STATEMENT OF

ELIZABETH GOITEIN
CO-DIRECTOR, LIBERTY AND NATIONAL SECURITY PROGRAM
BRENNAN CENTER FOR JUSTICE AT NEW YORK UNIVERSITY SCHOOL OF LAW

BEFORE THE

UNITED STATES SENATE
COMMITTEE ON THE JUDICIARY

HEARING ON

THE FISA AMENDMENTS ACT: REAUTHORIZING AMERICA'S VITAL NATIONAL SECURITY AUTHORITY AND PROTECTING PRIVACY AND CIVIL LIBERTIES

JUNE 27, 2017

Introduction

Chairman Grassley, Ranking Member Feinstein, and members of the committee, thank you for this opportunity to testify on behalf of the Brennan Center for Justice at New York University School of Law.[1] The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. I co-direct the Center's Liberty and National Security Program, which works to advance effective counterterrorism policies that respect constitutional values and the rule of law.

Congress's goal, when it passed the FISA Amendments Act in 2008 (thus creating Section 702 of FISA), was to give our government more powerful tools to address terrorist threats. In keeping with this goal, the authorities conferred by Section 702 have been used to monitor suspected terrorists overseas in order to trace their networks and interrupt their plots. This use of the law is widely recognized as appropriate and has caused little controversy.

In writing the law, however, Congress did not expressly limit Section 702 surveillance to such activities. Instead, Congress gave significant discretion to the executive branch and the FISA Court, trusting them to ensure that the law was implemented in a manner consistent with its objective. For instance, Congress allowed the government to target *any* foreigner overseas, counting on intelligence agencies to focus their efforts on those who pose a threat to our interests. Congress also did not specify what minimization should look like, leaving that to the agencies and the judges of the Foreign Intelligence Surveillance Court.

It would be wrong to suggest that this trust has somehow been betrayed. There has been very little evidence of intentional abuse or misuse. The executive branch, however, has taken full advantage of the leeway provided in the statute. Instead of simply acquiring the communications of suspected terrorists or foreign powers overseas, the government is scanning nearly all of the international communications that flow into and out of the United States via the Internet backbone, and is acquiring hundreds of millions of these communications each year. This surveillance inevitably pulls in massive amounts of Americans' calls and e-mails.

We have also seen mission creep. A statute designed to protect against foreign threats to national interests has become a major source of warrantless access to Americans' data, and a tool for ordinary domestic law enforcement. This outcome is contrary, not only to the original intent of the Foreign Intelligence Surveillance Act, but to Americans' expectations and their trust that Congress will protect their privacy and freedoms.

It is now up to Congress to enact reforms that will provide such protection. The core of Section 702 is the ability it gives the government to obtain the communications of foreign powers and suspected foreign terrorists without obtaining a warrant. There are several potential reforms that would leave this core intact, while adding badly needed protections for law-abiding citizens of this country and others. Most important, Congress should narrow the scope of

[1] This testimony is submitted on behalf of a Center affiliated with New York University School of Law but does not purport to represent the school's institutional views on this topic. More information about the Brennan Center's work can be found at http://www.brennancenter.org.

permissible targets to those suspected of posing a threat to the U.S. and its interests, and it should shore up protections for Americans whose communications are "incidentally" collected by requiring a warrant to search their calls and e-mails and by tightening minimization requirements.

I. Section 702: A Massive Expansion in the Scope of Foreign Intelligence Surveillance

Technological advances have revolutionized communications. People are communicating at a scale unimaginable just a few years ago. International phone calls, once difficult and expensive, are now as simple as flipping a light switch, and the Internet provides countless additional means of international communication. Globalization makes such exchanges as necessary as they are easy. As a result of these changes, the amount of information about Americans that the NSA intercepts, even when targeting foreigners overseas, has exploded.[2]

But instead of increasing safeguards for Americans' privacy as technology advances, the law has evolved in the opposite direction since 9/11. In its zeal to bolster the government's powers to conduct surveillance of foreign threats, Congress has amended surveillance laws in ways that increasingly leave Americans' information outside their protective shield (the USA FREEDOM Act being the notable exception). Section 702 is a particularly striking example.

Before 2007, if the NSA, operating domestically, sought to wiretap a foreign target's communications with an American inside the U.S., it had to show probable cause to the Foreign Intelligence Surveillance Court (FISA Court) that the target was a foreign power – such as a foreign government or terrorist group – or its agent. The Protect America Act of 2007 and the FISA Amendments Act of 2008 (which created Section 702 of FISA) eliminated the requirement of an individualized court order. Domestic surveillance of communications between foreign targets and Americans now takes place through massive collection programs that involve no case-by-case judicial review.[3]

Executive officials have often argued that Section 702 was necessary to address changes in communications technology and "modernize" FISA. It is true that, before 2007, the NSA was legally required to obtain a FISA Court order to collect foreign-to-foreign e-mails that were stored inside the United States – something Congress almost certainly did not intend when it originally passed FISA. Section 702, however, went much further than necessary to correct that problem. It did not simply allow the warrantless collection of foreign-to-foreign e-mails stored inside the U.S.; it allowed the warrantless collection of communications, both stored and in transit, between foreign targets and Americans. This state of affairs differs fundamentally from the regime Congress designed in 1978.[4]

---

[2] *See* ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CTR. FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 19-21 (2015), https://www.brennancenter.org/sites/default/files/analysis/What_Went_%20Wrong_With_The_FISA_Court.pdf.

[3] *See* 50 U.S.C. § 1881a.

[4] Some executive branch officials have suggested that Congress in 1978 intended to regulate surveillance only for purely domestic communications. They note that FISA required the government to obtain an individual court order

Another critical change is that the pool of permissible targets is no longer limited to foreign powers or their agents. Under Section 702, the government may target for foreign intelligence purposes any person or group reasonably believed to be foreign and located overseas.[5] The person or group need not pose any threat to the United States, have any information about such threats, or be suspected of any wrongdoing. This change not only renders innocent private citizens of other nations vulnerable to NSA surveillance; it also greatly increases the number of communications involving Americans that are subject to acquisition – as well as the likelihood that those Americans are ordinary, law-abiding individuals.

Further expanding the available universe of communications, the government and the FISA Court have interpreted Section 702 to allow the collection of any communications to, from, *or about* the target.[6] The inclusion of "about" in this formulation is a dangerous leap that finds no basis in the statutory text and little support in the legislative history. In practice, it has been applied to collect communications between non-targets that include the "selectors" associated with the target (e.g., the target's e-mail address or phone number). In theory, it could be applied even more broadly to collect any communications that even mention ISIS or a wide array of foreign leaders and public figures who are common topics of conversation. Although the NSA is prohibited from intentionally acquiring purely domestic communications, such acquisition is an inevitable result of "about" collection.

---

when collecting any communications involving Americans that traveled by wire, but required an individual court order to obtain satellite communications only when all of the communicants were inside the U.S. Asserting that wire technology was the norm for domestic calls, while most international communications were carried by satellite (and were thus "radio communications"), they infer that Congress intended to require the government to obtain an order when acquiring purely domestic communications, but not when obtaining communications between foreign targets and Americans. This intent, they argue, was undermined when fiber-optic cables later became the standard method of transmission for international calls.

The problem with this theory is two-fold. First, it would have been quite simple for Congress to state that FISA orders were required for purely domestic communications and not for international ones. Instead, Congress produced an elaborate, multi-part definition of "electronic surveillance" that relied on particular technologies rather than the domestic versus international nature of the communication. Second, contrary to the factual premise of this theory, the available evidence indicates that one third to one half of international communications *were* carried by wire back in 1978. David Kris, *Modernizing the Foreign Intelligence Surveillance Act* 3 (Brookings Inst., Working Paper, 2007), *available at* http://www.brookings.edu/~/media/research/files/papers/2007/11/15%20nationalsecurity%20kris/1115_nationalsecurity_kris.pdf.

A more plausible explanation for the original FISA's complex scheme was put forward by David Kris, a former head of the Justice Department's National Security Division. Mr. Kris concluded that Congress intended to require a court order for international wire communications obtained in the U.S., and that the purpose behind its definitional acrobatics was to leave legislation covering surveillance conducted outside the U.S. and NSA satellite surveillance for another day. *Id.* at 13-23. Although Congress never followed up, the legislative history of FISA made clear that the gaps in the statute's coverage of NSA's operations "should not be viewed as congressional authorization for such activities as they affect the privacy interests of Americans." S. REP. NO. 95-701, at 35 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4004.

[5] 50 U.S.C. § 1881a(b).

[6] PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 37 (2014) [hereinafter PCLOB 702 REPORT], *available at* https://www.pclob.gov/library/702-report.pdf.

The NSA's failure to comply with minimization rules for "about" collection (discussed later in this testimony), which delayed the FISA Court's approval of the program in 2016, led the agency to stop the practice in April of this year.[7] However, the agency is reportedly working to solve the problems that may have led to the non-compliance.[8] It is thus not only possible but likely that the agency will attempt to resume "about" collection in the future.

