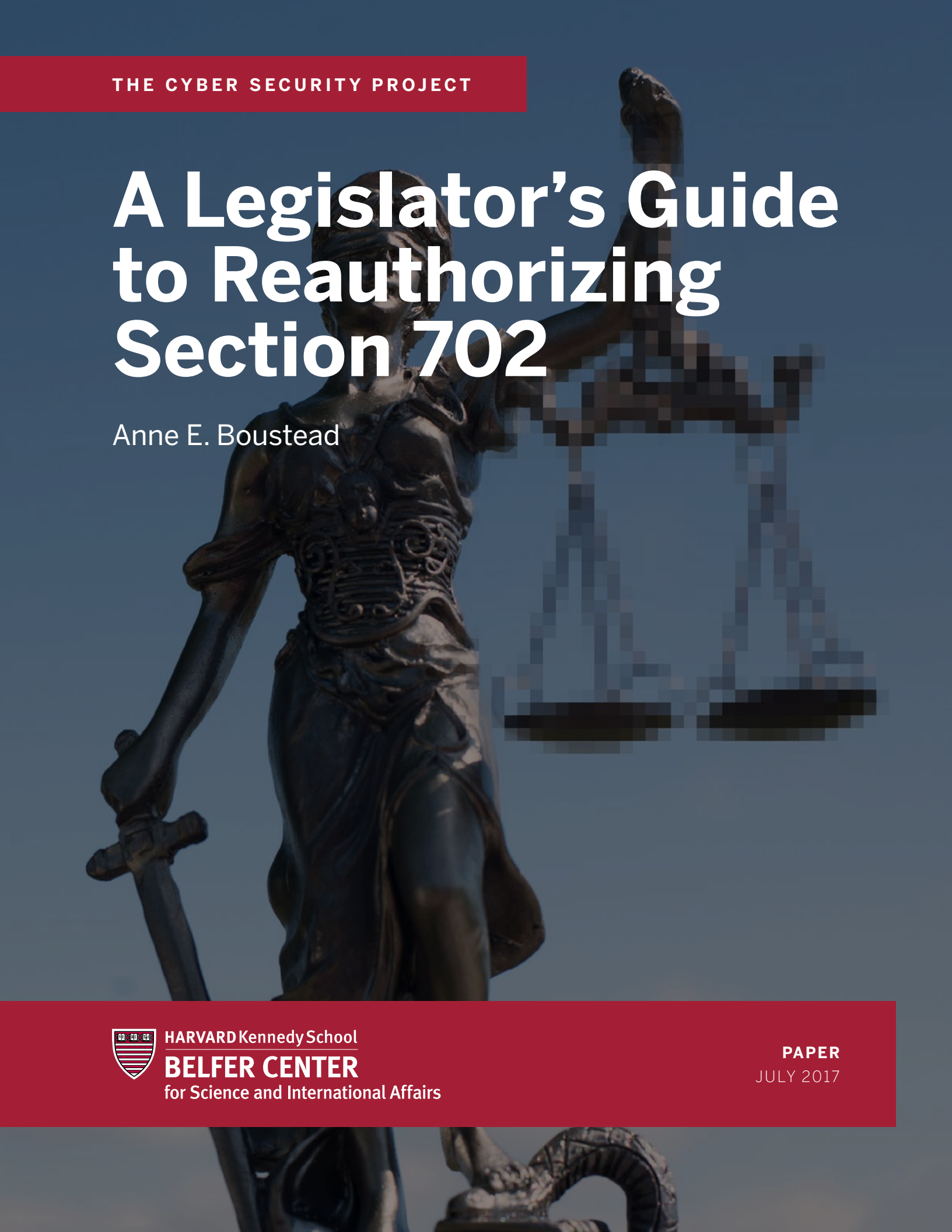

THE CYBER SECURITY PROJECT

A Legislator's Guide to Reauthorizing Section 702

Anne E. Boustead

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JULY 2017

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 JFK Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Cover, design, and layout by Andrew Facini

THE CYBER SECURITY PROJECT

A Legislator's Guide to Reauthorizing Section 702

Anne E. Boustead

HARVARD Kennedy School
BELFER CENTER
for Science and International Affairs

PAPER
JULY 2017

I. About the Author

Anne E. Boustead is a post-doctoral fellow at the Cyber Security Project at the Belfer Center for Science and International Affairs, Harvard Kennedy School, where she studies issues related to surveillance, security, and privacy. She has a Ph.D. in policy analysis from the Pardee RAND Graduate School and a J.D. from Fordham University School of Law.

Acknowledgements

The author would like to thank the Belfer Family and the Hewlett Foundation for supporting this research. She would also like to thank Jen Daskal, American University Washington College of Law, former Department of Defense Acting General Council Robert Taylor, and Raymond Brown for their helpful reviews of previous drafts.

I. Table of Contents

Executive Summary

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008, a powerful surveillance tool that allows U.S. government agencies to spy on foreign persons to collect counter-terrorism intelligence, will expire on December 31, 2017 without Congressional reauthorization. This paper has two goals: to concisely describe how agencies obtain information under Section 702, and to provide guidance to legislators and their staffs by examining the core issues they will confront as they consider reauthorizing this legislation.

Under Section 702, government agencies can obtain judicial approval to conduct surveillance programs without seeking specific authorization for each individual or device they target. Instead, agencies develop procedures governing the selection of targets for surveillance, and the protection of information related to U.S. persons who are mentioned or whose conversations are incidentally captured by the surveillance. Even though Section 702 was intended to authorize collection of foreign person communications, the communications of U.S. persons are inevitably collected as well, and consequently government agents can (and do) query databases that contain incidentally collected Section 702 data for information about U.S. persons. Both the "targeting" and the "minimization" procedures are essential to ensure that the Section 702 program does not become a means to circumvent legal protections for U.S. persons.

Although there is extensive testimonial evidence that Section 702 surveillance provides crucial national security information, there are also significant concerns that the regulatory regime governing this surveillance is inadequate to address important privacy interests. If these issues are not addressed in the debate regarding Section 702's reauthorization, Congress would miss an important opportunity to craft surveillance policies that ensure both national security and individual privacy. As shown in the chart below, each policy question identified by this paper can be addressed by Congress in a way that

will preserve both individual privacy and national security to the greatest extent possible.

Policy Issue	*Potential Action*	*Analysis*
Should additional protections be provided for U.S. person information?	Require the FBI to receive approval from the FISC before viewing Section 702 information through queries containing terms pertaining to U.S. persons	This amendment would increase privacy protections pertaining to government use of incidentally collected U.S. person information; the impact on use of that information can be mitigated by creating expedited approval mechanisms.
Should Congress explicitly define when criminal defendants are required to receive notice that Section 702 information will be used against them at trial?	Require government officials to give notice to defendant when evidence presented at trial would not have been discovered but for information obtained through Section 702	This amendment would ensure criminal defendants have the opportunity to defend their privacy rights, while having a minimal impact on collection of Section 702 information.
Should Congress require additional transparency mechanisms?	Mandate reporting of information, including statistics about collection of U.S. person data and the underlying reason for queries	This amendment would improve both governmental and public oversight of Section 702 surveillance without impacting the government's ability to collect information.
Should Congress continue to include a sunset provision in Section 702?	Remove the sunset provision, or lengthen the time before the sunset provision takes effect	This amendment would provide greater predictability for intelligence agencies, while maintaining oversight of Section 702 and ensuring that it is updated to reflect technological changes.

I. Introduction

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008[1] is an important – albeit controversial – source of legal authority for government surveillance. Under Section 702, the U.S. government can acquire foreign intelligence information from the electronic communications and transactions of non-U.S. persons that pass through commercial providers and infrastructure in the United States. While this surveillance must comply with a complex set of regulations involving both internal and external oversight, the government is neither required to provide evidence that intercepting an individual's communications will provide foreign intelligence information or evidence of a crime, nor obtain permission from a judge before accessing that individual's communications.

Section 702 plays a critical and unique role in protecting national security and preventing terrorism. According to a report by the Privacy and Civil Liberties Oversight Board [PCLOB], an independent executive branch agency tasked with ensuring that national security efforts do not unduly compromise civil liberties, "over a quarter of the NSA's reports concerning international terrorism include information based in whole or in part on Section 702 collection, and this percentage has increased every year since the statute was enacted."[2] At the same time, however, policy analysts and privacy advocates have expressed concern about the scope of Section 702 surveillance, particularly as it relates to the collection and use of information about U.S. persons incidentally obtained when non-U.S. persons are targeted for surveillance. Accordingly, Section 702 has been described as creating privacy concerns that are an "unnecessary symptom of a statute that has metastasized well beyond its purported goal."[3]

Congress must soon address the policy tradeoffs in Section 702. Section 702 will sunset on December 31, 2017 unless Congress acts to renew it.

---

1 Although more commonly referred to as Section 702, this provision is codified at 50 U.S.C. § 1881a.

2 Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* 10 (2014), https://www.pclob.gov/library/702-Report.pdf [hereinafter "PCLOB Report"].

3 Jadzia Butler and Jennifer S. Granick, *Correcting the Record on Section 702: A Prerequisite for Meaningful Surveillance Reform* 19, Just Security, Sept. 22, 2016, https://www.justsecurity.org/wp-content/uploads/2016/09/Butler-Granick-Correcting-the-Record-Scope-of-702.pdf.

Congress may elect to reapprove this statute as it currently exists, reapprove it with additional amendments, or allow it to expire. A broad range of potential amendments to Section 702 have been suggested, including enacting additional transparency mechanisms, establishing additional protections for information about U.S. persons, and regulating how information can be used during criminal investigations in the U.S. Each of these suggested amendments may impact the use of Section 702 information by the government, the commercial entities who are required to support Section 702 surveillance programs, and the privacy interests of persons living both in the U.S. and abroad.

