, 574 (1941) (“Civil liberties, as guaranteed by the Constitution, imply the existence of an organized society maintaining public order without which liberty itself would be lost in the excesses of unrestrained abuses.”). Nevertheless, the “recognition of these
When government abuses national security tools to make that forum impossible, *a posteriori*, the focus of the debate shifts to ask what principles the nation is actually protecting. To put it differently—and to paraphrase Benjamin Franklin—if we sacrifice liberty for national security, do we get neither? Or, if we sacrifice national security for liberty, do we also get neither? These questions are essentially the same but framed differently. And yet in different historical moments, the question is often asked in one way or another. This framing matters because it tilts the balance toward that which is being potentially sacrificed. The threat of ISIS, global terrorism, and the success of Section 702 placed civil liberty advocacy in the tough position of having to address the second framing: is national security worth sacrificing given these clear threats? But if these tools get abused, these advocates will benefit from being able to reframe the question and better reform Section 702 authorities. In the face of its enormous potential and success as a surveillance tool, 2017 was a difficult historical moment to push for major reform, even with credible concerns about abuse. The fluidity of this historical framing is a constant feature of electronic surveillance debates. But regardless of this changing context, whether the reformed Section 702 complies with the Constitution will remain a standard question.

---

elementary truths does not make the employment of by the Government of electronic surveillance a welcome development" disregarding completely the Bill of Rights. *Keith*, 407 U.S. at 313.

174 Although, “in the post-Snowden revelations era [there is an] absence of credible allegations of political or venal use of 702 authorities. In essence, the public evidence confirms that the problems that used to bedevil secret electronic surveillance through the Hoover/Nixon era—namely, senior political figures deploying intelligence agencies and tools for inappropriate, abusive political purposes—have been resolved by a robust legal regime of oversight and reporting.” Jack Goldsmith & Susan Hennessey, *The Merits of Supporting 702 Reauthorization (Despite Worries About Trump and the Rule of Law)*, LAWFARE (Jan. 18, 2018, 9:20 AM), https://www.lawfareblog.com/merits-supporting-702-reauthorization-despite-worries-about-trump-and-rule-law. In other words, absence of credible abuse may have helped kill the major reform efforts more than anything else—the historic moment did not compare to the abuse of electronic surveillance in the 20th Century. *See id.*
III. **THE REAUTHORIZATION ACT’S REFORM TO SECTION 702**

Section 702 has withstood frequent constitutional challenge. Whether it continues to succeed as a constitutionally viable law will depend on its recent changes. When President Trump signed S. 139 into law, Section 702 changed in the following ways:

- **Querying Procedures:** The AG and DNI must now adopt certain procedures that will regulate how intelligence analysts search databases of raw Section 702 intelligence. These querying procedures are subject to FISC review for compliance with the Fourth Amendment. Additionally, procedures must be adopted which keep “record of each ‘United States person query term’ used.” The FBI must get a court order on grounds of probable cause to access Section 702 intelligence communications “responsive to U.S. person search terms where the query ‘was not designed to find and extract foreign intelligence information’ and instead is performed ‘in connection with a predicated criminal investigation’ unrelated to national security.” Here, predicated criminal investigation likely means one that is beyond its initial stage, but already has some semblance of probable cause of illegality. But an order may not be required if there is a reasonable threat of serious harm or death.

- **Criminal Proceedings.** The reforms go on to detail the circumstances where a U.S. person’s data collected by a Section 702 surveillance can

---


176 Id.

177 Id.

178 See Croner, supra note 122 (“It would have been helpful to have defined “predicated criminal investigation,” but the statute is silent, so one is left to assume that it is an investigation that has moved beyond a preliminary assessment of suspected criminal activity that is unrelated in any way to national security; i.e., your garden variety criminal investigation conducted through the FBI’s criminal investigative division.”).

179 See Kohse, supra note 173.
be used in a criminal investigation. The FBI must otherwise get a court order described above or the criminal proceeding must "involve one of an enumerated list of conduct, including death, kidnapping, serious bodily injury, crimes against minors, incapacitation of critical infrastructure, cybersecurity, and transnational crime." \(^{180}\) Regardless, reporting requirements to Congress now exist to mandate disclosure of the use of Section 702 intelligence for law enforcement investigations against U.S. persons.\(^{181}\)

- **"About" Collection.** The new reforms do not ban "about" collection but allow the IC to resume such collection if it so chooses (i.e., should the NSA so choose since voluntarily ceasing such activities in 2017 amidst compliance concerns).\(^{182}\) However, the DNI and AG must inform Congress prior to restarting the program and provide a FISC opinion approving any specific program and "a summary of the protections in place to detect any material breach." \(^{183}\) The IC can begin "about" collection after the period of Congressional notice if any exigency exists. Anytime a material breach occurs in the program's protections, Congress must now be notified.\(^{184}\) Finally, because restarting about collection on approval of the FISC will likely "present a novel or significant interpretation of the law," amici briefs will be considered as to this question.\(^{185}\)

Overall, there were many more reforms made to Section 702, especially for transparency, including: publication of minimization procedures after declassification, increased whistleblower protections, review of applicable classification systems, strengthening of the PCLOB, increased capacity in civil liberties offices across the FBI and NSA, and clarification of the Section 705 emergency provision.\(^{186}\) However, the reforms to querying procedures and

---

\(^{180}\) Id.