Other than the foreignness and location criteria (and certain requirements designed to reinforce them), the only limitation on collection imposed by the statute is that the government must certify that acquiring foreign intelligence is a significant purpose of the collection.[9] FISA's definition of foreign intelligence, however, is not limited to information about potential threats to the U.S. or its interests. Instead, it includes information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[10] This could encompass everyday conversations about current events. A conversation between friends or colleagues about the merits of the North American Free Trade Agreement or whether the United States should build a wall along the border with Mexico, for instance, "relates to the conduct of foreign affairs." Moreover, while a significant purpose of the program must be the acquisition of foreign intelligence, the primary purpose may be something else altogether.[11] Finally, the statute requires the FISA Court to accept the government's certifications under Section 702 as long as they contain the required elements.[12] These factors greatly weaken the force of the "foreign intelligence purpose" limitation.

The government uses Section 702 to engage in two types of surveillance. The first is "upstream collection," whereby communications flowing into and out of the United States on the Internet backbone are scanned for selectors associated with designated foreigners. Although the data are first filtered in an attempt to weed out purely domestic communications, the process is imperfect and domestic communications are inevitably acquired.[13] The second type of Section 702 surveillance is "PRISM collection," under which the government provides selectors, such as e-mail addresses, to U.S.-based electronic communications service providers, who must turn over any communications to or from the selector.[14]

Using both approaches, the government collected more than 250 million Internet transactions a year as of 2011.[15] Because agencies generally may store Section 702 data for at least five years, a yearly intake of 250 million communications would result in at least 1.25 billion communications residing in government databases at any given time. The actual number

---

[7] Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets,* N.Y. TIMES, Apr. 28, 2017, https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html.
[8] Jenna McLaughlin & Elias Groll, *NSA Halts Controversial Spy Program,* FOREIGN POLICY, Apr. 28, 2017, http://foreignpolicy.com/2017/04/28/nsa-halts-controversial-spy-program/.
[9] 50 U.S.C. § 1881a(g)(2)(A)(v).
[10] 50 U.S.C. § 1801(e)(2).
[11] *In re* Sealed Case, 310 F.3d 717, 734 (FISA Ct. Rev. 2002).
[12] 50 U.S.C. § 1881a(i)(3)(A).
[13] PCLOB 702 REPORT, *supra* note 6, at 36-41.
[14] *Id.* at 33-34.
[15] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).

is almost certainly higher, as the 250 million figure does not include telephonic communications, and the number of targets today is likely significantly larger than in 2011.[16]

Due to these changes wrought by Section 702, it can no longer be said that FISA is targeted at foreign threats. To describe surveillance that acquires hundreds of millions of communications each year as "targeted" is to elevate form over substance. And on its face, the statute does not require that the targets of surveillance pose any threat, or that the purpose of the program be the collection of threat information.

Congress no doubt trusted that the executive branch would exercise these broad powers judiciously, and would not conduct surveillance of innocent private citizens abroad simply because the statute, on its face, allows it. And it is certainly possible that the government has chosen to focus its surveillance more narrowly than Section 702 requires. The certifications that the government provides to the FISA Court – which include the foreign intelligence categories at which surveillance is aimed, and could therefore shed some light on this question – have not been publicly disclosed by the government.

Even assuming that actual practices stop short of what the law allows, however, the available statistics suggest a scope of surveillance that is difficult to reconcile with claims of narrow targeting. A leaked copy of one of the certifications, listing the foreign nations and factions about which foreign intelligence may be sought, lends support to the conclusion that surveillance is in practice quite broad: it includes most of the countries in the world, ranging from U.S. allies to small countries that play little role on the world stage.

More important, Americans' privacy should never depend on any given administration's voluntary self-restraint, or on the hope that the FISA Court will impose additional requirements beyond those laid out in the statute. Section 702 establishes the boundaries of permissible surveillance, and it clearly allows collection of communications between Americans and foreigners who pose no threat to the U.S. or its interests. That creates an enormous opening for unjustified surveillance and implicates a range of other harms discussed in Part III of this testimony.

II. The Impact of Section 702 on Americans

Because the "target" of surveillance must be someone reasonably believed to be a foreigner overseas, the collection of Americans' communications with those targets is described as "incidental," and the statute requires "minimization" of those Americans' information. These are terms of art that have particular legal meanings. Legal and policy defenses of Section 702 in its current form rely heavily on these terms and concepts.

[16] The number of targets under Section 702 has increased for each of the 4 years that the statistic has been made available. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING THE USE OF NATIONAL SECURITY AUTHORITIES FOR CALENDAR YEAR 2016 (Apr. 2017), *available at* https://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2016.

The impact on Americans' privacy, however, does not. If the government is collecting tens of millions of Americans' communications and keeping them for years in databases where they are vulnerable to abuse, inadvertent mishandling, or hacking, it matters little – from a practical perspective – that their initial acquisition was "incidental," or that the procedures allowing them to be kept and stored include "minimization" in their title. And if FBI agents are searching this data for Americans' communications, reading and listening to them, and using them against Americans in legal proceedings, those Americans will not be particularly comforted (indeed, they may well be baffled) to hear that they are not "targets."

For these reasons, it is critical for Congress and the public to have a sense of the volume of Americans' communications being collected and stored, to examine whether the retention and dissemination of Americans' information is in fact being "minimized," and to confront the problem of back door searches.

A. How Many Americans' Communications Does the NSA Collect?

Section 702 surveillance obtains the communications, not only of foreign targets, but of any Americans who are in contact with them. The number of Americans' communications thus collected is likely quite large: if only one out of every twenty communications is with an American, that would still add up to more than 12.5 million communications a year. But there is no official public information on how many Americans' communications are in fact swept up in Section 702 surveillance.

In 2011, Senators Wyden and Udall asked the Inspectors General of the Intelligence Community and the NSA to come up with a public estimate of this number.[17] The Inspectors General responded that generating an estimate would itself violate Americans' privacy, ostensibly because it might involve reviewing communications that would otherwise not be reviewed.[18] In October of 2015, however, a coalition of more than thirty advocacy groups – including many of the nation's most prominent privacy organizations – sent a letter to the Director of National Intelligence (DNI) urging that the NSA go forward with producing an estimate.[19] The letter noted that, as long as proper safeguards were in place, the result would be a net gain for privacy.

In April 2016, a bipartisan group of fourteen House Judiciary Committee members sent the DNI a letter making the same request.[20] Eight months later, the members wrote again to

---

[17] *See* Letter from Senators Ron Wyden and Mark Udall to The Honorable I. Charles McCullough III, Inspector General of the Intelligence Cmty. and Dr. George Ellard, Inspector General, Nat'l Sec. Agency (May 4, 2011), *available at* https://www.wyden.senate.gov/download/?id=CE360936-DFF9-4273-8777-09BF29565086&download=1.

[18] Letter from The Honorable I. Charles McCullough, III, Inspector General of the Intelligence Cmty., to Senators Ron Wyden and Mark Udall (June 15, 2012), *available at* https://www.wyden.senate.gov/download/?id=E5DEF293-A8D6-4014-A23A-909C82A3C510&download=1.

[19] Letter from Brennan Ctr. for Justice, et. al, to James Clapper, Dir. Nat'l Intelligence (Oct. 29, 2015), *available at* https://www.brennancenter.org/sites/default/files/analysis/Coalition_Letter_DNI_Clapper_102915.pdf.

[20] Letter from Rep. John Conyers, Jr., et. al, to James Clapper, Dir. Nat'l Intelligence (Apr. 22, 2016), *available at* https://www.brennancenter.org/sites/default/files/legal-work/Letter_to_Director_Clapper_4_22.pdf.

memorialize their understanding, in light of interim conversations and briefings, that the DNI would provide the requested estimate "early enough to inform the debate," and with a target date of January 2017.[21] By all private and public accounts, the intelligence community was close to launching its count at the beginning of this year.

It appears, however, that the government is now backing down from this commitment. In recent testimony, DNI Dan Coats suggested that it was technologically infeasible to generate an estimate without invading Americans' privacy – the very same claim that was addressed and seemingly resolved under the previous administration.[22] In short, the government is retreating to its 2012 assertion that there is no automated way to assess whether a particular communication is to or from an American.

The problem with this claim is that the NSA can, and routinely does, make such an assessment when it conducts upstream surveillance. The FISA Court has held that the Constitution requires the government to take certain concrete steps to minimize the acquisition, retention, and searching of wholly domestic communications. One of these steps, as the Privacy and Civil Liberties Board reported in 2014, is the NSA's use of IP addresses and "comparable technical means" to automatically filter out domestic communications when conducting upstream surveillance of Internet transactions.[23] Both the NSA and the FISA Court consider this method of identifying the domestic-versus-foreign status of communicants sufficient for purposes of complying with the Constitution. If it is sufficient for that purpose, it is certainly adequate to give Congress and the public a rough sense of how Section 702 collection impacts Americans.