The goal of this paper is to provide guidance to legislators and staffers as they decide whether to reauthorize Section 702 – with or without amendments – as well as the advocates and analysts who aim to shape the reauthorization debate. I begin with an overview of the history of surveillance regulation in the United States, a description of how changes in communications infrastructure have changed this surveillance regulation, and a discussion of how post-9/11 efforts to prevent terrorist attacks led the U.S. government to use this emerging infrastructure to conduct surveillance of foreign communication. Section 702 is then described in detail. Next, the policy issues shaping the debate over Section 702 are discussed and analyzed in depth. This analysis includes recommendations for policymakers about changes to Section 702 that could be made as part of the reauthorization process. Finally, the paper concludes with a brief commentary on ensuring both individual privacy and national security are protected by Section 702.

II. Historical and Technical Background

A series of scandals in the 1970s raised public concern about the scope of government surveillance in the United States. The Watergate investigations revealed "a conspiracy of wiretapping, spying, campaign sabotage, secret funds, interference with investigations, and cover-up reaching to the top of the administration";[4] Seymour Hersch published an article on the front page of the New York Times contending that a C.I.A. internal review "produced evidence of dozens of … illegal activities by members of the C.I.A. inside the United States, beginning in the nineteen-fifties, including break-ins, wiretapping and the surreptitious inspection of mail."[5] In response to these scandals, the Senate established a select committee "to conduct an investigation and study of governmental operations with respect to intelligence activities."[6] This committee, which became known as the Church Committee, conducted extensive investigations and hearings over 16 months.[7] Their final report revealed both that U.S. government actors conducted extensive domestic and international surveillance and, more significantly, that this surveillance was being conducted without consideration of the laws regulating government surveillance.[8] The Committee concluded that "congressional oversight is necessary to assure that in the future our intelligence community functions effectively, within the framework of the Constitution."[9]

---

4 Robert R. Faulkner and Eric R. Cheney, *Crisis in the Conspiracy* 1 (2011), *available at* https://www.researchgate.net/profile/Robert_Faulkner6/publication/268421604_Crisis_in_the_Conspiracy_Watergate_and_the_Limits_of_Brokerage/links/54b931990cf2d11571a31cb9.pdf.

5 *Seymour M. Hersh, Huge C.I.A. Operation Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years, N.Y. Times,* Dec. 22, 1974, at 1, *available at* http://www.washingtondecoded.com/files/nyttext.pdf.

6 *S. Res. 21, 94th Cong. (1975), available at* http://www.senate.gov/artandhistory/history/common/investigations/pdf/ChurchCommittee_SRes21.pdf.

7 United States Senate, *Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, *available at* http://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm. The Church Committee's activities included "126 full committee meetings, 40 subcommittee hearings, interviewing some 800 witnesses in public and closed sessions, and combing through 110,000 documents[.]" *Id.*

8 "Too many people have been spied upon by too many Government agencies and to[o] much information has been collected….Government officials – including those whose principal duty is to enforce the law – have violated or ignored the law over long periods of time and have advocated and defended their right to break the law." Church Committee, *Book II: Intelligence Activities and the Rights of Americans* 5, *available at* http://aarclibrary.org/publib/church/reports/book2/html/ChurchB2_0011a.htm.

9 Church Committee, *Book I: Foreign and Military Intelligence* 2, *available at* http://www.aarclibrary.org/publib/church/reports/book1/contents.htm.

Based on the recommendations made by the Church Committee, Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978. FISA "attempts to apply domestic law enforcement principles to activities conducted for national security purposes"[10], resulting in a set of rules that allowed secret foreign intelligence surveillance with judicial authorization.[11] Although inspired by regulations governing law enforcement surveillance, the regulations established by FISA to govern foreign surveillance differ in several key respects. Under FISA, the Foreign Intelligence Surveillance Court (FISC) was created to oversee surveillance by allowing the government to present evidence and receive permission for surveillance in secret. Applications for surveillance can only be approved if "the target is a foreign power (i.e., foreign government, faction, terrorist or political group, or organization controlled by a foreign government) or an agent of a foreign power (i.e., a non-resident agent who is an officer, employee, or agent of a foreign power, and United States persons whose activities on behalf of a foreign power may involve criminal acts relating to intelligence or terrorist operations)."[12] Surveillance must be targeted at instrumentalities used by these foreign agents and powers, and must minimize collection of information from U.S. persons.[13] As originally written, FISA was not meant to create additional restrictions on entirely foreign communications, and indeed did not require approval of the FISC court "when surveillance is directed solely at communications among or between foreign powers."[14]

This regulatory regime was based on the assumption that the location of communications in transit is largely determined by the location of the persons communicating: in other words, that communications are generally transmitted directly between the sender and recipient.[15] Changes in technology after the 1970s undermined these assumptions. At the time

10 Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. Penn. L. Rev. 793, 794 (1989).

11 Peter P. Swire, *The System of Foreign Intelligence Surveillance*, 72 Geo. Wash. L. Rev. 1306, 1325 (2004).

12 Cinquegrana, *supra* note 10, at 812.

13 *Id*.

14 *Id*. at 813.

15 Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub. Pol'y 117, 147 (2015) ("Congress explicitly exempted foreign-to-foreign wire communications from FISA's remit. The exclusion made sense: the voice transmission of a British subject in London, calling a French citizen in Paris, at no point crossed U.S. borders.").

FISA was written, communications were primarily wire-based: phone calls traveled along phone wires, and telegraph communications traveled along telegraph lines. Because these communications travel along physical wires, the cheapest route was often the most direct route. However, digital communications may not travel in a straight line between the sender and recipient. Because the cost of transmitting data is so low, the most efficient route depends on the immediate availability of infrastructure to transmit the communication, and corresponding messages may travel far out of their way before they reach their destination. Additionally, because much of the technology that powers the internet was invented and commercialized within the U.S., much of the world's communications infrastructure is located in the United States. Consequently, it is possible that an internet communication traveling between two foreign persons would pass through infrastructure within the United States – thus implicating stricter legal protections – even though FISA, as originally written, was not intended to cover foreign-to-foreign communications.[16]

Even as technological changes created an unanticipated expansion of FISC processes, the terrorist attacks on September 11th increased America's interest in counterterrorism activities and surveillance. In response, the government created several new surveillance authorities, including the FISA Amendments Act of 2008.[17] However, policymaking surrounding these surveillance authorities has proven to be an ongoing challenge. The Snowden leaks provided extensive information about how these surveillance authorities worked in practice, which did not correspond to public perceptions of the scope of acceptable government surveillance.[18] The fallout from the Snowden leaks was significant, and included the invalidation of the E.U.-U.S. safe harbor provisions by the Court of Justice of the European Union in *Schrems v. Data Protection Commissioner*.[19] At the same

16 *Id.*

17 Edward C. Liu, *Surveillance of Foreigners Outside the United States Under Section 702 of the Foreign Intelligence Surveillance Act (FISA)*, Congressional Research Service (2016), https://fas.org/sgp/crs/intel/R44457.pdf.

18 Chandra Steele, *The 10 Most Disturbing Snowden Revelations*, PC Magazine, Feb. 11, 2014, http://www.pcmag.com/article2/0,2817,2453128,00.asp.

19 *See* Sarah St. Vincent, *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance Reform*, Center for Democracy and Technology, Oct. 26, 2015, https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/.

time, Section 702 has become an increasingly important source of foreign intelligence and counter terrorism information.

Some portions of these surveillance authorities – including Section 702 – contain sunset provisions which require periodic reauthorization of their provisions. Unless reauthorized, Section 702 will sunset in December 2017.

The upcoming debate around the reauthorization of Section 702 will be shaped by several key policy concerns. Defenders of Section 702 have described it as "a critical and invaluable tool for American intelligence professionals and officials"[20], while civil liberties advocates have argued that Section 702 is "in desperate need of reform"[21] to ensure that there is effective oversight of these surveillance programs and to limit the collection of information about U.S. persons. Both perspectives are correct: Section 702 programs provide important and unique information vital for protecting national security, and also raise significant privacy and civil liberties concerns. Additionally, there is a legitimate concern about the burden placed on the commercial entities that are required to assist with Section 702 surveillance.[22]

20 David Shedd, Paul Rosenzweig, and Charles Stimson, *Maintaining America's Ability to Collect Foreign Intelligence Program*, Heritage Foundation (2016), http://www.heritage.org/research/reports/2016/05/maintaining-americas-ability-to-collect-foreign-intelligence-the-section-702-program.

21 Butler and Granick, *supra* note 4.

22 Danielle Kehl, Kevin Bankston, Robyn Greene, and Robert Morgus, *Surveillance Costs: The NSA's Impact on the Economy, Internet Freedom & Cybersecurity*, New America's Open Technology Institute Policy Paper (2014), https://na-production.s3.amazonaws.com/documents/surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity.pdf.

III. Overview of Section 702

Section 702 allows the federal government to require commercial telecommunications and computing service providers[23] to provide information about non-U.S. persons. The federal government is not required to obtain specific judicial permission for every individual targeted by Section 702 surveillance programs.[24] Instead, the Attorney General (AG) and Director of National Intelligence (DNI) create guidelines governing the use of Section 702 surveillance, which must then be reviewed and approved by the FISC. After this approval is obtained, the federal government follows the established guidelines to select individuals whose communications are subject to surveillance. The information collected can then be queried by federal intelligence and law enforcement agencies – including the NSA, CIA, and FBI – for foreign intelligence, counterterrorism, or criminal investigatory purposes. These activities are subject by review by the AG, DNI, and the agency conducting the surveillance. While U.S. persons cannot be targeted directly or indirectly by Section 702 surveillance, their information may be collected "incidentally" when non-U.S. persons are properly targeted. The guidelines, including targeting and minimization procedures, are intended to ensure appropriate protection of U.S. person information. This process is subject to complex internal and external oversight mechanisms involving all three branches of government.[25]

In this section, I briefly discuss how Section 702 surveillance is conducted and regulated in the context of collecting information about non-U.S. persons. I then describe how U.S. person information may be incidentally collected during Section 702 surveillance, and analyze the regulations pertaining to its protection and use by the government.