\(^{181}\) Id.

\(^{182}\) See Jurecic, supra note 107 (explaining why the NSA stopped "about" collections).

\(^{183}\) Id.

\(^{184}\) Id.

\(^{185}\) Id.

\(^{186}\) Id.
“about” collection are most relevant to a re-evaluation of the Section 702’s constitutional compliance. The querying reforms might help assuage concerns about backdoor searches, but Gregory Croner has noticed that the FBI still has significant leeway. He points out that the querying reforms are merely a:

Political gesture offered to appease critics rather than seriously constrict access to the Section 702 database for foreign intelligence purposes. For example, after creating this new ‘querying’ limitation in purely criminal cases, the FISA Reauthorization Act hastens to point out that the FBI is relieved of any obligation to seek a FISC order: (1) where the FBI is conducting lawful queries of the Section 702 database (i.e., queries directed to producing foreign intelligence information); or (2) where the results of an FBI query are “reasonably designed to find and extract foreign intelligence information, regardless of whether such foreign intelligence information would also be considered evidence of a crime;” or (3) where the FBI query is initiated to evaluate “whether to open an assessment or predicated investigation relating to the national security of the United States;” or (4) where the query is initiated upon reasonable belief that the content of Section 702 communications “could assist in mitigating or eliminating a threat to life or serious bodily harm.”

Consequently, the strength of Section 702’s fundamental authorities, pending “about” collection re-evaluation, has been left intact notwithstanding the transparency reforms enacted.

IV. REEVALUATING POINTS OF CONSTITUTIONAL CONTENTION

There are open questions in the aftermath of Section 702’s reauthorization—not least of which is whether Congress was even aware of the full-extent of Section 702’s use to make an informed decision. Regardless, the program’s

---


188 Some commentators argue that “we don’t know how the government is using Section 702 data, but we do know that it is singling out communities for increased scrutiny based on country of origin, faith, and race. The administration has deemed illegal immigration as a leading national security threat, and President Trump has even said that legal immigration poses a national security threat.” Robyn Greene, *Americans Wanted More Privacy Protections. Congress Gave Them Fewer*, SLATE (Jan. 26, 2018;
expansion reopens the viability of constitutional challenge in areas where litigation has previously failed. Namely, the program’s changes to querying procedures and the possibility of restarting “about” collection are arguable violations of the Fourth Amendment. While the “course of true law pertaining to the [Fourth Amendment] . . . has not . . . run smooth[ly]”\textsuperscript{189} because it suffers from “both the virtue of brevity and the vice of ambiguity,”\textsuperscript{190} a few basic requirements are clear. First, only government surveillance that meets the Jones-Katz requirements\textsuperscript{191} will count as a “search” implicating the Fourth Amendment. Second, any such searches must be “reasonable.” And third, a warrant must be obtained to carry out these searches, unless an exception applies. Querying and “about” collection arguably violates each of these three requirements.

First, given the amount of incidental information that can be acquired in Section 702 surveillance (particularly “about” surveillance), it is no longer plausible under the Katz factors to claim the program does not amount to a Fourth Amendment search because it only targets foreigners abroad. Nevertheless, this question has not been directly addressed by the Supreme Court, and its resolution might greatly narrow the government’s ability to carry out the program.

Second, assuming Section 702 does involve Fourth Amendment searches, there is a strong argument that such searches are unreasonable. Trends in case law involving government searches using technology imply an uneasiness with technology that can acquire large amounts of information on a person. With increased collection ability, courts are becoming concerned that the government can acquire a mosaic of information that penetrates the most private aspects of a person’s life.\textsuperscript{192} As Section 702 collects more incidental

\textsuperscript{190} JACOB W. LANDYNISKI, SEARCH AND SEIZURE AND THE SUPREME COURT: A STUDY IN CONSTITUTIONAL INTERPRETATION 42 (1966).
\textsuperscript{191} See supra PART II.A. for a discussion of Katz and Jones.
information on U.S. persons, it surely triggers the same concerns that courts are increasingly striking down as unreasonable Fourth Amendment searches.

Third, even if Section 702 searches are considered reasonable, it is not clear that current Section 702 FISC orders can be considered warrants as contemplated by the Fourth Amendment. If they are not, then the government can only conduct such searches if an exception to the warrant requirement applies. Here, the special needs exception and the incidental overhear exception (the -often-cited exceptions justifying warrantless FISA searches) do not easily apply for Section 702’s new querying procedures and for “about” collection.

In sum, the new querying procedures and “about” collection authorizations are susceptible to constitutional challenge on just about every front of Fourth Amendment jurisprudence. The following discussion lays out the applicable doctrine for each of the three Fourth Amendment requirements and previews the legal analysis that might soon be presented to courts reviewing the Reauthorization Act.