In addition, there should be no difficulty in generating an estimate of how many Americans' telephone calls are collected: the government can simply use the country code as a proxy. The method is not perfect – a cell phone's country code does not always correspond with the location or nationality of the user – but again, lawmakers are seeking a rough estimate, not an exact count.

Stored e-mails, obtained through the PRISM program, are admittedly a harder case, and it is possible that some research would be required to ascertain the status of the communicants. The privacy community is nonetheless unanimous in its conclusion that the NSA should perform a one-time limited sampling of e-mails, under conditions (such as the immediate deletion of the communications after review) that would minimize the privacy intrusion.[24] Such a sampling would certainly be feasible: the NSA conducted a similar exercise in 2011 when the FISA Court ordered it to ascertain how many wholly domestic communications were captured in upstream

---

[21] *See* Press Release, U.S. House Comm. on the Judiciary Democrats, Bipartisan House Coalition Presses Clapper for Information on Phone & Email Surveillance (Dec. 16, 2016), *available at* https://democrats-judiciary.house.gov/news/press-releases/bipartisan-house-coalition-presses-clapper-information-phone-email-surveillance.

[22] Dustin Volz, *NSA Backtracks On Sharing Number of Americans Caught in Warrant-less Spying*, REUTERS, June 12, 2017, http://www.reuters.com/article/us-usa-intelligence-idUSKBN19031B.

[23] *See* PCLOB 702 REPORT, *supra* note 6, at 38.

[24] *See* Letter from Brennan Ctr. for Justice, et. al, to James Clapper, *supra* note 19.

surveillance.[25] Given the privacy community's overwhelming support for such an endeavor, the DNI's reliance on privacy concerns rings hollow.

Finally, if the government is truly incapable of ascertaining, even roughly, how many Americans' communications it is collecting, that fact is in itself alarming. Regardless of whether it is lawful, the "incidental" collection of Americans' communications has real and significant effects on privacy – particularly when (as discussed below) that information can be stored for years, searched, and used in legal proceedings. The government cannot simultaneously assure the public that the impact of Section 702 surveillance on Americans' privacy is minimal, while also maintaining that it has no idea – and no way to discover – how many Americans' communications it is acquiring and storing.

B. Minimization and Its Loopholes

Minimization procedures are intended to mitigate the effects of "incidental" collection. The concept behind minimization is fairly simple: The interception of Americans' communications when targeting foreigners is inevitable, but because such interception would otherwise require a warrant or individual FISA order, incidentally collected U.S. person information generally should not be kept, shared, or used, subject to narrow exceptions.

The statutory language, however, is much more complex. It requires the government to adopt minimization procedures, which it defines as procedures "that are reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[26] The statute also prohibits disseminating non-foreign intelligence information in a way that identifies U.S. persons unless their identity is necessary to understand foreign intelligence information or assess its importance. The one caveat is that the procedures must "allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes."[27]

The lack of specificity in this definition, and the tension between its general rule and its caveat, has allowed the government to craft rules that are permissive and contain multiple exceptions. To begin with, the NSA may share raw data from its PRISM collection with the FBI, the CIA, and (as of April 2017) the National Counterterrorism Center (NCTC).[28] All four agencies generally may keep unreviewed raw data – including data about U.S. persons – for five

[25] [Redacted], 2011 WL 10945618, at *11-12 nn. 30, 31, 39 (FISA Ct. Oct. 3, 2011).
[26] 50 U.S.C. § 1801(h)(1).
[27] 50 U.S.C. § 1801(h)(3).
[28] LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 6(c) (2016) [hereinafter NSA 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/icotr/51117/2016-NSA-702-Minimization-Procedures_Mar_30_17.pdf.

years after the certification expires;[29] they also can seek extensions from a high-level official,[30] and the 5-year limit does not apply to encrypted communications (which are becoming increasingly common among ordinary users of mobile devices) or communications "reasonably believed to contain secret meaning."[31] The agencies may keep indefinitely any U.S. person information that has foreign intelligence value or is evidence of a crime.[32]

If the NSA discovers U.S. person data that has no foreign intelligence value and contains no evidence of a crime, the agency is supposed to purge the data.[33] The NSA, however, interprets this requirement to apply only if the NSA analyst determines "not only that a communication is not currently of foreign intelligence value to him or her, but also would not be of foreign intelligence value to any other present or future foreign intelligence need."[34] This is an impossibly high bar, and so, "in practice, this requirement rarely results in actual purging of data."[35]

The FBI, CIA, and NCTC have no affirmative requirement to purge irrelevant U.S. person data on detection, relying instead on age-off requirements. Moreover, if the FBI reviews U.S. person information and makes *no determination* regarding whether it is foreign intelligence information or evidence of a crime, the 5-year limit evaporates, and the FBI may keep the data for a longer period of time that remains classified.[36] If the NCTC reviews U.S. person

---

[29] *Id.* at § 3(c)(1) (2016) (although the retention period for communications obtained through upstream collection is two years, as specified in section 3(c)(2)); LORETTA LYNCH, U.S. DEP'T OF JUSTICE, 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 § III.G.1.a (2016) [hereinafter FBI 702 MINIMIZATION PROCEDURES], *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; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE CENTRAL INTELLIGENCE AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § 2 (2016) [hereinafter CIA 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/icotr/51117/2016_CIA_Section_702_Minimization_Procedures_Se_26_2016.pdf; LORETTA LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED § B(2)(a) (2016) [hereinafter NCTC 702 MINIMIZATION PROCEDURES], *available at* https://www.dni.gov/files/documents/icotr/51117/2016_NCTC_Section_702_Minimizatio_Procedures_Sep_26_2016.pdf.

[30] PCLOB 702 REPORT, *supra* note 6, at 60; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B(2)(a).

[31] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 6(a)(1)(a); CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 3.c.

[32] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 6(a); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.G; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 3.a, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § B(3).

[33] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at §§ 3(b)(1), 3(c).

[34] PCLOB 702 REPORT, *supra* note 6, at 62.

[35] *Id.*

[36] FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.G.1.b.

information and makes no determination as to its status, it can keep the information for 15 years.[37]

If any of the four agencies – all of which have access to raw data – disseminate information to other agencies, they must first obscure the identity of the U.S. person; but once again, there are several exceptions to this rule. For instance, the agencies need not obscure the U.S. person's identity if it is necessary to understand or assess foreign intelligence or if the communication contains evidence of a crime.[38]

In short, the NSA routinely shares raw Section 702 data with the FBI, CIA, and NCTC; and the agencies' minimization procedures suggest that U.S. person information is almost always kept for at least five years and, in many circumstances, much longer. The sharing and retention of U.S. person information are not unrestricted, but it is a stretch to say that they are "minimized" under any common sense understanding of the term.

C. Back Door Searches

Perhaps the most problematic aspect of the minimization procedures is that they allow all four agencies to query Section 702 data using U.S. person identifiers, with the express goal of retrieving and analyzing Americans' communications.[39]

If the government wishes to obtain an American's communications for foreign intelligence purposes, it must secure an individual court order from the FISA Court after demonstrating that the target is an agent of a foreign power. If the government wishes to obtain an American's communications for law enforcement purposes, it must get a warrant from a neutral magistrate. To ensure that Section 702 is not used to avoid these requirements, the statute contains a prohibition on "reverse targeting" – i.e., targeting a foreigner overseas when the government's intent is to target "a particular, known person reasonably believed to be in the United States." Before conducting Section 702 surveillance, the government must certify that it does *not* intend to target particular, known Americans.

And yet, immediately upon obtaining the data, all four agencies may sort through it looking for the communications of particular, known Americans – the very people in whom the government just disclaimed any interest. Worse, even though the FBI would be required to obtain a warrant in order to access Americans' communications absent a significant foreign intelligence purpose, the FBI may – and, "with some frequency,"[40] does – search the Section 702 data for Americans' communications to use in criminal proceedings having no foreign

---

[37] [Redacted], No. [Redacted] at 40 (FISA Ct. Apr. 26, 2017), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[38] FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § V.A-B; NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 6(b); CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at §§ 5, 7.d; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § D(1)-(2).
[39] NSA 702 MINIMIZATION PROCEDURES, *supra* note 28, at § 3(b)(5); FBI 702 MINIMIZATION PROCEDURES, *supra* note 29, at § III.D; CIA 702 MINIMIZATION PROCEDURES, *supra* note 29, at § 4; NCTC 702 MINIMIZATION PROCEDURES, *supra* note 29, at § C(1).
[40] PCLOB 702 REPORT, *supra* note 6, at 59.

intelligence dimensions whatsoever.[41] This is a bait and switch that is utterly inconsistent with the spirit, if not the letter, of the prohibition on reverse targeting. It also creates a massive end run around the Fourth Amendment's warrant requirement.