---

23 50 U.S.C. §1881a allows collection of information from electronic communication service providers, which is defined broadly to include telecommunications carriers, electronic communication service providers, remote computing services, and "any other communication service provider who has access to wire or electronic communications." 50 U.S.C. § 1881(b)(4).

24 PCLOB Report at 6 ("Under Section 702, the Attorney General and Director of National Intelligence make annual certifications authorizing this targeting to acquire foreign intelligence information, without specifying to the FISA court the particular non-U.S. persons who will be targeted."). As I discuss in Section IV *infra*, this is in contrast to the authorities governing intentional acquisition of information about U.S. persons.

25 Chris Inglis and Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings*, Hoover Institution Essay, Series Paper No. 1604 (2016), https://lawfare.s3-us-west-2.amazonaws.com/staging/2016/310549748-In-Defense-of-FAA-Section-702-An-Examination-of-Its-Justification-Operational-Employment-and-Legal-Underpinnings-by-Chris-Inglis-and-Jeff-Kosseff.pdf.

A. Use of Section 702 to Obtain Foreign Intelligence Information

First, executive branch agencies develop policies to ensure that Section 702 surveillance comports with Constitutional and statutory requirements. Surveillance conducted under 702 is subject to three sets of restrictions; the Attorney General (AG) and Director of National Intelligence (DNI) are responsible for developing policies to ensure compliance with these restrictions. It must comply with a set of limitations set forth by the text of the statute, and with targeting requirements and minimization requirements crafted by executive branch agencies. These sets of restrictions are summarized in **Table 1** below.

Table 1: Procedures Governing Use of Section 702 Surveillance

	Statutory Limitations	Targeting Procedures	Minimization Procedures
Purpose	Establish requirements that Section 702 surveillance not be used to target U.S. citizens or persons present in U.S.	Provide guidance on choosing persons to target for surveillance, and how information about these persons may be gathered	Provide guidance on how information can be used and handled after it is collected
Creator	AG (in consultation with DNI)	AG (in consultation with DNI)	AG (in consultation with DNI)
External Approval	Must be submitted to the FISC, congressional intelligence and judiciary committees	Subject to review by FISC	Subject to review by FISC
Summary	• Cannot directly or indirectly target U.S. citizens, even if living abroad • Cannot collect communications if all parties within U.S. • Must comport with Fourth Amendment	• Can only target non-U.S. persons outside of U.S. • Make this determination based on totality of circumstances • Ongoing review required to ensure assessment is correct	• Section 702 information can be queried for foreign intelligence information or evidence of a crime • Information must be processed to protect privacy of U.S. persons unrelated to foreign intelligence
How Used	Must develop procedures to ensure these limitations not violated throughout surveillance process	Used to prior to surveillance to determine what information to obtain	Used after surveillance to determine what information to analyze

After the AG and DNI develop targeting and minimization procedures, they must submit these procedures to the FISC for approval, along with a certification that they have developed guidelines that will ensure compliance with the statutory limitations described above.[26] The FISC judge, who is supported by a staff of Court Attorneys, must review these Section 702 applications within 30 days.[27] The FISC judge reviews this application to determine whether "the certification contains all of the required elements, and … the targeting and minimization procedures adopted in accordance with 50 U.S.C. §§ 1881a(d) & (e) are consistent with the requirements of those subsections and with the Fourth Amendment."[28] The judge then issues an order either approving the application, or denying it and identifying any deficiencies. If the application is denied, then the government can choose to either correct the identified deficiencies within 30 days, or forgo the surveillance that would be authorized by the application.[29] The government may also appeal the decision within 30 days to the Foreign Intelligence Surveillance Court of Review (FISCR).[30] Decisions of the FISCR are appealable to the U.S. Supreme Court.[31]

After the government obtains approval from the FISC, it can begin to conduct surveillance. Under existing targeting guidelines, Section 702 surveillance authorities may not be used to obtain information indiscriminately. Rather, the NSA begins with information about a particular individual or communication identifier (such as a phone number or email address) that leads them to believe the individual is a non-U.S. person and that their communications might provide foreign intelligence information.[32] Information can be collected under Section 702 if

26 In addition to obtaining approval from the FISC, the government is also required to submit the guidelines for ensuring compliance with the statutory limitation to the congressional intelligence committees, and the House and Senate Judiciary committees. 50 U.S.C. § 1881a(f).

27 Letter from Reggie B. Walton to Patrick J. Leahy, Chairman, Committee on the Judiciary (July 29, 2013), *available at* http://www.fisc.uscourts.gov/sites/default/files/Leahy.pdf.

28 *Id.*

29 50 U.S.C. § 1881a(i)(3).

30 50 U.S.C. § 1881a(i)(4). Analogously to the FISC, the FISCR is comprised of three judges selected by the Chief Justice of the Supreme Court from federal district or appellate courts. These judges serve seven year staggered terms, and continue in their position as a federal district or appellate judge when they are not hearing appeals at the FISCR. 50 U.S.C. § 1803.

31 50 U.S.C. § 1803(b).

32 National Security Agency, *Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed To Be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended*, 2 (2016) [hereinafter NSA Targeting Procedures], *available at* https://www.dni.gov/files/documents/icotr/51117/2016_NSA_702_Targeting_Procedures_Mar_30_17.pdf.

it can be connected to a communication identifier used by a particular non-U.S. person who is selected for surveillance. Therefore, the individual whose information is being obtained is referred to as the "target"; the communication identifiers are referred to as "selectors" since they are used to select the particular communications to be gathered by the government.[33] Section 702 does not allow the government to choose communications for collection based on the presence of particular words or phrases. Selectors must refer to specific communication identifiers, and "may not be key words (such as 'bomb' or attack'), or the names of targeted individuals ('Osama Bin Laden')."[34]

After the NSA has specified particular selectors for tasking, the AG and DNI write a directive requiring electronic communication providers to provide the government with information associated with that selector or assist the government with directly obtaining information about that selector, and keep records associated with that data collection secure.[35] This directive is presented to any relevant electronic communications providers,[36] and data collection is formally handled by the Data Intercept Technology Unit (DITU)[37] at the FBI.[38] Information is obtained from the electronic communications provider using one of two methods: PRISM collection or upstream collection.[39] As summarized in the table below, these two methods differ in several key aspects. One particularly salient difference is the type of information that can be collected: upstream collection can be used to obtain all transactions that mention the tasked selectors – not just those transaction that are sent to or from the selectors.[40] Referred to as "about" collection, this data collection poses significant

33 PCLOB Report at 32 ("Thus, in the terminology of Section 702, people (non-U.S. persons reasonably believed to be located outside the United States) are *targeted*; selectors (e.g., email addresses, telephone numbers) are *tasked*.").

34 *Id.* at 33.

35 50 U.S.C. § 1881a(h)(1).

36 PCLOB Report at 33.

37 THE DITU has been described as "the FBI's equivalent of the National Security Agency and the primary liaison between the spy agency and many of America's most important technology companies, including Google, Facebook, YouTube, and Apple." Shane Harris, *This obscure FBI unit does the domestic surveillance that no other intelligence agency can touch*, Foreign Policy, Nov. 12, 2013, http://foreignpolicy.com/2013/11/21/meet-the-spies-doing-the-nsas-dirty-work/.

38 *NSA slides explain the PRISM data-collection program* (June 29, 2013), *available at* http://cyber-peace.org/wp-content/uploads/2013/06/NSA-slides-explain-the-PRISM-data-collection-program-The-Washington-Post.pdf.

39 PCLOB Report at 33.

40 *Id.*

challenges to the protection of U.S. person information, as it can allow the collection of communications between two U.S. persons who are discussing the tasked selector.[41] Given these challenges, the NSA recently discontinued upstream about collection.[42] However, about collection remains technically feasible, and a potential source of valuable information.

Table 2: Comparison of PRISM and Upstream Data Collection

	PRISM	Upstream Collection
Who is the information obtained from?	Electronic and computing service providers (e.g., Microsoft, Apple, Google)	Companies responsible for telecommunications infrastructure
What government agency conducts the surveillance?	FBI DITU, on behalf of the NSA	NSA
Who may use the information?	NSA; may also be received by the CIA, FBI, and NCTC	NSA only
Is "about" data collection possible?	No	Possible; however, NSA recently discontinued its practice of "about" data collections because of concerns about collection of U.S. person communications
What types of data can be collected?	Email, VoIP calls, file transfers, video, photo, social networking	Data packets
Proportion of Section 702 information obtained using method	Approximately 90%	Approximately 10%

As the NSA acquires information from either PRISM or upstream data collection programs, they perform periodic checks to "detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States."[43] If these checks reveal that the target has entered the United States, then acquisition is terminated and the incident is reported to authorities within the AG and

41 *Id.* at 36-38. While entirely domestic communications probably make up a very small percentage of the overall number of communications obtained through upstream collection, it could amount to many thousands of communications given the large volume of collection. *Id.*

42 Press Release, National Security Agency, *NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702* (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml.

43 NSA Targeting Procedures at 6.

ODNI's office. After it is collected, intelligence agencies can query Section 702 data to obtain evidence relevant to foreign intelligence or criminal investigations. Section 702 data must generally be destroyed after five years, although it may be retained longer if "the NSA specifically determines" that it is foreign intelligence information or necessary for understanding foreign intelligence information.[44] The agents involved in collecting and analyzing this data receive extensive training that "not only explains the law, but also provides practical guidance as to how analysts can meet those legal requirements."[45] The entire process of collecting and using data pursuant to Section 702 authority is subject to regular and thorough oversight from within the executive branch.[46]

Several challenges remain for the continued use of Section 702 surveillance. As communications technology and practices change, surveillance programs conducted under Section 702 must be adapted accordingly. For example, Section 702 surveillance programs may need to respond to the spread of consumer products that encrypt communications by default. One possible way to ensure that Section 702 remains a vital surveillance tool that respects civil liberties is to require subsequent, periodic reauthorization. The debate that surrounds reauthorization helps to ensure the continued relevance of both the surveillance that can be conducted under Section 702 and the associated protections for civil liberties. However, this debate also imposes a cost on the Intelligence Community, which must both advocate for the continuation of the program and deal with the uncertainty that the program will not be reauthorized. Additionally, although the NSA in particular has taken unprecedented steps to improve public understanding of its role and activities, there still remain significant concerns that the public has not been provided with sufficient information about how Section 702 works. For example, Senator Wyden has repeatedly argued that "it is critical that the government provide Congress and the public the information needed to assess the impact of the program and

44 *Id.* at 7. For further discussion of destruction of data collected under Section 702, *see* Inglis and Kosseff, *supra* note 24, at 14-15.