A. Querying and “About” Collection are Fourth Amendment Searches

As mentioned above, the foreign intelligence surveillance doctrine established in Keith lays the foundation for FISA surveillance under a theory that surveillance targeting foreigners implicates less privacy concerns than domestic surveillance. As such, this surveillance does not amount to a Fourth Amendment search. But as commentators note, by passing Section 702 Congress “specifically authorized programmatic warrantless foreign intelligence surveillance in a manner almost guaranteed to sweep up a substantial volume of communications involving U.S. persons.”^193 And so the debate between courts like Troung Dinh Hung and Zweibon v. Mitchell remains a continuous issue: is it really the case today that foreign intelligence surveillance targeting foreigners abroad does not implicate privacy concerns of U.S. persons caught up in the surveillance? And would requiring

compliance with the Fourth Amendment frustrate the Executive’s Article II power?

As to the first, it seems hard to believe that individuals do not have a recognizable expectation of privacy over the content of their communications that are increasingly swept up, and subject to review, by Section 702:

[T]he 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.194

As to whether complying with the Fourth Amendment will frustrate the Executive, that does not seem to be the case with the current operation of the FISC. While the FISC rarely rejects FISA or Section 702 applications,195 the process of approving such generalized requests has hardly reduced the amount of people the government has surveilled under these programs.196 The Supreme Court has explicitly rejected arguments that lack of resources or

---

194 Goitein & Patel, supra, note 65, at 21.
195 “From 1996 to 2013, less than 0.032 percent of applications were denied, even though requests grew by more than 200 percent.” Id. at 37 (citing Admin. Off. of the U.S. Cts., Wiretap Rep. tbl. 7 (2013); Admin. Off. of the U.S. Cts., Wiretap Rep. tbl. 7 (2002)).
196 See generally Statistical Transparency Report Regarding the Use of National Security Authorities—Calendar Year 2017, Office of the Director of National Intelligence, https://www.dni.gov/files/documents/icotr/2018-ASTR-CY2017-FINAL-for-Release-5.4.18.pdf (while exact numbers may be hard to specify with certainty, the ODNI lays out a steady increase in the estimated targets of Section 702 orders, increasing from roughly 89,000 in 2013 to about 129,000 in 2017. These numbers likely do not account for the number of individuals incidentally caught up in the surveillance.).
strain on the Executive automatically obviates the warrant requirement.\textsuperscript{197} Thus, as a matter of operation, FISA surveillance does constitute "searches" under the Fourth Amendment—particularly because the government has done just fine complying with procedural restrictions enacted by Congress. Even if such searches focus on metadata or individual information not subject to privacy protections, courts are "take[ing] a more holistic and less formalistic view of the government's actions and examine[ing] what the government is really learning about us when it collects and processes massive amounts of data."\textsuperscript{198} Enough "non-searches" can amount to a constitutionally recognized search when a government program is viewed holistically.\textsuperscript{199}

As discussed above, the Supreme Court never had to explicitly address the Katz framework left open by Keith in the foreign intelligence space because Congress essentially assumed foreign surveillance did constitute a Fourth Amendment search by creating FISA procedures which mimic Title III warrant processes.\textsuperscript{200} Nevertheless, if the Supreme Court were to wholly review Section 702, it might be compelled to once and for all declare such foreign surveillance as Fourth Amendment searches when U.S. persons are involved. Such a finding would hardly be surprising given FISA's development. But how the Supreme Court—or even lower courts—opine on the scope of these searches, and its interaction with Article II powers, will have ramifications on how "reasonable" they are when conducted by increasingly

\textsuperscript{197} See United States v. Karo, 468 U.S. 705, 718 (1984) (rejecting the Government's argument that an obligation to obtain warrants for monitoring beepers withdrawn from public view would lead to the Government obtaining warrants in a large number of cases as unpersuasive); see also Zweibon, 516 F.2d at 636-37 (recognizing the U.S. Supreme Court's warning that arguments regarding the foreign intelligence warrant exception cannot be based on the length of time needed to obtain the warrant or the potential amount of warrants necessary to comply).


\textsuperscript{199} Indeed, this is the general theory of the mosaic theory: government acquisition of seemingly inconsequential personal information can, when added together, amount to such an intrusive holistic picture into an individual's life that it can implicate the Fourth Amendment. For a full explanation, including criticism, see generally Orin Kerr, The Mosaic Theory and the Fourth Amendment, 111 MICH. L. REV. 311 (2012).

\textsuperscript{200} See supra Part II.A.
intrusive and advanced surveillance methods. Here is where future litigants have room to argue, particularly for "about" searches. Not only do these collection methods count as Fourth Amendment searches, but they are so broad that no argument can make them reasonable, even when interacting with the Executive's Article II powers related to foreign affairs and national security. The scope of these Article II powers in this space will undoubtedly influence the means by which the government can continue to adapt its surveillance methods under Section 702. Indeed, courts seem to care about the mode by which the government intrudes as part of the search analysis. Consequently, litigation against Section 702 might proceed by challenging specific types of surveillance (e.g., upstream) as not only searches, but unreasonable per se by nature of its technology alone.