Some have defended these "back door searches," claiming that as long as information is lawfully acquired, agencies may use the information for any legitimate government purpose. This argument ignores Congress's command to agencies to "minimize" information about U.S. persons. The very meaning of "minimization" is that agencies may *not* use the information for any purpose they wish. Minimization is a constitutional requirement as well as a statutory one: as Judge Bates of the FISA Court has observed, "[T]he procedures governing retention, use, and dissemination bear on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information."[42]

Indeed, restrictions on searches of lawfully obtained data are the constitutional norm, not the exception. In executing warrants to search computers, the government routinely seizes and/or copies entire hard drives. However, agents may only conduct searches reasonably designed to retrieve those documents or files containing the evidence specified in the warrant.[43] Moreover, if a different agency wishes to search the seized data for a different purpose, it must obtain a separate warrant for that search.[44] The fact that the government lawfully obtained and is in possession of the computer's contents does not give it license to conduct any search it wishes; that would violate the terms on which the government obtained the computer's contents in the first place.

The same principle holds true in the analog world. When the police obtain a warrant to search a house for a murder weapon, they may enter the house and, in appropriate cases, search every room. But after they find (or fail to find) the murder weapon, they are not allowed to continue searching for other items they may have some interest in, simply because they are now in the house. Their entrance into the house was legal, but that does not entitle them to search for anything inside it. That would be exceeding the terms accompanying their initial access to the house.

---

[41] ROBERT S. LITT, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, PRIVACY, TECHNOLOGY AND NATIONAL SECURITY: AN OVERVIEW OF INTELLIGENCE COLLECTION (July 18, 2013), https://www.dni.gov/index.php/newsroom/speeches-and-interviews/195-speeches-interviews-2013/896-privacy,-technology-and-national-security-an-overview-of-intelligence-collection.

[42] [Redacted], 2011 WL 10945618, at *27 (FISA Ct. Oct. 3, 2011). In cases involving the foreign intelligence exception to the warrant requirement, the reasonableness of a surveillance scheme turns on weighing the government's national security interest against the privacy intrusion. While the surveillance scheme should be evaluated as a whole, it is difficult to see how any scheme could pass the reasonableness test if a significant component of the scheme were not justified by any national security interest. This is one of several errors, in my view, in the FISA Court's 2015 decision upholding the constitutionality of back door searches. *See* Elizabeth Goitein, *The FBI's Warrantless Surveillance Back Door Just Opened a Little Wider*, JUST SEC. (Apr. 21, 2016), https://www.justsecurity.org/30699/fbis-warrantless-surveillance-door-opened-wider/.

[43] *See, e.g.*, United States v. Ganias, 755 F.3d 125 (2nd Cir. 2014), *rev'd en banc on other grounds*, 824 F.3d 199 (2nd Cir. 2016).

[44] *See* United States v. Hulscher, 2017 WL 657436 (D.S.D. February 17, 2017).

Under Section 702, the terms on which the government is authorized to collect data *without* a warrant include a limitation on whom the government may target – i.e., the government may only target foreigners overseas. To obtain access to the data on those terms and then search for Americans' data is the equivalent of seizing a computer to search for child pornography and then searching for evidence of tax fraud, or obtaining access to a house to search for a murder weapon and then conducting a search for drugs.

Back door searches are not rare occurrences. In 2016, the NSA and CIA – agencies that are have limited jurisdiction within the United States – performed U.S. person queries of communications *content* on 5,288 occasions.[45] The NSA further conducted U.S. person queries of communications *metadata* 30,355 times (the CIA does not report this data).[46] The FBI, however, is by far the most prolific user of back door searches. Although the FBI is exempt from the statutory requirement to report U.S. person query statistics, the Privacy and Civil Liberties Oversight Board (PCLOB) has reported that the FBI searches databases containing 702 data "whenever [i]t opens a new national security investigation or assessment," and conducts similar searches "with some frequency" when performing "criminal investigations and assessments that are unrelated to national security efforts."[47]

The government has attempted to downplay the effect on Americans' privacy, asserting that back door searches rarely return information in non-national security cases. In November 2015, the FISA Court ordered the FBI to report on "[e]ach instance in which FBI personnel received and reviewed Section 702-acquired information that the FBI identified as concerning a U.S. person in response to a query that was designed to return evidence of a crime unrelated to foreign intelligence."[48] The FBI reported only one such instance in 2016.[49]

But this number is almost certainly misleading. For one thing, the FBI has long claimed that it cannot ascertain how many back door searches it conducts because it often does not know, or attempt to learn, the U.S. person status of the subjects of its queries. If that is the case, limiting the reporting to cases in which the information has been affirmatively "identified as concerning a U.S. person" will result in an undercount. At a more basic level, limiting the reporting to queries "unrelated to foreign intelligence" ignores the fact that the government ordinarily must obtain an individualized order from the FISA Court in order to access Americans' communications in foreign intelligence investigations. That requirement is being circumvented in an untold number of cases.

Compounding the constitutional harm of back door searches, the government has not fully and consistently complied with its statutory and constitutional obligation to notify criminal defendants when it uses evidence "obtained or derived from" Section 702 surveillance. Before 2013, the government interpreted "obtained or derived from" so narrowly that it notified no one.

---

[45] *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT, *supra* note 16, at 8.
[46] *Id.* at 9.
[47] PCLOB 702 REPORT, *supra* note 6, at 59.
[48] OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT, *supra* note 16, at 10.
[49] *Id.*

In the four years since the government's approach reportedly changed,[50] the government has provided notification in only eight known cases, even though the PCLOB reports that the FBI searches Section 702 every time it conducts a national security investigation and there have been several hundred terrorism and national security convictions during this time.[51]

There is reason for concern that the government is avoiding its notification requirements by engaging in "parallel construction" – i.e., recreating the Section 702 evidence using less controversial means.[52] Attorneys have asked the Department of Justice to share its policies for determining when information is considered to be "derived from" Section 702, but the Department refuses to provide them.

Importantly, opposition to warrantless searches for U.S. person information is not a call to re-build the barriers to cooperation among agencies often attributed to "the wall." Threat information, including threat information that focuses on U.S. persons, can and should be shared among agencies when identified, and the agencies should work together as necessary in addressing the threat. What the Fourth Amendment cannot tolerate is the government collecting information without a warrant with the intent of mining it for use in ordinary criminal cases against Americans. That is why President Obama's Review Group on Intelligence and Communications Technologies – a five-person panel including a former acting director of the CIA (Michael J. Morell) and chief counterterrorism advisor to President George W. Bush (Richard A. Clarke) – unanimously recommended closing the "back door search" loophole by prohibiting searches for Americans' communications without a warrant.[53]

III. Risks and Harms of Mass Data Collection

The mass collection and storage of communications that include sensitive information about Americans carries with it significant risks and harms, which must be considered in evaluating what the appropriate scope of surveillance should be.

A. Risk of Abuse or Mishandling of Data

The substantive legal restrictions on collecting information about Americans are looser than they have been since before 1978. At the same time, the amount of data available to the government and the capacity to store and analyze that data are orders of magnitude greater than

---

[50] For more background, see Patrick C. Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance — Again?*, JUST SEC. (Dec. 11, 2015), https://www.justsecurity.org/28256/arent-criminal-defendants-notice-section-702-surveillance-again.

[51] DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2015 at 14; DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2014 at 12; DEP'T OF JUSTICE, UNITED STATES ATTORNEYS' ANNUAL STATISTICAL REPORT FISCAL YEAR 2013 at 60.

[52] *See* Toomey, *supra* note 50; John Shiffman and Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013, 3:25 PM), http://www.reuters.com/article/us-dea-sod-idUSBRE97409R20130805#X7BeCQSb0GrEDTJX.97.

[53] *See* PRESIDENT'S REVIEW GRP. ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD 29 (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

they were during the period of J. Edgar Hoover's worst excesses. History teaches us that this combination is an extraordinarily dangerous one.

To date, there is only limited evidence of intentional abuse of foreign intelligence surveillance authorities.[54] There have, however, been multiple significant instances of non-compliance by the NSA with FISA Court orders. Notably, these include cases in which the NSA did not detect the non-compliance for years, and the agency's overseers had no way to uncover the incidents in the meantime. Given that these incidents went unreported for years even when the agency was *not* trying to conceal them, it is not clear how overseers would learn about intentional abuses that agency officials were making every effort to hide.

Moreover, the fact that little evidence of intentional abuse has emerged to date is not a cause for complacency. Government insiders have made reference to a "culture of compliance" and professionalism that emerged in the decades following the Church Committee's investigation.[55] But organizational cultures change, and are highly influenced by leadership. There is simply no guarantee that the degree of institutional self-restraint exercised in the past will continue indefinitely.