45 Inglis and Kosseff, *supra* note 24, at 16.

46 "At least once every 60 days, NSN and ODNI conduct oversight of the agencies' activities under Section 702....The team evaluates and, where appropriate, investigates each potential incident of noncompliance and conducts a detailed review of agency targeting and minimization procedures." *The FISA Amendments Act: Q&A* 6 (2017), https://www.dni.gov/files/icotr/FISA%20Amendments%20Act%20QA%20for%20Publication.pdf.

determine whether it should be reauthorized and whether it should be reformed."[47]

Therefore, in amending Section 702, Congress may consider:

- Whether to require additional transparency mechanisms
- Whether to require subsequent reauthorization of Section 702

B. Incidental Collection of U.S. Person Information Under Section 702

Although Section 702 is primarily intended to collect information about non-U.S. persons, these surveillance programs still gather significant amounts of U.S. person information. Such collection could occur because a U.S. person is communicating with a non-U.S. person who has been properly targeted for surveillance, or because two non-U.S. persons are communicating about an identifiable U.S. person. Collection of U.S. person information by Section 702 surveillance programs is referred to as "incidental collection." However, the fact that it is referred to as "incidental" collection does not mean that it is done infrequently, merely that it is not done purposefully. In fact, the sheer "volume of communications monitored is … at odds with claims that downplay the impact of the action in question."[48]

The targeting and minimization procedures that agencies are required to adopt under Section 702 are intended to protect the privacy of U.S. person communications incidentally collected. The targeting procedures implement the requirement that Section 702 surveillance be used to obtain foreign intelligence information from non-U.S. persons located outside the United States by providing guidance to the analysts responsible for determining whether a particular person can be the subject of Section 702

47 Letter from Senator Ron Wyden to Senator Coats (Mar. 8, 2017), *available at* https://www.wyden.senate.gov/download/?id=167EDE43-DEFB-4723-843D-44BCBD263BEF&download=1.

48 Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J.L. & Pub Pol'y 117, 179 (2015).

surveillance.[49] According to publicly released versions of the targeting procedures adopted by the NSA, this judgment is made "in light of the totality of the circumstances based on the information available on that person."[50] The targeting procedures require NSA analysts to make a "particularized and fact-based [assessment], informed by analytic judgment, the specialized training and experience of the analyst, as well as the nature of the foreign intelligence information expected to be obtained."[51] This analysis may vary based on how the potential target is communicating, as telephonic and internet devices reveal different information about the user and his location. The targeting procedures also require that the decision to target a particular individual for Section 702 surveillance be subject to ongoing review in order to "detect those occasions when a person who when targeted was reasonably believed to be located outside the United States has since entered the United States" and prevent the collection of communications between U.S. persons.[52]

Minimization procedures must be "reasonably designed…to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[53] Under these procedures, a U.S. person's identity cannot be disseminated unless it is needed to interpret the foreign intelligence information or is evidence of a crime being used for law enforcement purposes.[54] To implement this requirement, intelligence agencies have adopted minimization procedures governing how this information must be processed in order to protect the privacy of U.S. persons, who may access the information, how sensitive or privileged information should be handled, and how long the information may be retained. Agencies vary in terms of their access to U.S. person information,

49 50 U.S.C. § 1881a(d). The certification to be provided to the court must attest that "a significant purpose" of the acquisition is to obtain foreign intelligence information; it does not require that collecting foreign intelligence information must be the sole or predominant purpose. 50 U.S.C. § 1881a(g)(2)(A)(v). This feature of the statute has been identified by critics as especially problematic.

50 NSA Targeting Procedures at 1.

51 *Id.* at 4.

52 *Id.* at 6.

53 50 U.S.C. § 1801(h).

54 *Id.*

their use of U.S. person information, and the agency minimization procedures regulating these processes.

The NSA, FBI, and CIA have all established procedures to generally require identifying information about U.S. persons be de-identified prior to dissemination, usually by replacing the identifying characteristic with a symbol or generic phrase (i.e., "U.S. Person 1"). However, these agencies differ somewhat in terms of when they allow U.S. person identity information to be retained during subsequent analysis and dissemination of Section 702 surveillance. For example, the NSA allows U.S. person identifying information to be retained if there are indications that the person in question might be an agent of a foreign power, a target of intelligence activities, disclosing classified information, engaged in terrorist activity, or the communication itself is evidence of a crime.[55] The FBI only allows U.S. person identifying information to be retained in subsequent use of Section 702 surveillance if it appears "to be foreign intelligence information, to be necessary to understand or assess the importance of foreign intelligence information, or to be evidence of a crime."[56] The NSA's procedures explicitly contemplate a variety of circumstances under which a U.S. person's identifying information may shed insight into the activities of foreign nations, while the FBI's procedures merely rely on a generic allowance that U.S. person's identifying information can be used when it is necessary to understand foreign intelligence information.

Although data obtained through Section 702 surveillance is required to be stripped of identifying information regarding U.S. persons prior to dissemination unless certain agency-specific requirements are met, these agencies may search unminimized Section 702 data using U.S. person identifiers. The requirements for conducting such searches differ across agencies. Both the NSA and the CIA may search using terms likely to return foreign intelligence information, while the FBI may use search terms likely

55 *Minimization Procedures Used by the National Security Agency in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* [hereinafter NSA Minimization Procedures] at 12-3, *available at* https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf.

56 *Minimization Procedures Used by the Federal Bureau of Investigation in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, As Amended* [hereinafter FBI Minimization Procedures] at 9, *available at* https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf.

to return either foreign intelligence information or evidence of a crime. Furthermore, before analysts at the NSA or CIA can conduct queries using U.S. person identifiers, they must produce a written statement of facts and receive intra-agency approval.

The FBI's process for querying Section 702 data is different, and as a result FBI agents and analysts are not required to produce specific documentation prior to querying Section 702 data using U.S. person identifiers. Due to the FBI's need to make connections between disparate pieces of information, the FBI combines all of their information from various sources into "confederated databases" located in a "single cloud-type environment."[57] Consequently, agents querying FBI databases will be notified if there is relevant data from Section 702 surveillance. Agents who have received specialized training in handling Section 702 data will receive the information directly; agents without this training will "be alerted that there is information, then have to go to the appropriate training and the appropriate oversight to be able to see it."[58]

Although the information on the number of queries involving U.S. person identifying information has been published as part of the ODNI yearly transparency report, these data do not include information on queries conducted by the FBI.[59] The data that have been published suggest that queries of Section 702 data for information about U.S. persons are not unusual: over 4,500 search terms concerning U.S. persons were used to search content information obtained under Section 702, and almost 24,000 queries concerning U.S. persons were used to search non-content information obtained under Section 702.

Both the scope of U.S. person information incidentally collected and the use of U.S. person identifiers to query collected data have created concerns that use of Section 702 surveillance may be spreading beyond Congress' initial intent. These concerns are amplified when this data is used during

57 *Read the full testimony of FBI Director James Comey in which he discusses Clinton email investigation*, Washington Post, May 3, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/?utm_term=.11e2243fcb12.

58 *Id.*

59 *See* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, *available at* https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

criminal investigations in the United States, particularly as uncertainties have arisen about when criminal defendants will receive notice that Section 702 information will be used during their trial.[60] As described by Elizabeth Goitein, Co-Director of the Liberty & National Security Program at the Brennan Center for Justice, NYU School of Law, concerns about Section 702 surveillance are focused less on fears of outright abuse and more on concerns about "mission creep, so that a law designed to protect against foreign threats to the United States has become a major tool for ordinary domestic law enforcement…contrary not only to the original intent of FISA, but to Americans' expectations and their trust that Congress will protect their Privacy and their freedoms."[61] On the other hand, the text of "FISA does not merely contemplate, but expressly requires, that the government's procedures provide for the retention and dissemination of Section 702-acquired information that is evidence of a crime for law enforcement purposes…whether or not the crime in question relates to foreign intelligence or national security."[62]

Therefore, in amending Section 702, Congress may consider:

- Whether to provide additional protections for use of U.S. person information collected by Section 702 surveillance programs
- Whether and how to ensure criminal defendants receive notice that Section 702 information will be used against them at trial

60 Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?*, Just Security, Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

61 *Section 702 of the Foreign Intelligence Surveillance Act: Hearing Before the Committee on the Judiciary, House of Representatives*, Serial No. 115-2 at 35, *available at* https://judiciary.house.gov/wp-content/uploads/2017/03/115-2_24726.pdf [hereinafter House Committee Report]

62 2015 FISC Memorandum Opinion at 32, https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

IV. Issues that Should Be Addressed During Reauthorization

Because of its unique and important role in protecting national security, it is highly likely that Congress will reauthorize Section 702. Reauthorization would maintain government access to a valuable antiterrorism tool, which has been described by leaders of the Intelligence Community as "provid[ing] critical foreign intelligence that cannot practicably be obtained through other methods."[63] Although the government could continue conducting surveillance under other legal authorities should reauthorization fail, the absence of the clear statutory authority provided by Section 702 may simultaneously inhibit crucial government surveillance and erode the privacy of U.S. persons.[64]

However, assuming Congressional reauthorization, Congress may act to amend Section 702. These amendments could take on many forms; policymakers, advocates, and government officials have already begun to discuss potential changes. Although the range of possible amendments to Section 702 surveillance authorities is broad, much of the debate so far has centered on the collection and use of information about U.S. persons incidentally collected under Section 702, and the lack of public transparency surrounding Section 702 surveillance. Additionally, there has been some discussion of whether Section 702 should be reauthorized without a sunset provision, such that periodic reauthorization is no longer required.