B. Newly Authorized Section 702 Searches are Unreasonable

Litigants need not focus too much on the scope of whether a search occurred because current case law suggests courts are increasingly amendable to finding overbroad technological collection as unreasonable, even in the metadata space. "A search is not beyond Fourth Amendment scrutiny; for it must be reasonable in its scope and manner of execution." Scholars have pointed to the D.C. District Court in Klayman v. Obama as portending a shift among courts to reign in the definition of reasonableness in the intelligence collection context, particularly with new trends in the Supreme Court's Fourth Amendment jurisprudence. Klayman was a successful challenge to the FISA Section 215 metadata program on unreasonableness grounds, but its

201 See, e.g., State v. Bonnell, 856 P.2d 1265, 1276–77 (Haw. 1993) (finding that the mode of government intrusion matters as to whether government surveillance counts as a Fourth Amendment search).
implications are far reaching. 204 \"The Klayman court emphasized that one of the driving purposes behind the Fourth Amendment is to prevent the government from acquiring a significant amount of private information without a judicial determination of probable cause.\" This concern is equally implicated with Section 702, particularly regarding incidental \"about\" collection. Instructive too is how the FISCR treated the predecessor to Section 702 in In re Directives. 205 The court determined that the special needs exception to warrant requirement applies \"when surveillance is conducted to obtain foreign intelligence for national security purposes and is directed against foreign powers or agents of foreign powers reasonably believed to be located outside the United States.\" 206 Again, scholars note that \"a strict reading of the In re Directives foreign intelligence exception would result in a determination that Section 702 does not qualify for this exception to the warrant requirement.\" 207 The court in In re Directives upheld the Section 702 predecessor on reasonableness grounds but based on protections that were not replicated when Section 702 was updated in 2008 and in subsequent years. 208

These cases demonstrate a willingness for FISA courts and district courts to strike down provisions of statutes similar to Section 702 on Fourth Amendment reasonableness grounds and a narrower conception of the special

---

204 See generally Klayman, 957 F. Supp. 2d 1, 41 (D.D.C. 2013) (holding that the phone record metadata collection constituted a search under the Fourth Amendment and that Klayman was likely to succeed in demonstrating that the government’s searches were unreasonable under the Fourth Amendment).

205 See In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008) (reviewing the identical predecessor to Section 702 under the 2007 short-lived Protect America Act and holding that directives issued to the petitioning service provider under the Protect America Act satisfied the Fourth Amendment’s reasonableness requirement).

206 Id. at 1012 (emphasis added).

207 Walsh, supra note 200, at 786.

208 See id. at 787 (\"Unlike the PAA, section 702 does not require a determination that \"probable cause existed to believe that the targeted person is a foreign power or an agent of a foreign power.\" This negatively affects both sides of the balancing test as applied to section 702. Without a connection to a foreign power, the government interest in national security is reduced. \ldots \" (quoting In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008)).
needs exception described below. They also portend precedent that does not quite match with the increasingly expansive Section 702. The FISC court will have to squarely face this issue if the government decides to reactivate “about” collection programs as part of the recent reauthorization. Whether “about” collection passes reasonableness muster might very well hinge on the changing privacy implications at the core of the third-party doctrine. In United States v. Jones, the concurring opinions contemplate the fact that “it may be that [long-term surveillance] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy.”\(^{209}\) Indeed, the surveillance data collected via the third-party doctrine is so much more intrusive in the information era than the phone records which spawned the creation of the doctrine in Smith v. Maryland.\(^{210}\) A mosaic of data points can pierce one’s private life in intricate detail, even when incidentally collected.\(^{211}\) The reasonableness prong of the Fourth Amendment turns on a balancing test between privacy interests and security interests that has frequently favored an expansive interpretation of Section 702. But if the Court amends the reach of the third-party doctrine based on “technological advances that have made possible non-trespassory surveillance techniques” courts may very well lean on cases like Klayman and In re Directives to preserve “the evolution of societal privacy expectations.”\(^{212}\) Future cases might address the so-called equilibrium-adjustment theory whereby the Court does and should update Fourth Amendment rules to maintain the balance of government power as technology changes. The idea that is that some technological shifts so transform the level of government investigative power (whether expanding it


\(^{210}\) See Smith v. Maryland, 442 U.S. 735, 742–43 (1979) (holding that a pen register does not constitute a search under the Fourth Amendment because individuals do not have a subjective or societal reasonable expectation of privacy in regard to their phone numbers).


\(^{212}\) Jones, 565 U.S. at 414–15 (Sotomayor, J., concurring).
or restricting it) that they justify new rules to restore the prior level of government power.213

The outcome of Carpenter v. United States, which evaluated the bulk collection of cell-site data, seems to confirm this theory by recognizing that "seismic shifts in digital technology" which produce "deeply revealing" amounts of information can constitute a search, regardless of the third-party doctrine.214 In other words, people have a cognizable privacy interest in the information they give to third parties, particularly when this information reveals more as its collected and evaluated in bulk. Each individual data point may not violate any privacy interests. But when technology permits the government to put together a complex mosaic made of these individual points, the resulting picture can implicate Fourth Amendment protections. While the Court clarified that its holding "does not consider other collection techniques involving foreign affairs or national security," Carpenter will provide ammunition for those who will argue that bulk collection programs constitute protected searches. These arguments might restrict the government’s ability to search unminimized data or the breadth of "about" collection.