In this vein, it is significant that some intelligence experts who until recently defended the wide discretion permitted by Section 702 have seemingly revisited their conclusions in light of today's tumultuous and uncertain political landscape. Matthew Olsen, who served as NSA General Counsel and the Director of the National Counterterrorism Center, was a strong supporter of the FISA Amendments Act when it was being debated in 2008 and has often testified on its behalf.[56] At a recent public conference, however, he stated: "I fought hard . . . for increasing information sharing… [and] for the modernization of FISA. . . . As I fought for these changes, I did not bargain on [the current political environment]. That was beyond my ability to imagine . . . [T]his is a time of . . . soul-searching for me."[57]

In any event, inadvertent failures to adhere to privacy protections are a concern in their own right. On multiple occasions in the past decade, the FISA Court has had occasion to rebuke the NSA for repeated, significant, and sometimes systemic failures to comply with court orders. These failures took place under multiple foreign intelligence collection authorities (including Section 702) and at all points of the programs: collection, dissemination, and retention. It is

---

[54] *See, e.g.*, Letter from Dr. George Ellard, Inspector Gen., Nat'l Sec. Agency, to Sen. Charles E. Grassley (Sept. 11, 2013), *available at* http://www.privacylives.com/wp-content/uploads/2013/09/09262013-NSA-Surveillance-09-11-13-response-from-IG-to-intentional-misuse-of-NSA-authority.pdf (detailing 12 instances of intentional abuse of NSA bulk surveillance data, most involving employees searching for information on their romantic partners).

[55] See Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO.WASH. L. REV. 1306, 1326 n.135 (2004).

[56] *See, e.g., Oversight and Reauthorization of the FISA Amendments Act: The Balance between National Security, Privacy, and Civil Liberties: Hearing Before the S. Comm. on the Judiciary*, 114th Cong. (2016) (statement of Matthew G. Olsen, Former Director, National Counterterrorism Center) [hereinafter Olsen Statement].

[57] *Intelligence Under a Trump Administration*, Panel Discussion at 2016 Cato Surveillance Conference, CATO INSTITUTE, at 47:20 (Dec. 14, 2016), https://www.cato.org/multimedia/events/2016-cato-surveillance-conference-panel-intelligence-under-trump-administration.

instructive to review some of the Court's comments in these cases. The following statements are excerpted from five opinions spanning the years 2009 through 2017:

- "In summary, since January 15, 2009, it has finally come to light that the FISC's authorizations of this vast [Section 215 telephony metadata] collection program have been premised on a flawed depiction of how the NSA uses [the] metadata. This misperception by the FISC existed from the inception its authorized collection in May 2006, buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime. The minimization procedures proposed by the government in each successive application and approved and adopted as binding by the orders of the FISC have been so frequently and systemically violated that it can fairly be said that this critical element of the overall [bulk collection] regime has never functioned effectively."[58]
- "The government has compounded its non-compliance with the Court's orders by repeatedly submitting inaccurate descriptions . . . to the FISC."[59]
- "[T]he NSA continues to uncover examples of systematic noncompliance."[60]
- "Under these circumstances, no one inside or outside of the NSA can represent with adequate certainty whether the NSA is complying with those procedures."[61]
- "[U]ntil this end-to-end review is completed, the Court sees little reason to believe that the most recent discovery of a systemic, ongoing violation . . . will be the last."[62]
- "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[63]
- "The current application [for pen register/trap and trace data] . . . raises issues that are closely related to serious compliance problems that have characterized the government's implementation of prior FISA orders."[64]
- "As far as can be ascertained, the requirement was simply ignored."[65]
- "Notwithstanding this and many similar prior representations, there in fact had been systematic overcollection since [redacted]. . . . This overcollection . . . had occurred continuously since the initial authorization . . . ."[66]
- "The government has provided no comprehensive explanation of how so substantial an overcollection occurred."[67]
- "[G]iven the duration of this problem, the oversight measures ostensibly taken since [redacted] to detect overcollection, and the extraordinary fact that the NSA's end-to-end

[58] *In re* Production of Tangible Things from [Redacted], No. BR 08-13, at 10-11 (FISA Ct. Mar. 2, 2009).
[59] *Id.* at 6.
[60] *Id.* at 10.
[61] *Id.* at 15.
[62] *Id.* at 16.
[63] [Redacted], 2011 WL 10945618, at *5 n. 14 (FISA Ct. Oct. 3, 2011).
[64] [Redacted], Docket No. PR/TT [Redacted], at 4 (FISA Ct. [Redacted]) *available at* https://www.dni.gov/files/documents/1118/CLEANEDPRTT%202.pdf.
[65] *Id.* at 19.
[66] *Id.* at 20.
[67] *Id.* at 21.

review overlooked unauthorized acquisitions that were documented in virtually every record of what was acquired, it must be added that those responsible for conducting oversight at NSA failed to do so effectively."[68]

- "The history of material misstatements in prior applications and non-compliance with prior orders gives the Court pause before approving such an expanded collection. The government's poor track record with bulk PR/TT acquisition…presents threshold concerns about whether implementation will conform with, or exceed, what the government represents and the Court may approve."[69]
- "As noted above, NSA's record of compliance with these rules has been poor. Most notably, NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained… The government has provided no meaningful explanation why these violations occurred, but it seems likely that widespread ignorance of the rules was a contributing factor."[70]
- "Given NSA's longstanding and pervasive violations of the prior orders in this matter, the Court believes that it would be acting well within its discretion in precluding the government from accessing or using such information."[71]
- "[The] cases in which the FBI had not established the required review teams seemed to represent a potentially significant rate of non-compliance."[72]
- "The Court was extremely concerned about these additional instances of non-compliance."[73]
- "Perhaps more disturbing and disappointing than the NSA's failure to purge this information for more than four years, was the government's failure to convey to the Court explicitly during that time that the NSA was continuing to retain this information . . . ."[74]
- "The Court did not find entirely satisfactory the government's explanations of the scope of [its] segregation errors and the adequacy of its response to them . . . ."[75]
- "[A] non-compliance rate of 85% raises substantial questions about the appropriateness of using [a redacted tool] to query FISA data."[76]
- "At the October 26, 2016 hearing, the Court ascribed the government's failure to disclose those [Inspector General] and [NSA Office of Compliance for Operations] reviews at the October 4, 2016 hearing to an institutional lack of candor on NSA's part and emphasized that this is a very serious Fourth Amendment issue."[77]

---

[68] *Id.* at 22.
[69] *Id.* at 77.
[70] *Id.* at 95.
[71] *Id.* at 115.
[72] [Redacted], at 48-49 (FISA Ct. Nov. 6, 2015), *available at* www.dni.gov%2Ffiles%2Fdocuments%2F20151106-702Mem_Opinion_Order_for_Public_Release.pdf&t=MDM3MGZmYjY1ZWQ5YjUyMTQ5ZjQ1ZTA0ZDExNjY2NWU0ZTE1ZWJlNSxaRjRxYlRaQg%3D%3D.
[73] *Id.* at 50.
[74] *Id.* at 58.
[75] [Redacted], No. [Redacted] at 80 (FISA Ct. Apr. 26, 2017), *available at* https://www.dni.gov/files/documents/icotr/51117/2016_Cert_FISC_Memo_Opin_Order_Apr_2017.pdf.
[76] *Id.* at 82.
[77] *Id*. at 19 (internal quotation marks omitted).

The most notable recent compliance failure, discussed in the FISA Court's April 26, 2017 opinion, is the NSA's widespread use of U.S. person identifiers to query certain data obtained through upstream collection. The FISA Court had prohibited such queries in 2011, in response to its discovery that the NSA had for years been pulling in substantial numbers of wholly domestic communications by virtue of "about" collection. The Court had found the NSA's handling of this data unconstitutional, and the ban on U.S. person queries of upstream data was one of the key remedies adopted to cure the constitutional defect.

In January 2016, however, the NSA Inspector General reported internally that agency analysts were not fully complying with this limitation, based on an examination of three months of audit data from early 2015. The Inspector General and the NSA's Office of Compliance for Operations began studies of other time periods, and "preliminary results [suggested] the problem was widespread during all periods under review."[78] In other words, at no point during the operation of upstream collection – either in the years before the NSA informed the Court that it was sweeping in wholly domestic communications, or in the subsequent years when this data was supposedly off limits to U.S. person queries – had this surveillance operated within the bounds of the Constitution.

Nonetheless, the NSA waited for several months before informing the FISA Court of the problem, which it blamed on "human error" and "system design issues."[79] The Court chided the government for this "institutional lack of candor."[80] It granted short-term extensions of Section 702 surveillance authority while the government attempted to resolve the issue, but as of late January 2017, "[t]he government still had not ascertained the full range of systems that might have been used to conduct improper U.S.-person queries,"[81] and as of March, "continued to . . . investigate potential root causes of non-compliant querying practices."[82] With no resolution in sight, and with the Court unwilling to certify the program for another year while the problem remained, the NSA made the only possible choice: to halt "about" collection for the time being.