In this section, I discuss the issues that Congress should consider during the reauthorization proceedings, and their options for addressing these issues. These issues include additional protections for both U.S. persons in general and those persons who are the subject of criminal prosecutions, as

63 Joint Unclassified Statement of Robert S. Litt, Stuart J. Evans, Michael B. Steinback, and Jon Darby Before the Committee on the Judiciary, United States House of Representatives, https://judiciary.house.gov/wp-content/uploads/2016/02/joint-sfr-for-doj-fbi-odni-and-nsa-updated.pdf.

64 For example, Executive Order 12333 establishes "certain general principles that, in addition to and consistent with applicable laws, are intended to achieve the proper balance between the acquisition of essential information and the protection of individual interests," but has been described as "provid[ing] the intelligence community with vague powers and very little guidance as to how to exercise them." Executive Order 12,333, https://www.archives.gov/federal-register/codification/executive-order/12333.html; Charlotte J. Wen, *Secrecy, Standing, and Executive Order 12,333*, 89 S. Cal. L. Rev. 1099, 1109 (2016).

well as concerns about transparency and the continued need for periodic reauthorization of Section 702. While this list is necessarily incomplete, it includes the options most likely to be discussed in the upcoming debate. I begin by describing each potential issue with Section 702 and discussing how Congress may elect to address it by amending Section 702. I then analyze whether and how such an amendment might affect the policy concerns that have so far shaped the debate over Section 702 surveillance: the government's access to effective and timely information, potential harm to U.S. telecommunications companies, the collection and use of information about U.S. persons, and effectiveness of oversight provisions.[65] This analysis is summarized in Table 3 on the following page.

65 *See* discussion *supra* Sec.I.

Table 3: Analysis of Potential Amendments to Section 702

Question	Potential Action or Amendment	*Analysis of Impact on Key Policy Concerns*			
		Government Information Access	**Impact on Communications Companies**	**Collection/Use of U.S. Person Information**	**Effectiveness of Oversight**
Should additional protections be provided for U.S. person information?	Require the FBI to receive approval from the FISC before viewing Section 702 information through queries containing terms pertaining to U.S. persons	Agencies may not be able to access information previously collected if they cannot justify their use of U.S. person identifiers to the FISC, and access may be delayed while they wait for approval	No effect – would change neither the role commercial entities play in Section 702 surveillance, nor public awareness of this role.	Use of U.S. person information may decrease, as the barriers to use of this information would increase	FISC would be authorized to conduct additional reviews of agency use of information, thus increasing oversight
Should Congress explicitly define when criminal defendants are required to receive notice that Section 702 information will be used against them at trial?	Require government officials to give notice to defendant when evidence presented at trial would not have been discovered but for information obtained through Section 702	No effect – regulation of government collection and use of information under Section 702 will remain unchanged	May have a negative impact on companies if it is revealed that use of Section 702 surveillance in criminal trials is more pervasive than previously thought.	Use of U.S. person information may decrease, as the government may restrict use of this information in criminal trials to avoid demonstrating the scope of Section 702 surveillance	Would increase both judicial and public oversight by providing additional information about how Section 702 surveillance is used
Should Congress require additional transparency mechanisms?	Mandate reporting of information, including statistics about collection of U.S. person data and the underlying reason for queries	No effect – disclosure of information will not impact collection of information, or unduly tax agency resources	May have a slight negative effect on commercial entities, as it draws public attention to their role in surveillance	No effect – would not impose additional barriers or crease additional protections	Would increase both governmental and public oversight of Section 702 surveillance
Should Congress continue to include a sunset provision in Section 702?	Lengthen the time before the sunset provision takes effect from 5 years to 10 years	Agencies would have greater certainty and confidence in their use of Section 702 authorities; however, without a sunset provision, Section 702 may be less likely to get updated in response to technological changes	Companies could be negatively impacted by uncertainty surrounding future use of Section 702 or repeated debate that brings their role in Section 702 surveillance to public attention	No effect – would change neither the amount of information collected about U.S. persons nor the protections that apply when information is queried with U.S. person identifiers.	Congressional and public oversight would decrease without mandated periodic debate and reapproval of Section 702

A. Should Additional Protections Be Provided for U.S. Person Information?

1. Description of Potential Amendment

Both decision makers and policy advocates have voiced concern over the protections applied to U.S. person information incidentally collected by Section 702 surveillance. The contents of these communications may have "nothing to do with terrorism or crime…[and] can include family photographs, love letters, personal financial matters, discussions of physical and mental health, and political and religious exchanges."[66] Given the potentially intimate information about U.S. persons that may be obtained through Section 702 surveillance, several commentators have suggested formalizing and strengthening the procedures that an agency must follow when querying surveillance collected under Section 702 for information about a specific U.S. person. When crafting additional protections to U.S. person information incidentally collected under Section 702, Congress may address three key questions: Who should be regulated? Who should regulate? What standard of evidence should be required to satisfy the regulation?

Congress may either seek to regulate use of U.S. person identifiers to query unminimized Section 702 surveillance by any federal agency, or focus only on those agencies most likely to threaten American's civil liberties. On one hand, uniform regulation across government agencies could promote consistency and minimize inefficiencies. On the other hand, because of their dual role as both an intelligence agency and a criminal investigatory agency, "the FBI's querying of 702 data for evidence of a crime…raises the most difficult Fourth Amendment issues."[67] Even though the FISC has held that the FBI's current minimization procedures comport with Fourth

66 David Medine, *Statement of David Medine, Chairman, Privacy and Civil Liberties Oversight Board, for the Senate Committee on the Judiciary on Oversight and Reauthorization of the FISA Amendments Act: the Balance Between National Security, Privacy and Civil Liberties* at 7, *available at* https://www.pclob.gov/library/20160510-SJC%20Medine%20Testimony.pdf. However, Rachel Brand has argued that it is highly unlikely that such information would be returned in response to a query of Section 702 data. *See* Rachel Brand, *Response to Questions for the Record from Chairman Charles E. Grassley*, *available at* https://www.judiciary.senate.gov/imo/media/doc/Brand%20Responses%20to%20QFRs.pdf.

67 House Committee Report at 7.

Amendment protections,[68] these procedures may raise significant policy issues by allowing "the FBI [to] read[] Americans' emails and listen[] to their phone calls without a factual basis to suspect wrongdoing, let alone a warrant."[69] Because U.S. person privacy concerns are so much more acute in the context of criminal investigations, Congress may want to consider only enacting further regulation of FBI queries of Section 702 data using U.S. person identifiers.

However, the way that the FBI stores data obtained through Section 702 surveillance could complicate this process. As previously discussed, unlike other agencies, the FBI stores information from all sources in confederated databases. FBI agents query these combined databases directly, and an agent cannot tell whether a query will return Section 702 information before she conducts the query. Therefore, placing restrictions on when the FBI can query databases containing Section 702 information using U.S. person identifiers could in practice place restrictions on all FBI queries involving U.S. person identifiers. Alternatively, such restrictions could lead the FBI to remove Section 702 information from the confederated databases, undercutting the advantages of such consolidation for law enforcement purposes.

Under the FBI's current procedures, agents who are trained to review Section 702 information are granted immediate access when their queries return Section 702 information; agents without this training must either undergo the training or consult with a trained agent.[70] The FBI could adopt similar practices to ensure that agents only view Section 702 information after some sort of higher level approval has been granted. Queries could notify FBI agents when Section 702 information is available without providing them access to that information; the agents could then be required to go through some sort of approval process to be granted access to that data. As discussed in the remainder of this section, Congress would have several options for designing this approval process.

---

68 FISC Memorandum Opinion and Order at 39 (2015), *available at* https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

69 House Committee Report at 34.

70 *Read the full testimony of FBI Director James Comey in which he discusses Clinton email investigation*, Washington Post, May 3, 2017, https://www.washingtonpost.com/news/post-politics/wp/2017/05/03/read-the-full-testimony-of-fbi-director-james-comey-in-which-he-discusses-clinton-email-investigation/?utm_term=.11e2243fcb12.

Congress could require agencies to seek additional approvals either from within their own agency or from external organizations, such as the FISC. David Medine, former chairman of the PCLOB, recommended that agencies "should be required to submit each U.S. person identifier to the FISA Court for approval before the identifier may be used to query information collected under Section 702" for either foreign surveillance or criminal investigatory purposes, unless exigent circumstances exist.[71] However, this proposal may unduly hamper intelligence agencies, who often act under intense time constraints. As former NSA lawyer April Doss testified before the House Judiciary Committee, "if it were necessary for intelligence analysts, who work 24 hours a day, 7 days a week, to receive prior approval from somewhere outside of the NSA or the CIA or the FBI, for instance, from the FISC to conduct a query, that could have a significant detrimental impact on intelligence activities."[72] This impact could be minimized by creating expedited approval mechanisms or allowing delayed approval under exigent circumstances. Additionally, if requiring FISC approval is too burdensome, Congress could impose additional regulatory processes either within each agency that uses Section 702 information or within the executive branch more broadly.

If Congress imposes additional protections for queries involving U.S. person identifiers, then they would need to establish the level of proof required to obtain approval for these queries. While Chairman Medine did not unequivocally describe the appropriate standard of review in instances where information collected under Section 702 is being queried using U.S. person identifiers for national security purposes,[73] queries conducted for criminal investigatory purposes should "at a minimum…meet[] the standard that the identifier is reasonably likely to return information relevant to an assessment or investigation of a crime, or a higher probable cause standard should Congress choose to impose it."[74]

---

71 Medine, *supra* note 71, at 8-9.

72 House Committee Report at 21.

73 While Chairman Medine stated that he "would not oppose requiring the government to meet a more exacting probable cause standard as others have suggested", he also supported the PCLOB recommendation that "the court should determine whether the use of the U.S. person identified for Section 702 queries is reasonably likely to return foreign intelligence information." *Id.* at 8.