C. Exceptions to the Warrant Requirement Do Not Apply

Even assuming Section 702’s newest authorities are considered reasonable searches, they still need go through a warrant process to comply with the Fourth Amendment. Whether or not current Section 702 FISC orders are considered permissible warrants is still an open question. In the regular FISA context—where the FISC approves individualized orders to surveil agents of foreign powers—the answer is clearer. In re Sealed Case held that the pre-2008 FISA “did not itself violate the Fourth Amendment, at least largely because FISA warrants were probably still effectively ‘warrants’ within the meaning of


214 See generally Carpenter, 138 S. Ct. at 2217 (holding that the Government usually must obtain a search warrant in order to request cell location information from a wireless carrier).
The alternative argument was that the Keith and Troung Dinh Hung line of cases creates a foreign intelligence surveillance exception to the warrant requirement because of the strain such a warrant would place of the Executive's Article II responsibilities and due to the minimal privacy implications. But as discussed above, both of these arguments seem operationally unpersuasive, and In re Sealed Case refused to "endorse a categorical foreign intelligence surveillance exception" to warrant requirement by effectively holding traditional FISA warrants as in compliance with the Fourth Amendment.

But with Section 702, FISA warrants are no longer necessary for surveilling foreigners abroad, just programmatic FISC orders. If In re Sealed Case did not opine on pre-Section 702 compliance with the foreign intelligence exception, then whether Section 702 complies with the exception is an open question. This question is especially important considering that the exception is based on the Keith rationale that foreign surveillance does not require a warrant because privacy interests are not as implicated compared to domestic surveillance. Given Section 702's expansion, that is an assumption worth reevaluating, particularly as it relates to the reasonableness of searches. This question was one the plaintiffs sought to address in Clapper v. Amnesty International. As that case was dismissed on standing grounds, the issue remains a live question that could upend Section 702 in favor of the government.

216 See id. (discussing the origins of the foreign intelligence exception to the Fourth Amendment's warrant requirement).
217 Id.
219 Id. at 402 (holding that "respondents cannot manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending. We therefore hold that respondents lack Article III standing."); id. at 422 (preserving the core of the merits by noting that "any dissatisfaction that respondents may have about the Foreign Intelligence Surveillance Court's rulings—or the congressional
Nevertheless, many commentators proceed on the assumption that notwithstanding the uncertainty about the foreign intelligence exception, the special needs and incidental overhear exceptions are more than enough to permit warrantless Section 702 searches. But in this space, litigants have the strongest arguments to challenge the new provisions of Section 702 because neither of the exceptions seem to permit querying of incidentally collected data or “about” collection.

*Griffen v. Wisconsin* made clear that “when special needs, beyond the normal need for law enforcement, make the warrant and probable cause requirement impracticable,” court-issued warrants are unnecessary. Promoting public safety is often considered one such exigency and the FISCR has permitted FISA under these grounds, remarking that such foreign intelligence surveillance “goes well beyond any garden-variety law enforcement objective,” even with the incidental collection of a U.S. person’s data. Although the Supreme Court has never directly endorsed foreign surveillance under the special needs analysis, it would likely accept the FISC’s rationale that there is a “high probability that requiring a warrant” could harm “vital national security interests” that depend on the time sensitive information Section 702 is able to acquire. This view seems especially likely given the holding of *City of Indianapolis v. Edmond*, where the Court recognized stopping a terrorist attack as justification for a suspiciousness search. But the new Section 702 authorities might go beyond this broad exception. Under delineation of that court’s role—is irrelevant to our standing analysis” and therefore remains a live question.

---


222 *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d at 1011 (FISA Ct. Rev. 2008); [Redacted Case Name], 68–69 (FISA Ct. 2011) (Bates, J., mem.).

223 *Id.* at 69.

224 *City of Indianapolis v. Edmond*, 531 U.S. 32, 44 (2000) ("The Fourth Amendment would permit an appropriately tailored roadblock set up to thwart an imminent terrorist attack or to catch a dangerous criminal who is likely to flee by way of a particular route." (citing *Edmond v. Goldsmith*, 183 F.3d 659, 662–63 (7th Cir. 1999)).
the reauthorized Section 702, backdoor searches of incidentally collected data on U.S. persons seem permissible when the investigations are related to foreign intelligence, national security, or imminent threat of injury. Moreover, it seems like law enforcement can search this data at any point, for any purpose, before a fully "predicated" investigation—i.e., before they suspect a particular U.S. person has committed a crime in question, they can query Section 702 databases looking for any connections on which to establish probable cause. The ability for law enforcement to undertake these warrantless fishing expeditions arguably stretches beyond the special needs exception.