The Court's April 2017 opinion also includes a long list of other compliance failures. For instance, between November 2015 and May 2016, no less than *85 percent* of queries using identifiers of U.S. persons targeted under Sections 704 and 705(b) resulted in improper querying of Section 702 data.[83] The Court also found that the FBI had shared raw Section 702 information with a redacted entity "largely staffed by private contractors," and that "the [redacted] contractors had access to raw FISA information that went well beyond what was necessary" to perform their jobs.[84] And the Court noted that "[r]ecent disclosures regarding [redacted] systems maintained by the FBI suggest that raw FISA information, including Section 702 information,

[78] *Id.* at 19.
[79] *Id.* at 20.
[80] *Id.* at 19.
[81] *Id.* at 21.
[82] *Id.* at 23.
[83] *Id.* at 82.
[84] *Id.* at 84.

may be retained on those systems in violation of applicable minimization requirements," resulting in "indefinite retention" of some data.[85]

It is unclear whether these failures are occurring because the NSA is not putting sufficient effort into compliance, because the NSA lacks the technical capability to ensure compliance, or for some other reason. It may be the case that Section 702 collection has become so massive in scope, and the systems for retaining and processing the data so technically complex, that it is simply impossible to achieve consistent compliance with the rules governing its use. Whatever the explanation, the fact that the agency's many failures to honor privacy protections were inadvertent is of limited comfort when the NSA is asking Congress and the American public to entrust it with extensive amounts of private data.

B. Chilling Effect

When Americans are aware that intelligence agencies are collecting large amounts of their data (and not just the data of suspected criminals and terrorists), it creates a measurable chilling effect on free expression and communication. After Edward Snowden's revelations in June 2013, an analysis of Google Trends data showed a significant five percent drop in U.S.-based searches for government-sensitive terms (e.g., "dirty bomb" or "CIA"). A control list of popular search terms or other types of sensitive terms (such as "abortion") did not show the same change.[86] In 2013, PEN America surveyed 528 American writers to learn how the disclosures affected their behavior. Twenty-eight percent reported curtailing social media activities; 24 percent avoided certain topics by phone or email; 16 percent chose not to write or speak on a certain topic; and 16 percent avoided Internet searches or website visits on controversial or suspicious topics.[87] These kinds of self-censorship are inimical to the robust exchange of ideas necessary for a healthy democracy.

The impact of overbroad surveillance has been particularly acute in Muslim American communities. According to one study, after the Associated Press reported on the New York City Police Department's surveillance activities, Muslims reported a decline in mosque attendance and Muslim Student Association participation, as well as a marked reticence to speak about political matters in public places or to welcome newcomers into the community.[88] Fear of surveillance, and the possibility that religious or political discussions could be misconstrued or misunderstood, has measurably impeded these communities' ability to freely practice their faith or even to participate fully in civic life.

---

[85] *Id.* at 87-89.
[86] Alex Marthews & Catherine Tucker, *Government Surveillance and Internet Search Behavior* (Apr. 29, 2015), *available at* http://dx.doi.org/10.2139/ssrn.2412564.
[87] Lee Rainie & Mary Madden, *Americans' Privacy Strategies Post-Snowden*, PEW RESEARCH CTR. (Mar. 16, 2015), http://www.pewinternet.org/2015/03/16/americans-privacy-strategies-post-snowden/.
[88] *See generally* MUSLIM AMERICAN CIVIL LIBERTIES COALITION (MACLC) ET AL., MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS (2013), *available at* http://www.law.cuny.edu/academics/clinics/immigration/clear/Mapping-Muslims.pdf.

C. Risk of Data Theft

Any massive government database containing sensitive information about Americans also raises concerns about data theft. The disastrous 2015 attack on the Office of Personnel Management's database, in which personal data concerning more than 21 million current and former federal employees was stolen (ostensibly by the Chinese government), illustrated how vulnerable government databases are.[89] A few months later, hackers published contact information for 20,000 FBI employees and 10,000 Department of Homeland Security employees that they may have obtained by hacking into a Department of Justice database.[90] The intelligence community's data systems are not immune from being compromised, as evidenced by the theft of the NSA's top-secret hacking tools in 2016,[91] followed by WikiLeaks' publication of the CIA's hacking tools earlier this year.[92]

The broad scope of Section 702 data, and the possibility that it could include a wealth of valuable foreign intelligence information, makes it an attractive target for hacking or data theft. Its inclusion of large amounts of information about presumptively innocent Americans significantly increases the harm that would be caused by such an event.

D. Economic Consequences

Another important concern is the negative impact of Section 702 collection on the U.S. technology industry. After Snowden's disclosures revealed the extent of NSA collection, American technology companies reported declining sales overseas and lost business opportunities. In a survey of 300 British and Canadian businesses, 25 percent of respondents indicated they were moving their data outside of the U.S.[93] An August 2013 study by the Information Technology and Innovation Foundation estimated that the revelations could cost the American cloud computing industry $22 to $35 billion over the coming years, representing a 10-20% loss of the foreign market share to European or Asian competitors.[94] Another analyst found this estimate to be low, and predicted a loss to U.S. companies as high as $180 billion.[95]

---

[89] Kaveh Waddell & Dustin Volz, *OPM Announces More Than 21 Million Victims Affected by Second Data Breach*, ATLANTIC (July 9, 2015), http://www.theatlantic.com/politics/archive/2015/07/opm-announces-more-than-21-million-affected-by-second-data-breach/458475/.

[90] Mary Kay Mallonnee, *Hackers Publish Contact Info of 20,000 FBI Employees*, CNN (Feb. 8, 2016), http://www.cnn.com/2016/02/08/politics/hackers-fbi-employee-info/.

[91] *See* Scott Shane, Matt Apuzzo, & Jo Becker, *Trove of Stolen Data Is Said to Include Top-Secret U.S. Hacking Tools*, N.Y. TIMES, Oct. 19, 2016, *available at* https://www.nytimes.com/2016/10/20/us/harold-martin-nsa.html.

[92] *See* Scott Shane, Matthew Rosenberg, & Andrew W. Lehren, *Wikileaks Releases Trove of Alleged C.I.A. Hacking Documents*, N.Y. TIMES, Mar. 7, 2017, *available at* https://www.nytimes.com/2017/03/07/world/europe/wikileaks-cia-hacking.html.

[93] DANIELLE KEHL, ET. AL, OPEN TECHNOLOGY INSTITUTE, SURVEILLANCE COSTS: THE NSA'S IMPACT ON THE ECONOMY, INTERNET FREEDOM & CYBERSECURITY 8 (2014), https://static.newamerica.org/attachments/534-surveillance-costs-the-nsas-impact-on-the-economy-internet-freedom-cybersecurity/Surveilance_Costs_Final.pdf.

[94] DANIEL CASTRO, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION, "HOW MUCH WILL PRISM COST THE US CLOUD COMPUTING INDUSTRY?" (Aug. 5, 2013), http://www.itif.org/publications/how-much-will-prism-cost-us-cloud-computing-industry.

[95] James Staten, *The Cost of PRISM Will Be Larger Than ITIF Projects*, FORRESTER (Aug. 14, 2013), http://blogs.forrester.com/james_staten/13-08-14-the_cost_of_prism_will_be_larger_than_itif_projects.

The economic news went from bad to worse in late 2015, when the Court of Justice of the European Union (CJEU) invalidated the "Safe Harbor" agreement – a 2000 decision of the European Commission allowing the transfer of personal data from the European Union (EU) to the United States, based on the premise that the U.S. met certain EU-law requirements about the handling of that information. The court held that EU law requires U.S. companies to give the data a level of protection that is essentially equivalent to the protections under EU law, including the Charter of Fundamental Rights of the EU – akin to an EU bill of rights. Under this standard, the court found that the European Commission had failed to ensure that EU citizens' data was sufficiently protected within the U.S. While the court did not make express findings about Section 702, the law unquestionably loomed large in the court's analysis, as the authority it confers is inconsistent with many of the essential rights and principles the court described. For instance, upstream surveillance is clearly implicated by the CJEU's conclusion that "generalized" access to the content of electronic communications compromises the essence of the right to privacy.[96]

Although the U.S. and the European Commission have devised a new arrangement, known as the "Privacy Shield," legal challenges to that agreement are underway[97] – and recent developments have given a boost to these challenges. In particular, some of the protections U.S. officials had cited to assuage concerns about the breadth of Section 702 and other U.S. surveillance programs have been, or may soon be, eroded. The Privacy and Civil Liberties Oversight Board has lost its chairman and three other members, and is effectively dormant. A recent executive order issued by President Trump removes Privacy Act protections for foreigners. The current CIA director previously proposed revoking a directive issued by President Obama that extended some protections to foreigners' data obtained under foreign intelligence programs.[98]

In the absence of reforms to Section 702 and other surveillance authorities, it appears likely that the Privacy Shield will ultimately be invalidated by the CJEU or potentially even by the European Commission itself (which can suspend the arrangement unilaterally). Experts believe this would deal a massive economic blow to U.S. companies and could undermine the very structure of the Internet, which requires free data flow across borders. In the meantime, the legal limbo in which U.S. companies find themselves constrains their ability to pursue business opportunities in Europe. That is why over 30 leading technology companies, including

---

[96] *See* Case C-362/14, Schrems v. Data Protection Commissioner, ECLI:EU:C:2015:650 (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en; *see also* Sarah St. Vincent, *Making Privacy a Reality: The Safe Harbor Judgment and Its Consequences for US Surveillance*, CTR. FOR DEMOCRACY & TECH. (Oct. 26, 2015), https://cdt.org/blog/making-privacy-a-reality-the-safe-harbor-judgment-and-its-consequences-for-us-surveillance-reform/ (describing the relationship between the CJEU's holding and Section 702 surveillance).