74 *Id.* at 9.

Consequently, Congress should consider providing additional protections for U.S. persons whose information is collected under Section 702 by requiring the FBI to obtain permission from the FISC, based on a showing that they are reasonably likely to obtain foreign intelligence information or information relevant to a crime, before they are shown Section 702 data from queries using U.S. person identifiers.

2. Analysis Of Potential Amendment

Amending Section 702 to require permission from the FISC before receiving Section 702 data through queries that use U.S. person identifiers is likely to have a negative impact on the ability of government agencies to use information in an effective and timely manner. FBI agents would both need to go through the necessary processes to obtain permission of the FISC and develop sufficient evidence to support their request for FISC permission prior to obtaining Section 702 information from queries using U.S. person identifiers. Both of these factors would make it more difficult for agents to use Section 702 information to conduct investigations of U.S. persons. Furthermore, requiring government agents to obtain permission before receiving Section 702 information from searches involving U.S. persons may have downstream effects on their ability to conduct investigations.[75] If government agents can no longer use Section 702 information during the preliminary phase of investigations, they may have difficulties developing the evidence required to use more invasive, more highly regulated forms of surveillance.

However, there may be significant benefits to requiring government agents to obtain permission from the FISC prior to receiving Section 702 information from queries that use U.S. person identifiers. This amendment would decrease the use of information about U.S. persons incidentally collected under Section 702, as the barriers to use of this information increased. Additionally, the effectiveness of judicial oversight of Section

75 For evidence of this phenomenon in the context of a different type of surveillance, *see* Anne E. Boustead, *Police, Process, and Privacy: Three Essays on the Third Party Doctrine* (2016), *available at* http://www.rand.org/content/dam/rand/pubs/rgs_dissertations/RGSD300/RGSD384/RAND_RGSD384.pdf.

702 surveillance would increase, as judges would be afforded many new opportunities to review use of Section 702 information to investigate U.S. persons.

Congress may want to navigate this tradeoff by requiring FISC permission before Section 702 information is received through queries involving U.S. persons, but setting a low showing before such permission is granted. For example, Congress could decide to require agents to demonstrate a reasonable likelihood that they will obtain information relevant to foreign intelligence or criminal activity, rather than adopt a higher probable cause standard. This would provide increased protection for U.S. person information and improved oversight of Section 702 surveillance, while still allowing Section 702 information to be used during the preliminary phases of investigations.

B. Should Congress Explicitly Define When Criminal Defendants Are Required To Receive Notice That Section 702 Information Will Be Used Against Them At Trial?

1. Description of Potential Amendment

While the primary goal of Section 702 was to facilitate the collection of foreign intelligence information, the text of the statute allows the use of collected data either for either foreign intelligence or law enforcement purposes.[76] Foreign intelligence must be one purpose for the collection of communications under Section 702, but it need not be the sole or predominant purpose.[77] Surveillance conducted under Section 702 may reveal information relevant to criminal investigations related to terrorism – as in

76 50 U.S.C. § 1801(h).

77 *See* Donohue, *supra* note 49.

the cases of Adel Daoud[78] and Mohamed Mohamud,[79] both of whom were prosecuted for their roles in foiled terrorist plots based in part on the use of Section 702 information. However, Section 702 surveillance programs could also reveal information about criminal activity completely unrelated to terrorism. For example, if a U.S. person suspected of a robbery was in frequent communication with foreign nationals, the FBI could decide to query databases containing Section 702 data to see if any information about the robbery had been incidentally collected. Even though data collected under Section 702 was not collected with the goal of providing information about domestic, non-terrorism related criminal activity, the government has incentives to use this information to pursue the important objective of preventing and prosecuting crime.[80]

Although society benefits when law enforcement is able to investigate crimes efficiently and effectively, criminal investigations are regulated by Constitutional and statutory law to protect individual rights and prevent government overreaching and abuse. Criminal trials serve an important role in ensuring these goals are both accomplished, in part by requiring the government to both demonstrate the evidence against the defendant and explain how that evidence was obtained.[81] The criminal defendant's right to a fair trial also requires the state to provide an explanation of how evidence was obtained, since it allows him to decide whether his rights were violated during the collection of this evidence.[82] In the context of Section 702 surveillance, these norms are served by requiring that a U.S. person "must be notified by the government before any information obtained from

78 *Government wants to keep evidence secret in terrorism trial, but what does it have to hide?*, Privacy SOS, June 16, 2014, *available at* https://privacysos.org/blog/government-wants-to-keep-evidence-secret-in-terrorism-trial-but-what-does-it-have-to-hide/.

79 Bryan Denson, *Feds acknowledge warrantless wiretaps played role in Portland bomb-plot case against Mohamed Mohamud*, The Oregonian, Sept. 30, 2014, http://www.oregonlive.com/portland/index.ssf/2013/11/feds_acknowledge_warrantless_w.html.

80 The existence of these incentives has been remarked upon for years. As the Church Committee noted, "[t]he tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our findings. Intelligence collection programs naturally generate ever-increasing demands for new data. And once intelligence has been collected, there are strong pressures to use it against the target." Church Committee, *supra* note 9, at 4.

81 Patrick Toomey and Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 Santa Clara L. Rev. 843, 846 ("A society unaware that its government is secretly engaging in a particular surveillance method – even and especially one that breaks the law or violates the Constitution – can do nothing to challenge that practice.").

82 *Id.* at 847 ("and without notice of the use of surveillance in an individual case, a criminal defendant faced with a loss of liberty cannot put forward informed or specific arguments about whether the surveillance was lawful.").

or derived from Section 702 acquisition is used against him or her in any legal proceeding in the United States."[83]

In practice, this notice has rarely been provided.[84] This apparent discrepancy seems to be due to the way that the Department of Justice has defined "derived from."[85] For example the DOJ might define "evidence to be 'derived from' Section 702 surveillance only when it has expressly relied on Section 702 information in a later court filing…[and] then avoid giving notice to defendants simply by avoiding all references to Section 702 information in those court filings, citing information gleaned from other investigative sources instead – even if the information from those alternative sources would never have been obtained without Section 702."[86] However, because the DOJ's guidelines governing when defendants must be provided with notice have not been released to the public, it is virtually impossible to draw inferences about how Section 702 information is being used in investigations leading to criminal trials based on the instances in which notice has been provided. Without additional clarification, it is difficult for the public to understand how and why Section 702 is used during criminal proceedings – and for government agencies to rebut charges that Section 702 surveillance authorities may lead to pervasive government spying on U.S. citizens.

Furthermore, the DOJ's narrow construction of notice requirement also makes it more difficult for individuals to demonstrate standing to challenge the constitutionality of the use of Section 702 surveillance in criminal trials. Prior efforts by U.S. persons to challenge the constitutionality of Section 702 were rejected by the Supreme Court in *Clapper v. Amnesty International* because the plaintiffs were unable to establish that their communications had been intercepted, let alone that such interception was being conducted pursuant to Section 702.[87] In support of this decision, Justice Alito noted that the notice requirement ensured that there would be instances where a person could demonstrate that their communications

83 PCLOB Report at 64. *See* 50 U.S.C. ¶ 1806(c),(d).

84 Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?*, Just Security, Dec. 11, 2015, https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

85 *Id.*

86 *Id.*

87 *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013).

had been collected pursuant to Section 702, and consequently would have a strong claim of standing to challenge the statute.[88] Indeed, during oral arguments, Solicitor General Donald Verrilli described a situation where "an aggrieved person, someone who is a party to a communication, gets notice that the government intends to introduce information in a proceeding against them" as a "clear example[]" of a person who would have standing to challenge Section 702.[89] However, a narrow definition of "derived from" that denies criminal defendants notice that evidence against them was obtained through information learned by Section 702 surveillance limits the pool of individuals who could successfully demonstrate standing to challenge Section 702 – and therefore reduces the probability that the Supreme Court will have the opportunity to evaluate the constitutionality of Section 702.

Congress could explicitly define "derived from" to make clear when the government must provide notice to criminal defendants that Section 702 information has been used in an investigation. For example, Congress could require that the government provide notice whenever they rely on evidence that would not have been discovered but for information obtained through Section 702 surveillance. Explicitly and statutorily defining when evidence is "derived from" Section 702 would fulfill two functions. First, it would increase the frequency with which criminal defendants receive notice that Section 702 information was used to develop the case against them. This change would both ensure that criminal defendants would have complete knowledge of the evidence against them and increase public understanding of how Section 702 evidence is used at criminal trials. Second, it would also improve the predictability of such notice. Commenters have expressed concern that the government has not provided notice in criminal cases where it is later discovered that Section 702 surveillance did play a role in the development of the case. An explicit statutory definition would establish public expectations of the circumstances under which notice will be provided.

88 *Id*. at 1154 ("Thus, if the Government were to prosecute one of respondent-attorney's foreign clients using §1881a-authorized surveillance, the Government would be required to make a disclosure. . . . Such an attorney would certainly have a stronger evidentiary basis for establishing standing than do respondents in the present case.").

89 Transcript of Oral Argument at 4, *Clapper v. Amnesty International*, 133 S.Ct. 1138 (2013), *available at* https://www.supremecourt.gov/oral_arguments/argument_transcripts/11-1025.pdf

Therefore, Congress should consider statutorily defining when evidence is "derived from" Section 702 surveillance such that government agencies must provide notice when information used during the criminal investigation against them would not have been uncovered without reliance on information obtained through Section 702 surveillance.

2. Analysis of Potential Amendment

A clearer definition of when evidence is "derived from" Section 702 surveillance would increase both judicial and public oversight of Section 702. Requiring the government to give notice whenever they use evidence that would not have been discovered but for Section 702 information would provide the judicial branch with a more accurate picture of when this surveillance is used in the context of domestic criminal investigations – and when it is not. This would allow improved oversight, and a robust debate about whether Section 702 comports with the relevant Constitutional rights and norms. It would also put the public on notice of how frequently Section 702 surveillance is used at trial in the United States.