In City of Los Angeles v. Patel, the Court clarified the special needs exception as applying in situations where there is a special need and "where the primary purpose of the searches is distinguishable from the general interest in crime control." Consider too some crucial points in Edmond. The Court cited Delaware v. Prouse for the proposition that discretionary roadblocks set for public safety were unconstitutional extensions of the special needs exception primarily because "discretionary, suspicionless stop[s]" constituted an "exercise of standardless and unconstrained discretion"—discretion which could be abused. If warrantless roadblock searches could be permitted under the special needs exception, they would have to apply to all cars or be randomized to prevent abuse of discretion. Additionally, "the Court must consider the nature of the interests threatened and their connection to the particular law enforcement practices at issue." In Edmond, roadblocks designed to stop cars for drug searches were impermissible

225 See Croner, supra note 149 (explaining how a reading of the statute arguably permits backdoor searches where the FBI query is initiated to evaluate "whether to open an assessment or predicated investigation relating to the national security of the United States;" or where the query is initiated upon reasonable belief that the content of Section 702 communications "could assist in mitigating or eliminating a threat to life or serious bodily harm.").

226 Id.


229 Id. at 33.
because searching for drugs is not a law enforcement practice connected to the public safety interest in promoting safe driving (whereas, stopping cars to prevent DUIs is much more clearly connected to promoting safe driving). Applying these principles, the Reauthorization Act's backdoor provisions seem dubious. In the first instance, the significant purpose standard for FISA searches permitted by In Re Sealed Case seems to conflict with the Patel court's clarification that the special needs exception must have a primary purpose distinct from law enforcement. In Re Sealed Case upheld the congressional decision under Fourth Amendment grounds to require only a "significant purpose" of collecting foreign intelligence to receive a FISC surveillance order. Unlike the previous standard, law enforcement could also be a significant purpose so long as collecting foreign intelligence remained significant. It is important to notice the incongruity between the more permissive significant purpose test to begin foreign surveillance and what is permitted under the special needs exception for warrantless searches of U.S. persons in the public safety context. When incidental data on U.S. persons is collected under the significant purpose collection, there might be a problem in later using this information under the more restrictive primary purpose Patel standard. For example, if foreign intelligence is collected with the main aim of prosecuting a foreign terrorist—but nevertheless meets the threshold for a significant foreign intelligence aim—there is an issue if incidental information is picked up. Suppose a potential U.S. person is caught up in this surveillance as a co-conspirator. Because the initial aim of the surveillance had a significant purpose of prosecuting a foreign terrorist, the primary purpose of later using incidental information to prosecute a U.S. co-

---

230 Whereas, stopping cars to prevent DUI's is much more clearly connected to promoting safe driving. Id. at 43 ("Nor can the narcotics-interdiction purpose of the checkpoints be rationalized in terms of a highway safety concern similar to that present in Sitz... only with respect to a smaller class of offenses, however, is society confronted with the type of immediate, vehicle-bound threat to life and limb that the sobriety checkpoint in Sitz was designed to eliminate.").

231 310 F.3d 717 (FISA Ct. Rev. 2002) ("The FISA as amended is constitutional because the surveillances it authorizes are reasonable [under the significant purpose test].").

232 Id.
conspirator is indistinguishable from the crime control purpose in *Patel* if the special needs requirement underpins Section 702. Without a separate warrant/probable cause determination, the very act of conducting a query triggers Fourth Amendment concerns. To conduct a warrantless special needs search, the primary purpose must be distinguishable from crime control. In many cases this requirement is impossible to meet because the data is collected *ex ante* via a FISC order which applies a standard that allows law enforcement purposes to be a substantial reason to implement foreign intelligence surveillance.

Much of the complexity arises from the meaning (or lack thereof) of the "significant purpose" test required for the collection of foreign intelligence. Nevertheless, as the wall between foreign intelligence and law enforcement continues to weaken, an argument can be made that backdoor searches—or even Section 702 surveillance generally—stretches the limit of the special needs exception. This is not the case because the national security interests implicated are not special needs within the doctrine—promoting national security squarely falls under the purview of public safety recognized as the classic exigency within the doctrine. It stretches the limit because the use of the information collected is increasingly tied up in the crime control which the special needs analysis excludes from its purview under *Patel*.

More clearly problematic is the ability for law enforcement to query Section 702 databases before a predicated investigation. To the extent that law enforcement queries data in an unrandomized or exclusive fashion, it would seem no different than the contexts held unconstitutional in *Prouse* or *Edmond*. It might just be data in this situation, but the same abuse of discretion and privacy concerns are still relevant. The implication in *Prouse* was that if officers had full discretion to make any suspicionless stop grounded in public safety reasons, they could use this authority to search people based on race, gender, or any immutable characteristics. Likewise, in *Edmond*, the implication was that impermissible profiling could also be deployed in the drug stop situation. Whether someone is carrying drugs is much less obvious compared to drunkeness. Officers might rely on stereotyping or animus in subjecting individuals to an invasion of privacy to conduct searches. These concerns are present with the pre-predicated backdoor searches: unless the
querying is conducted in the same randomized or all-encompassing way, nothing stops law enforcement from abusing its discretion in similar ways.