[97] *See* Reuters, *French Privacy Groups Challenge the EU's Personal Data Pact with U.S.*, FORTUNE (Nov. 2, 2016), http://fortune.com/2016/11/02/privacy-shield-pact-challenge/.

[98] *See* Letter from Fanny Hidvégi, European Policy Manager, & Amie Stepanovich, U.S. Policy Manager, Access Now, for Vera Jourová, Commissioner, European Commission, & Claude Moraes, Member, European Parliament, re: Impact of new U.S. policies and regulatory frameworks on the privacy rights of users in Europe (Feb. 8, 2017), *available at* https://www.accessnow.org/cms/assets/uploads/2017/02/Letter-to-Jourova.pdf.

Microsoft, Google, and Facebook, recently signed a letter urging Congress to enact changes to Section 702. The reforms they propose include codifying the current prohibition against "about" collection and narrowing the definition of "foreign intelligence information" under FISA "to reduce the likelihood of collecting information about non-U.S. persons who are not suspected of wrongdoing."[99]

E. Potential National Security Harms

Last but clearly not least, there is a risk to national security in acquiring too much data. While computers can glean relationships and flag anomalies, they cannot replace human analysis, and human beings have limited capacity. When they are presented with an excess of data, real threats can get lost in the noise. This is not merely a theoretical concern. After the intelligence community failed to intercept the so-called "underwear bomber" (the suicide bomber who nearly brought down a plane headed to Detroit on Christmas Day 2009), an official White House review observed that a significant amount of critical information was available to the intelligence agencies but was "embedded in a large volume of other data."[100] Similarly, the independent investigation of the FBI's role in the shootings by U.S. Army Major Nidal Hasan at Fort Hood concluded that the "crushing volume" of information was one of the factors that hampered accurate analysis prior to the attack.[101]

Whatever threat information may exist amidst the 250 million Internet communications acquired yearly under Section 702, there is surely a large amount of chaff. Because this may make it more difficult to find the threats, it is important for lawmakers to examine whether the current scope of Section 702 collection may be too broad from a security standpoint as well as a privacy one.

IV. Constitutional Concerns

In addition to the practical risks and harms discussed above, the warrantless acquisition of millions of Americans' communications presents deep Fourth Amendment concerns.[102] The

---

[99] Letter from Adobe, et. al, to Representative Bob Goodlatte, Chairman, House Judiciary Committee (May 26, 2017), *available at* http://www.ccianet.org/wp-content/uploads/2017/05/702-letter-201705-FINAL.pdf?ct=t(PR_LabMD_Amicus_January_20171_4_2017)&mc_cid=6fb377afc0&mc_eid=5a85186927.

[100] THE WHITE HOUSE, SUMMARY OF THE WHITE HOUSE REVIEW OF THE DECEMBER 25, 2009 ATTEMPTED TERRORIST ATTACK 3, *available at* http://www.whitehouse.gov/sites/default/files/summary_of_wh_review_12-25-09.pdf.

[101] *Lessons from Fort Hood: Improving Our Ability to Connect the Dots: Hearing Before the Subcomm. on Oversight, Investigations, and Mgmt. of the H. Comm. on Homeland Security*, 112th Cong. 2 (2012) (statement of Douglas E. Winter, Deputy Chair, William H. Webster Commission on the Fed. Bureau of Investigation, Counterterrorism Intelligence, and the Events at Fort Hood, Texas on November 5, 2009).

[102] Although a full discussion of this issue is beyond the scope of this testimony, Section 702 surveillance also raises concerns about the privacy and human rights of foreign nationals. While the Fourth Amendment might not apply to these individuals, the right to privacy is a fundamental human right recognized under international law – including treaties, such as the International Covenant on Civil and Political Rights, that the U.S. has signed. In Presidential Policy Directive 28 (PPD-28), President Obama acknowledged that "all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and . . . all persons have legitimate privacy

communications obtained under Section 702, like any e-mails or phone calls, include not only mundane conversations, but the most private and personal confidences, as well as confidential business information and other kinds of privileged exchanges. Since the Supreme Court decided *Katz v. United States* in 1967, the government has been required to obtain a warrant to wiretap Americans' communications.[103] Moreover, in a subsequent case, the Court made clear that this requirement applied in domestic national security cases as well as criminal cases.[104]

A. "Incidental" Collection

The government nonetheless justifies the warrantless collection of international communications under Section 702 on the ground that the targets themselves are foreigners overseas, and the Supreme Court has held (in a different context) that the government does not need a warrant to search the property of a non-U.S. person abroad.[105] Although the communications obtained under Section 702 sometimes involve both foreigners and Americans, the FISA Court, along with federal courts in two circuits,[106] have held that the authority to conduct warrantless surveillance of the foreign target entails the authority to "incidentally" collect the communications of those in contact with the target.

Outside of Section 702, however, the case law does not support the existence of a right to warrantless "incidental" collection. The courts reviewing Section 702 have relied on a line of cases dating back to the 1970s, sometimes called the "incidental overhear" cases, in which

---

interests in the handling of their personal information." EXEC. OFFICE OF THE PRESIDENT, PRESIDENTIAL POLICY DIRECTIVE/PPD-28 (2014), *available at* http://www.lawfareblog.com/wp-content/uploads/2014/01/2014sigint.mem_.ppd_.rel_.pdf.

PPD-28 requires agencies to extend certain privacy protections to foreign nationals when conducting electronic surveillance. However, the future viability of PPD-28 is uncertain, given that President Trump already has rescinded several of President Obama's orders and CIA Director Mike Pompeo, when he served in Congress, argued that PPD-28 should be revoked. *See* Mike Pompeo & David B. Rivkin Jr., *Time for a Rigorous National Debate About Surveillance*, WALL ST. J. (Jan. 3, 2016), https://www.wsj.com/articles/time-for-a-rigorous-national-debate-about-surveillance-1451856106. Moreover, even if PPD-28 remains in place, it does not prevent the acquisition of information about foreign nationals who pose no threat to the United States.

A particular concern relates to the sharing of Section 702 information with foreign governments. Agencies have significant leeway to engage in such sharing. Although they should have "confidence" that the information "is not likely to be used by the recipient in an unlawful manner or in a manner harmful to U.S. interests," OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, CRITERIA FOR FOREIGN DISCLOSURE AND RELEASE OF CLASSIFIED NATIONAL INTELLIGENCE, ICPG 403.1 § (D)(2) (Mar. 13, 2013), there is no express requirement or mechanism to ensure that governments with poor or spotty human rights records will not use the information to facilitate human rights violations – for instance, to harass or persecute journalists, political dissidents, human rights activists, and other vulnerable groups whose communications may have been caught up in the Section 702 collection. *See* AMOS TOH, FAIZA PATEL & ELIZABETH GOITEIN, BRENNAN CTR. FOR JUSTICE, OVERSEAS SURVEILLANCE IN AN INTERCONNECTED WORLD 28-31 (2016), http://www.brennancenter.org/sites/default/files/publications/Overseas_Surveillance_in_an_Interconnected_World.pdf.

[103] 389 U.S. 347 (1967).

[104] United States v. U.S. Dist. Court for the E. Dist. Of Mich. (*Keith*), 407 U.S. 297 (1972).

[105] *See* United States v. Verdugo-Urquidez, 494 U.S. 259 (1990).

[106] *See* United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016); United States v. Hasbajrami, No. 11-CR-623 (JG), 2016 WL 1029500 (E.D.N.Y. Mar. 8, 2016); *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

defendants challenged Title III wiretap orders on the ground that they did not name everyone whose communications might be recorded. The courts held that a warrant meets the Fourth Amendment's "particularity" requirement as long it specifies the phone line to be tapped and the conversations to be acquired, and if the government takes reasonable steps to avoid recording "innocent" conversations.[107] It is hard to see how these rulings on the criteria for a valid warrant could justify *warrantless* collection of Americans' communications.[108]

If, on the other hand, the courts reviewing Section 702 have correctly interpreted the rule emerging from the "incidental overhear" cases, then applying that rule in the Section 702 context would be a classic case of the law failing to keep up with technology. A blanket rule that no warrant is needed for Americans who are in contact with a lawfully surveilled target might have made sense in the 1970s, when there was almost certainly a warrant for the target himself (given the infrequency of international communication) and when government agents monitored the wiretap in real time so that they could turn off the recording equipment if "innocent conversations" were taking place. That rule does not sufficiently protect Americans' reasonable expectation of privacy in an era where millions of Americans communicate with foreigners overseas on a routine basis, those communications can easily be intercepted in massive amounts without any warrant, and there is no mechanism for "turning off" the collection of "innocent communications." Equating the incidental surveillance that takes place in these materially different contexts is like equating "a ride on horseback" with "a flight to the moon."[109]

B. The Foreign Intelligence Exception

Alternatively, the FISA Court (and, more recently, a district court following its lead[110]) has relied on the "foreign intelligence exception" to the Fourth Amendment's warrant requirement. The Supreme Court has never recognized this exception, and there is significant controversy over its scope. The FISA Court has construed the exception extremely broadly, stating that it applies even if the target is an American and even if the primary purpose of collection has no relation to foreign intelligence.[111]

In the era before FISA, however, several federal courts of appeal had the opportunity to review foreign intelligence surveillance, and they articulated a much narrower version of the

---

[107] *See, e.g.*, United States v. Donovan, 429 U.S. 413 (1977); United States v. Kahn, 415 U.S. 143 (1974); United States v. Figueroa, 757 F.2d 466 (2d Cir. 1985).