U.S. government agencies may decrease their use of U.S. person information collected under Section 702 if they can no longer obscure use of this information at trial. Assuming the government has an interest in keeping use of Section 702 surveillance authorities as secret as possible in order to prevent countersurveillance, they may restrict their use of Section 702 information to the investigation of serious crimes, when the cost of disclosing the use of surveillance is exceeded by the societal benefit in stopping and prosecuting criminal activity. In other words, mandating disclosure creates incentives for government officials to more closely police their use of Section 702 surveillance.

However, improved disclosure about use of Section 702 information during criminal trials may harm the commercial entities that are required to participate in these surveillance programs. Section 702 surveillance has been justified to the public in part based on its role as a mechanism for collecting foreign intelligence and counterterrorism information; disclosure of its use in criminal trials would seem to undermine this justification. Under

those circumstances, commercial entities may face a backlash similar to the one they faced when their role in Section 702 surveillance programs was originally disclosed.

C. Should Congress Require Additional Transparency Mechanisms?

1. Description of Potential Amendment

Policymakers have long struggled with how much information about government use of electronic surveillance should be made public. "Complete transparency paralyzes planning and action; complete opacity endangers both liberty and security."[90] The government often seeks to keep information about electronic surveillance secret, to avoid warning those under surveillance and to limit the development of counter-surveillance practices more broadly. However, publishing information about electronic surveillance both increases public oversight and helps align public expectations with government practices. These concerns are particularly salient in the context of Section 702 programs, as their controversial nature is in part due to the fact that they became public knowledge through leaked information rather than voluntary public disclosure and education.

The public release of information describing surveillance practices under Section 702 may also assist the Intelligence Community in advocating for the value of these programs. Public availability of data regarding Section 702 surveillance programs would help the government prospectively argue for the value of specific collection practices, and retrospectively demonstrate how changes in surveillance practices affected the volume of data obtained. For example, the NSA has argued their recent decision to discontinue "about" collection while conducting upstream collection will cause them to "los[e] some other important data."[91] The public availability

90 Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. Chi. L. Rev. 245, 246 (2008).

91 Press Release, National Security Agency, NSA Stops Certain Foreign Intelligence Collection Activities Under Section 702 (Apr. 28, 2017), *available at* https://www.nsa.gov/news-features/press-room/press-releases/2017/nsa-stops-certain-702-activites.shtml.

of data regarding Section 702 surveillance could help shape the conversation around how that decision affected access to information.

The text of Section 702 does not include a requirement that information about programs authorized under this statute be made available to the general public. Instead, a public oversight function is partially fulfilled by the requirement that the executive branch provide regular reports assessing their compliance with targeting and minimization procedures to the congressional intelligence committees and the Committees on the Judiciary of the Senate and the House of Representatives.[92] Additionally, in 2014, the PCLOB recommended that the NSA release annual statistics on the number of communications obtained through Section 702 surveillance, including "the number of telephone communications acquired in which one caller is located in the United States" and "the number of queries performed that employ U.S. person identifiers, specifically distinguishing the number of such queries that include names, titles, or other identifiers potentially associated with individuals."[93]

In response to the PCLOB recommendations, the ODNI adopted the practice of releasing an annual transparency report providing some statistics about the use of Section 702 programs, among other things.[94] These reports describe the number of Section 702 orders, estimated number of affected targets, estimated number of search terms related to a known U.S. person use to query Section 702 information, and the estimated number of queries related to a known U.S. person used to query Section 702 information in a given year.[95] However, these data do not describe the use of Section 702 information by the FBI. This is particularly problematic as the most controversial uses of Section 702 relate to criminal prosecutions of U.S. persons, which would fall within the purview of the FBI.

Congress could choose to increase the transparency of Section 702 surveillance in a number of ways. First, Congress could make the disclosure of

92 50 U.S.C. 1881a(l)(2)(B).

93 Privacy & Civil Liberties Oversight Board, *Recommendations Assessment Report* 24 (2016).

94 *See, e.g.,* Office of the Director of National Intelligence, *Statistical Transparency Report Regarding Use of National Security Authorities – Annual Statistics for Calendar Year 2015*, *available at* https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2015.

95 *Id.*

data and guidelines regarding Section 702 surveillance mandatory rather than voluntary. Mandatory reporting mechanisms provide assurance that data will continue to be collected and disclosed, even as the leadership of the ODNI and intelligence agencies change. Additionally, Congress can mandate not only the fact of disclosure, but also the method calculating the statistics to be disclosed. This allows Congress to ensure that these statistics are calculated in a reliable and consistent fashion, so that trends over time can be described and analyzed. However, the release of data about the number of affected targets, search terms, and queries are necessary but not sufficient to provide effective public oversight. The public must also be provided with enough information to understand the context of these data. Without this context, the numbers themselves may serve to obfuscate rather than clarify use of the underlying surveillance programs.[96] The disclosure of targeting and minimization guidelines are just as important for transparency as the disclosure of annual statistics, as they provide the necessary context for the reported numbers.

Second, members of Congress involved in oversight of Section 702 have repeatedly asked for an "estimate of the impact of 702 on United States citizens,"[97] generally meaning either the number of U.S. persons whose communications have been collected under Section 702[98] or the number of communications to/from U.S. persons collected under Section 702.[99] However, some current and former government officials have argued that requiring the government to estimate the amount of U.S. person information incidentally collected under Section 702 would itself "raise[] significant privacy implications" as it would require the government to "deliberately hold and analyze information about U.S. persons…that it would otherwise have no reason to collect or retain."[100] As described by

96 For example, the vast majority of government surveillance requests made to the FISC are approved through a process where the government is able to consult with and obtain feedback from a FISC judge before the application is formally submitted. Consequently, statistics on the approval rate of applications may understate the rigor of FISC oversight, since they do not reflect applications altered or withdrawn during the initial consultation process. Without this additional information about the application process, statistics about the FISC's application approval rate and misleading and do not serve the goals of public transparency.

97 House Committee Report at 3.

98 Press Release, Sen. Ron Wyden, *Wyden: The Public Must Know How Many Americans Are Swept Up in Warrantless Surveillance Under FISA 702* (March 15, 2017), *available at* https://www.wyden.senate.gov/news/press-releases/wyden-the-public-must-know-how-many-americans-are-swept-up-in-warrantless-surveillance-under-fisa-702.

99 House Committee Report at 81.

100 House Committee Report at 21, 30.

April Doss, a former lawyer at the NSA, counting the number of U.S. person communications would "require the Intelligence Community to conduct exhaustive analysis of every unknown identifier in order to determine whether they are being used inside or outside the U.S., and whether their users might be U.S. persons located anywhere in the world,"[101] which would both infringe the privacy of U.S. persons and drain agency resources.

However, there are several practices that may make an estimate of incidental collection of U.S. person information under Section 702 feasible. First, those interested in measuring incidental collection should be precise about the quantity of interest: it is a very different thing to estimate the number of U.S. persons who have had their information collected under Section 702 than to estimate the number of communications to/from U.S. persons that have been collected under Section 702. Although they may sound similar, in practice it is much easier to estimate the number of communications to/from U.S. persons collected under Section 702 than it is to estimate the number of persons who have their communications collected. Second, members of Congress interested in estimating the incidental collection of U.S. person communications should specify more precisely how a communication should be determined to be to/from a U.S. person for purposes of this estimate. The NSA should provide technical support as Congress develops these specifications, to ensure they are feasible. It may be sufficient to demonstrate that a phone number has a U.S. country code or that an email is being sent from a U.S. IP address, rather than definitely demonstrate that a party to the conversation is a U.S. person.[102] While this method would introduce some inaccuracies, it would also have the effect of lowering the cost of estimating the number of U.S. person communications incidentally collected under Section 702, both in terms of agency time and individual privacy. Finally, to further lower the cost of collecting this information, the estimate could be based on a random sample of communications collected under Section 702. Third, additional information and statistics may also help advance transparency and help assuage public concerns about the use of Section 702 surveillance authorities. There are many compelling policy questions about Section 702 that would increase public

101 *Id. at* 31.

102 See House Committee Report at 80-81. This approach to estimating the number of U.S. person communications would not work for communications collected through the PRISM program. *Id*.

understanding without sacrificing the effectiveness of this surveillance. For example, there are currently concerns that Section 702 surveillance may be used in criminal prosecutions unrelated to terrorism.[103] However, the yearly transparency reports currently released by the ODNI provide no data on how many criminal prosecutions initiated in a particular year have used Section 702. It might be feasible to ask the DOJ to disclose either the yearly number of prosecutions that have used Section 702 surveillance across different categories of crimes, or indicate whether any prosecutions for particular categories of crimes have used Section 702 surveillance in a given year. In such a reporting regime, the categorization of crimes could be borrowed from existing crime reporting efforts, such as the Uniform Crime Reports.[104]

These requirements may appear to place a heavy burden on the intelligence agencies that conduct surveillance. However, similar reporting standards are required for agencies that use other surveillance authorities, including state and local agencies with significantly fewer resources. One example of this reporting is the Wiretap Reports, which have been released yearly by the Administrative Office of the U.S. Courts since 1968. These reports include detailed information on each Wiretap Request made by federal and state law enforcement. While it may not be feasible (or even advisable) to provide a similar level of disclosure for Section 702 surveillance, Congress could require every agency that queries databases containing Section 702 data to complete a yearly disclosure form that would provide information about how and how often these databases are used to obtain information about U.S. persons. Furthermore, in some cases the information collection necessary to calculate these statistics could be built into existing internal oversight mechanisms. For example, as prosecutors are already required to obtain permission from the AG prior to using Section 702 information at trial, the burden created by requiring them to provide information about the type of crime being prosecuted would appear to be minimal.

103 *See*, *e.g.*, Dia Kayyali, *The Way the NSA Uses Section 702 is Deeply Troubling. Here's Why*, Electronic Frontier Foundation, May 7, 2014, https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why ("While the justification we've heard repeatedly is that NSA surveillance is keeping us safer, data collected under Section 702 can be shared in a variety of circumstances, such as ordinary criminal investigations.").