There are undoubtedly some caveats to these cases. For one, it can be argued that querying can be conducted in a randomized way. Plus, when law enforcement seeks to prosecute under terrorism statutes, there might be enough of a connection to the special need of national security to pass muster under Prouse/Edmond. Not to mention the Patel case was decided in the administrative search context (i.e., ordinance compliance), so it is not completely clear its clarification of the special needs analysis maps onto the foreign intelligence surveillance context. Additionally, some courts have held that "subsequent querying of a Section 702 collection, even if U.S. person identifiers are used, is not a separate search" which "does not make Section 702 surveillance unreasonable under the Fourth Amendment." But many courts have found in other contexts that "subsequent querying of the information after acquisition is a search requiring a warrant." Thus, it is an open question whether Section 702 querying by law enforcement is a separate search from that of the initial intelligence collection. If so, Fourth Amendment concerns are heavily implicated. Regardless, the Reauthorization Act extends Section 702 authority far enough to at least allow reasonable grounds for litigation in this area. And the Supreme Court’s decisions in "United States v. Jones and Riley v. California show that at least some Justices recognize the heightened potential for governmental overreach in an age when digital records are kept on nearly every aspect of our lives . . . now more than ever, because of their heightened vulnerability to government abuse in the Information Age." Indeed, some suggest that technological advancement

---

233 See, e.g., MacWade v. Kelly, 460 F.3d 260, 263–64 (2d Cir. 2006) (explaining that lower courts have endorsed the applicability of the special needs doctrine, at least in the national security context).


235 Id. at *24 (citing United States v. Sedaghaty, 728 F.3d 885, 910–13 (9th Cir. 2013) (computer search)); United States v. Young, 573 F.3d 711, 720–21 (9th Cir. 2009) (searching a backpack after accessing a hotel room); United States v. Mulder, 808 F.2d 1346, 1348 (9th Cir. 1987) (laboratory testing of pills).

can actually help reduce the use of the special needs exception—with one suggestion calling on courts to “use statistical forecasting to measure whether continued surveillance is necessary to address the special needs of law enforcement.”

As to the potential application of the so-called “incidental overhear” exception, similar doctrinal concerns are implicated. Before reauthorization, three district courts—United States v. Mohamud, United States v. Muhtorov, and United States v. Hasbajrami—heard cases challenging Section 702, all of which upheld the program citing the foreign intelligence exception to the warrant requirement and its reasonableness after a balancing of interests. But these cases failed to appreciate the incidental overhear arguments that defendants were making about incidental collection under Section 702. The incidental overhear doctrine was established in the Title III context where “defendants argued that their own communications were acquired unlawfully because they were not identified by name in [search] orders.” Essentially, law enforcement placed a wiretap on a suspect that incidentally caught incriminating evidence on bystanders, who were never targeted in the initial warrant. Nevertheless, the Supreme Court held that it was not unlawful to introduce this incidentally overheard evidence so long as the warrant in dispute was sufficiently particularized: “identify[ing] the phone line to be tapped and the conversations to be acquired, and the government followed rigorous ‘minimization’ procedures to avoid the collection of ‘innocent conversation.’” In many ways, FISA’s own procedural requirements map onto these same restrictions. But if the courts conceive of these protections as

240 Id.
something more—as creating an exception to the warrant requirement for incidentally collected communications—then Section 702 seems further insulated from constitutional challenge.

Indeed, this jump is what the *Mohamud, Muhtorov, and Hasbajrami* courts have assumed by including incidental U.S. person data within the foreign intelligence exception. Yet they are two different issues. It is one thing to say Section 702 surveillance is permitted without a warrant due to the *Keith* foreign intelligence exception. Yet is quite another to say incidental data are swallowed by this exception because the Supreme Court has permitted such an overlap in the criminal investigation context. Elizabeth Goitein frames the issue accordingly:

> If Americans have a reasonable expectation of privacy in their communications with foreigners overseas, then the ‘incidental overhear’ cases would justify dispensing with a warrant only if they established an exception to the warrant requirement. This follows from the basic rule... that warrantless searches and seizures are per se unreasonable unless an established exception applies.

Yet courts have made a flawed assumption. It may be that “when surveillance is lawful in the first place... the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful.” But this does not mean that subsequent querying of the incidental communications does not require a warrant. In Goitein’s words: the cases establishing the incidental overhear doctrine did not “hold or suggest that no warrant was necessary to collect the defendants’ conversations, as long as there was a warrant for the person with whom the defendants were

---


242 Goitein, *supra* 236, at 120.

243 United States v. Mohamud, 843 F.3d 420, 440–41 (9th Cir. 2016).
communicating.” 244 To the contrary, the warrants questioned in these cases had been broad to anticipate the capture of incidental incriminating information because the warrant had detailed the phone line and conversations it sought to pick up. 245 Moreover, exceptions to the warrant requirement are “jealously and carefully drawn” to an extent that it is hard to imagine the Supreme Court has created an incidental overhear exception without expressly saying so. 246 Additionally, with Section 702’s increased collection and querying authorities, it is hard to argue that the Title III incidental overhear doctrine is as easily applicable in the FISA context—where incidental collection is magnified tenfold. If anything, the incidental overhear doctrine stands for the proposition that a “small number of innocent conversations” [picked up] does not invalidate a warrant. This is a far cry from holding that the government can warrantlessly acquire the communications of anyone in contact with a lawfully surveilled target.” 247

And yet this is the position held by many district courts as well as the FISC for FISA applications. Consequently, the point of contention is that incidentally collected information on U.S. persons may not invalidate the foreign intelligence exception to the warrant requirement (if it is recognized), but that does not mean such incidental information can be searched by the government in any meaningful way without judicial review. Such an argument could challenge the FBI’s new ability to search incidentally collected Section 702 data to fish for information to establish probable cause.

All this analysis highlights a shaky foundation for Fourth Amendment authority to query incidental data collected about U.S. persons under the Reauthorization Act. The government’s reliance on the special needs exception and the incidental overhear doctrine are open to substantial challenge given Section 702’s expansion. And the reasonableness of the searches conducted—particularly regarding “about” collection—exist in an

244 Goitein, supra note 236, at 122.
245 Id.
247 Goitein, supra note 236, at 123.
era where courts are increasingly finding ways to rollback principles like the third-party doctrine to protect privacy interests in an intrusive digital age.

In short, these areas of constitutional contention are a few among many open issues that have been made viable by the expansion of Section 702. Notwithstanding narrow cases challenging the vagueness of statutory phrases in the Reauthorization Act (e.g., what does "predicated" mean?), these contention points are places where courts are most likely to restrain Section 702—something Congress could not manage to do. It is unlikely any court will find the program completely unconstitutional, but it will not be surprising if certain querying procedures or "about" collection (which now likely just require a "reference" to the target) are restricted given trends in the precedent discussed above. Nevertheless, Clapper v. Amnesty International serves as warning that justiciability will be a difficult issue to surmount because it is often difficult for plaintiffs subject to surveillance to prove injury in fact caused by a specific Section 702 search. In the future, the best chance for justiciable challenges may come from the ISPs who cooperate with the government and are increasingly required to provide more and more technical assistance to carry out downstream surveillance imposed by the NSA.

V. Conclusion

It is easy to find many missed opportunities for reform with the Reauthorization of Section 702. The concerns of privacy advocates were not meaningfully addressed, including clarification on unmasking. Some of the more complicated issues that will face FISA in the next decade were seemingly unanticipated. For example, the role of international data sharing, whether service providers will be compelled to provide increasingly complicated technical assistance to de-encrypt Section 702 data, and the growing ability to exploit smart technology connected the Internet for surveillance purposes.

248 See, e.g., 50 U.S.C. § 1881a (2018) (defining “[t]he term “abouts communication” means a communication that contains a reference to, but is not to or from, a target of an acquisition authorized under subsection.”).

249 Examples of smart technology connected to the internet, commonly known as the internet of things, include doors, appliances, and cars.
These are all open issues that Section 702 is unprepared to explicitly address. Nevertheless, ideas abound for reforming FISA and Section 702. Some propose an “inextricably intertwined test” to replace the significant purpose test such that FISA material would be admitted in court only if it is intertwined with national security related crimes. The idea would prevent the use of incidental FISA data on U.S. person’s to be used in prosecutions for ordinary crime. Others push for procedural protections, such as “expand[ed] opportunities for appellate review of FISC and FISCR cases.” Additionally, “increased public reporting, mandatory disclosure of FISC opinions, and more adversarial briefing at the FISC” have frequently been proposed. Relatedly, many propose that “querying procedures should provide for some independent periodic auditing of the queries and the recorded justifications for them” to ensure maximum accountability and to provide litigants with a record to challenge searches.

There is no shortage of ideas for improving FISA and Section 702. But there is often a shortage of political capital which is almost always contingent on the historical moment in which changes to FISA are considered. Broadly speaking, the history of electronic surveillance is one of ebb and flow. Evolving threats to national security demand evolving tools for staying ahead of those threats. But the government’s long history and record of abusing these tools often causes a cyclical curtailing of those instruments. Depending on the moment, the issue of balancing liberty and safety gets framed in the alternative ways discussed above.

The least nuanced—but perhaps truest—explanation for Section 702’s expansion in 2018 is that the question was framed as liberty reducing security rather than the alternative. In this narrative—with the threat of ISIS and a

250 See Kris, supra note 18, at 13-27
252 Id. at 1171.
253 Id. at 1166.
program that has not yet compared to the government abuses of surveillance emblematic of the mid-20th century—Congress was not willing to cripple the crown jewel of the IC. But because history tells us that it is certainly possible Congress does not know the full extent of Section 702 or has been confused about the extent of its success, courts must remain vigilant. The power of Section 702 belongs to the flexibility at which it can be used. Congress has likely relinquished its power to amend the program until it again faces renewal six years from now. But the courts have several avenues to hear constitutional litigation against the program. Perhaps the greatest obstacles are justiciability doctrines like standing, which prevent cases from easily being brought before Article III courts. Nevertheless, one hopes that as the government continues to expand its electronic surveillance programs, the probability of a case and controversy increases so courts can adequately weigh in. And lest courts give a blank check to the government, we can expect that the judicial drama surrounding the heightened strength of Section 702 is far from over.