104 For a discussion of how the Uniform Crime Reports define and categorize different types of criminal activities, *see* U.S. Department of Justice, *UCR Offense Definitions* (2009), https://www.ucrdatatool.gov/offenses.cfm.

Fourth, Congress may want to ensure that the PCLOB has the personnel, power, and resources needed to continue "ensur[ing] that the federal government's efforts to prevent terrorism are balanced with the need to protect privacy and civil liberties."[105] The PCLOB is intended to be comprised of five members, including four part-time members and one full-time chairman who is authorized to hire staff to support the agency's work. However, there is currently only one member serving on the PCLOB – two short of the three necessary for a quorum.[106] As a result, the PCLOB is expected to be "unable to function for all of 2017 if not longer."[107] Although the president is tasked with appointing members to the PCLOB,[108] Congress could act to ensure the continued viability of the PCLOB in other ways. For example, during recent House Judiciary Committee meetings on Section 702, one witness suggested that Congress could allow PCLOB members other than the chairman to hire staff, and "to require, as part of the FISA Court's annual review, [that the government] certify that the President has made nominations to fill any vacancies."[109] Allowing existing members to act as chairperson in the absence of an appointed chairman would allow the PCLOB to continue functioning even when it is not fully staffed. However, conditioning FISA Court annual review on the nomination of PCLOB members could unduly complicate the review process.

Consequently, Congress should consider requiring yearly disclosure of an estimate of the number of communications with at least one U.S. correspondent collected through Section 702 surveillance; and that the FBI release a yearly estimate of the number of times they queried data collected under Section 702 for information about a U.S person, the number of U.S. persons who the FBI sought to obtain information about through these queries, and high-level statistics on the types of crimes that were under investigation, as well as the targeting and minimization guidelines used to collect this information. Congress should also consider allowing remaining PCLOB members to serve as acting chairperson.

105 Privacy and Civil Liberties Oversight Board, *About the Board* (last visited May 17, 2017), https://www.pclob.gov/about-us.html.

106 42 U.S.C. § 2000(h).

107 Paul Rosenzweig, *Near-Death of the PCLOB*, Lawfare, Dec. 21, 2016, https://www.lawfareblog.com/near-death-pclob.

108 *Id.* PCLOB members must also be confirmed by the senate.

109 House Committee Report at 94.

2. Analysis of Potential Amendment

Increased, mandatory reporting of statistics related to Section 702 would significantly strengthen the effectiveness of both legislative and public oversight. First, legislators would be better positioned to maintain awareness of how Section 702 is being used, in order to spot both circumstances where this surveillance may be threatening civil liberties and circumstances where the intelligence community may need additional authority or resources. Additionally, legislators would also be more able to educate their constituents about how Section 702 is being used and regulated, as they could rely on this publicly available information to support their arguments. Second, the public would be better informed and therefore would be better positioned to advocate for future amendments of Section 702 if needed to maintain both the public interest in national security and the individual interest in privacy.

However, the release of additional data regarding the use of Section 702 might have a slight negative effect on the commercial entities who are required to participate in these surveillance programs. The yearly disclosure of data regarding Section 702 would repeatedly draw attention to their role in government surveillance programs. Congress could mitigate this harm by not disclosing statistics about the commercial entities that participate in Section 702 surveillance programs.

Increased reporting of statistics related to Section 702 will probably not have a significant impact on the government's ability to obtain and use information under this program. Additional transparency measures would not restrict the amount of information government agencies can collect, nor place additional requirements upon this collection – simply require that data about this collection be released to the public after the fact. Furthermore, some disclosures are already taking place on a voluntary basis, suggesting that the process of gathering and disclosing this information does not unduly tax agency resources. Similarly, transparency requirements are unlikely to affect collection and use of information about U.S. persons. These requirements would not impose any additional barriers on collection of information, or increase protections for U.S. persons whose information is incidentally collected.

D. Should Congress Continue to Include a Sunset Provision in Section 702?

1. Description of Potential Amendment

Every version of section 702 enacted over the years has included a sunset provision: a clause that causes it to expire on a given date unless Congress affirmatively acts to reauthorize it.[110] Section 702 was last due to sunset on December 31, 2012; it was reauthorized without amendments on December 30, 2012, by simply extending its expiration date to December 31, 2017.[111] If Congress reauthorizes Section 702 without a sunset provision, the statute would remain valid indefinitely unless it was repealed by subsequent Congressional action or ruled to be unconstitutional by the Supreme Court.

Many calls to reauthorize Section 702 are silent on whether Congress should include a new sunset provision, such that the reauthorized Section 702 would expire at a future date unless Congress once again reauthorized it. However, some commenters have argued that additional sunset provisions should not be required, as Section 702 "has demonstrated its usefulness; and an arbitrarily forced reconsideration by Congress is unnecessary, a waste of time and money, and at the expense of national security."[112] During an open meeting of the Senate Judiciary Committee, Senator Grassley asked three expert panels whether Section 702 should be reauthorized without a sunset provision; they agreed that a sunset provision was no longer necessary.[113] **Therefore, Congress should consider reauthorizing Section 702 with a sunset provision that takes effect in ten years, rather than five.**

110 For further discussion of sunset provisions, *see* Brian Baugus and Feler Bose, *Sunset Legislation in the States: Balancing the Legislature and the Executive*, Mercatus Research Center at George Mason University (2015), *available at* https://www.mercatus.org/system/files/Baugus-Sunset-Legislation.pdf.

111 P.L. 112-238 (2012), *available at* https://www.congress.gov/112/plaws/publ238/PLAW-112publ238.pdf.

112 *Id.*

113 *See* Responses to Questions for the Record from Ranking Member Charles E. Grassley (2016), *available at* https://www.judiciary.senate.gov/imo/media/doc/Wainstein%20Respoonses%20to%20QFRs.pdf, https://www.judiciary.senate.gov/imo/media/doc/Olsen%20Responses%20to%20QFRs.pdf, https://www.judiciary.senate.gov/imo/media/doc/Brand%20Responses%20to%20QFRs.pdf.

2. Analysis of Potential Amendment

Removing the sunset provision would provide additional certainty to actors in the Intelligence Community,[114] and avoid economic, political, and security costs associated with reauthorization. As described by Matthew Olsen, "[t]he authority is well-established, and maintaining a sunset provision may only add uncertainty to the Executive Branch's operation of the program and potentially undermine its effectiveness."[115] However, without periodic review of Section 702 in light of contemporary technology, there is a risk that it would become yet another outdated and ineffective surveillance authority, which could harm the ability of the government to the information necessary to protect national security and prevent terrorist activity. However, requiring repeated reauthorization of Section 702 forces Congress to reconsider this surveillance authority in light of changes in communication technology and consumer practices, ensuring that it remains relevant. Periodic reauthorization may allow Section 702 to avoid becoming outdated and ineffective, which is a frequent concern for electronic surveillance laws. Consequently, a sunset provision that takes effect in ten years (rather than five) might prove to be an acceptable compromise.

Removing the sunset provision in Section 702 would harm legislative oversight of this surveillance program. Reauthorization requirements compel Congress to consider the value of Section 702 surveillance and the potential impact on civil liberties both inside and outside the United States. Without periodic deadlines, Congress would have fewer incentives to monitor Section 702 surveillance. Additionally, the general public may become less aware of Section 702 and its role in protecting national security, as Section 702 surveillance would be featured less often in the news without regular Congressional action.

On the other hand, reauthorizing Section 702 without a sunset provision may minimize future harm to American companies. Regular debates surrounding the reauthorization of Section 702 may cause ongoing difficulty to American telecommunication and computing companies, as their

114 "[A] sunset clause serves little purpose at this point and may only add uncertainty to the Executive Branch's operation of Title VII programs." *Id.*

115 *Id.*

participation in Section 702 surveillance programs again becomes the subject of public discussions both domestically and internationally.

All-in-all, it appears that removing the sunset provision from Section 702 may have a mixed impact. While it would improve certainty for intelligence agencies and possibly minimize harm to telecommunications companies, it would decrease oversight and decrease the likelihood that Section 702 would be revised in response to technological changes. Consequently, Congress should consider lengthening the period before the sunset provision takes effect, in order to maximize the benefits and minimize the costs of a reauthorization debate.

V. Conclusion

During the upcoming reauthorization debate, Congress has several options to amend Section 702. As these options may differentially impact key policy concerns, Congress is now faced with the task of negotiating the tradeoffs inherent in these choices, particularly their potential impact on privacy and national security. However, while privacy and national security may sometimes be viewed as competing values, the ultimate goal of surveillance law is to ensure that both are protected. As Representative Goodlatte stated during a recent House Judiciary Committee meeting on Section 702, "[s]trong and effective national security tools, like Section 702, and civil liberties can and must coexist."[116]

Consequently, Congress can – and should – prioritize options that protect both security and privacy. For example, when deciding whether to further regulate government queries of Section 702 data using U.S. person identifiers, Congress could minimize the burden created by this amendment by establishing a relatively low burden for receiving FISC approval: requiring that the government demonstrate that they are reasonably likely to obtain relevant information, rather than establishing a more exacting probable cause standard. However, establishing a low burden of proof would lessen – although not eliminate – the privacy protections created by requiring FISC approval for queries involving U.S. person identifiers. Alternatively, Congress could reduce the burden of this new policy on the government by developing a streamlined process for obtaining FISC approval to query Section 702 information using U.S. person identifiers. Lowering the practical barriers to obtaining FISC permission would not require lowering the legal impact of those barriers: it is possible to simultaneously mandate that the government demonstrate a high level of proof before obtaining information, and make the process of demonstrating that proof as straightforward as possible. Such an option would promote both privacy and security.

116 House Committee Report at 3.

The Cyber Security Project
Belfer Center for Science and International Affairs
Harvard Kennedy School
79 John F. Kennedy Street
Cambridge, MA 02138

www.belfercenter.org/Cyber

Printed in the United States of America