[108] *See* Elizabeth Goitein, *The Ninth Circuit's Constitutional Detour in Mohamud*, JUST SEC. (Dec. 8, 2016), https://www.justsecurity.org/35411/ninth-circuits-constitutional-detour-mohamud/. The rulings are particularly inapt because Section 702 minimization procedures present little or no barrier to collection, and the back-end protections on retention and use are significantly weaker than those that apply in the Title III context. *See* Brief for Appellant at Argument I, *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002) (No. 02-001) (noting that "FISA's minimization standards are more generous than those in Title III").

[109] Riley v. California, 134 S. Ct. 2473, 2488 (2014).

[110] United States v. Mohamud, No. 3:10-cr-00475, 2014 WL 2866749 (D. Or. June 24, 2014), *aff'd on other grounds*, 843 F.3d 420 (9th Cir. 2016).

[111] *See, e.g., In re Directives*, 551 F.3d 1004; *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01 (FISA Ct. Sept. 4, 2008).

exception.[112] They held that it applies only if the target is a foreign power or agent thereof, and only if the acquisition of foreign intelligence is the primary purpose of the surveillance. They also emphasized the importance of close judicial scrutiny (albeit after-the-fact) in cases where the target challenges the surveillance. While these cases addressed surveillance activities that differed in many respects from Section 702, it is clear that Section 702 surveillance would not pass constitutional muster under the standards they articulated.

A detailed analysis of the case law is beyond the scope of this testimony, but the Brennan Center's report, *What Went Wrong With the FISA Court*, engages in such an analysis and explains why the foreign intelligence exception does not justify Section 702 surveillance in its current form.[113]

C. The Reasonableness Test

Even if a foreign intelligence exception applied, the surveillance would still have to be "reasonable" under the Fourth Amendment. The "reasonableness" inquiry entails weighing the government's interests against the intrusion on privacy.[114]

In undertaking this analysis, courts generally accept that the government's interest in protecting national security is of the highest order – as it certainly is. But to determine the reasonableness of a surveillance scheme, one must also ask whether it goes further than necessary to accomplish the desired end. For instance, how does it further national security to allow the targeting of foreigners who have no known or suspected affiliation with foreign governments, factions, or terrorist groups? How does it further national security to permit the FBI to search for Americans' communications to use in prosecutions having nothing to do with national security?

Moreover, in assessing the impact on privacy rights, the FISA Court has focused on the protections offered to Americans by minimization procedures.[115] As discussed above, however, these protections fall short in a number of significant respects. On their face, they allow Americans' communications to be retained, disseminated, and used in a wide range of circumstances.

V. Reforming Section 702

There are several reforms that would go far toward mitigating the privacy risks posed by Section 702, while retaining the core functionality of the statute: the ability of the government to conduct warrantless surveillance of foreigners overseas who may pose a threat to the U.S. or its interests. These reforms would also retain the principle that communications between foreigners

---

[112] *See, e.g.*, United States v. Truong Dinh Hung, 629 F.2d 908, 913 (4th Cir. 1980); United States v. Brown, 484 F.2d 418, 426 (5th Cir. 1973); United States v. Butenko, 494 F.2d 593, 604-05 (3rd Cir. 1974) (*en banc*); United States v. Buck, 548 F.2d 871, 875 (9th Cir. 1977).
[113] GOITEIN & PATEL, *supra* note 2, at 11-12, 35-43.
[114] Maryland v. King, 133 S. Ct. 1958, 1970 (2013).
[115] *In re Directives*, 551 F.3d at 1015.

do not fall within FISA even if they happen to transit through or be stored within the U.S. And because they would not affect the government's ability to collect the communications of suspected terrorists, there is no reason to believe that they would compromise Section 702's effectiveness as a counterterrorism tool.

A. Narrowing the Scope of Collection

Congress should narrow the scope of permissible targets. Currently, the government may target anyone reasonably believed to be a foreigner overseas, as long as the purpose of collection is to acquire information "that relates to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States."[116] As discussed above, this language is permissive enough to allow surveillance of innocent conversations between foreigners and Americans about current events. If, in fact, the government does not condone or conduct such broad, non-threat-based surveillance, it should have no objection to statutory changes to codify a more narrow approach.

This could be accomplished through two measures. First, Congress should require the government to have a reasonable belief that the target of surveillance is a foreign power (FP) or an agent of a foreign power (AFP). The statute defines these terms quite broadly to include not only foreign governments or factions, but also private citizens who are suspected of involvement in international terrorism. The FP/AFP determination would be an internal one; it would not have to be submitted to the FISA Court for case-by-case approval or meet a "probable cause" standard. Second, Congress should narrow the permissible purposes of Section 702 surveillance so that it they are limited to protecting the U.S. against (1) actual or potential attacks or other grave hostile acts, including cyberattacks; (2) sabotage, international terrorism, or the international proliferation of weapons of mass destruction; or (3) clandestine intelligence activities.[117] It would not be sufficient that the information sought merely "relates to" the "conduct of foreign affairs."

Limiting the scope of surveillance to those suspected of posing a threat to the U.S. would not undermine the statute's effectiveness. The government has made public several examples of Section 702's importance to its counterterrorism efforts; in each of these examples – including the cases of Najibullah Zazi, Khalid Ouazzani, David Headley, Agron Hasbajrami, and Jamshid Muhtorov – the targets of the Section 702 surveillance were known or suspected to have terrorist affiliations.[118] Intelligence officials have confirmed that this is the norm in cases where Section 702 surveillance has been critical – i.e., that the "typical" such case has involved "narrowly focused surveillance" targeting "a specific foreign individual overseas[,] based on the

---

[116] 50 U.S.C. § 1801(e)(2).
[117] *Cf.* 50 U.S.C. § 1801(e)(1).
[118] *See 2009 Subway Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1543; *2009 New York Stock Exchange Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1542; *2009 Jyllands Posten Plot*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1583; *2011 Agron Hasbajrami*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1616; *2012 Islamic Jihad Union Support Network*, NEW AMERICA, http://securitydata.newamerica.net/extremists/terror-plot.html?id=1575.

government's reasonable belief the individual was involved with terrorist activities."[119] The changes suggested here would not have prevented or limited Section 702 surveillance in those cases.

In addition, Congress should codify the current cessation of "about" collection. This type of surveillance greatly increases the chances of pulling in wholly domestic communications, not to mention other completely innocent communications between people who are not themselves permissible targets of surveillance. Moreover, although "about" collection poses uniquely significant risks to privacy, it is a relatively small part of the upstream program, which itself comprises less than one tenth of Section 702 collection.[120] This is clearly a situation in which the privacy risks outweigh the benefits – a point the NSA effectively acknowledged when it stopped "about" collection in April.[121]

B. Shoring Up Protections for Americans' "Incidentally" Collected Communications

Narrowing the scope of surveillance will reduce the amount of "incidental" collection of Americans' communications that can take place, but it will not and cannot eliminate "incidental" collection altogether. It is thus critical that Congress breathe life into its statutory command to agencies to "minimize" the retention, use, and sharing of Americans' information acquired through Section 702 surveillance.

First, Congress should require all government agencies to obtain a warrant or an individualized FISA Court order before using U.S. person identifiers to query raw Section 702 data. This would close the loophole that currently allows the government to read Americans' e-mails and listen to their phone calls without any factual predicate to suspect wrongdoing, let alone a warrant. What makes the warrantless surveillance lawful in the first instance is the government's certification that it is targeting *only* foreigners. That representation becomes a semantic sleight of hand when the government simultaneously adopts procedures allowing it to search the data for particular Americans' communications.

The FBI has pointed out that its databases contain information from multiple sources, and other agencies may also conduct federated searches that run against multiple data sets. In such cases, there is a simple way to implement a warrant requirement for just the Section 702 data. Such data is specially tagged to enable compliance with notification requirements as well as legal limitations on who may access it. Currently, if an FBI agent performs a query that returns Section 702 data, the agent is notified of its 702 status. The systems could instead be configured not to return Section 702 data at all, unless the agent enters a code certifying that one of two

---

[119] *See* Olsen Statement, *supra* note 56, at 5.
[120] [Redacted], 2011 WL 10945618, at *9 (FISA Ct. Oct. 3, 2011).
[121] *See* Statement, Nat'l Sec. Agency, NSA Stops Certain 702 "Upstream" Activities (Apr. 28, 2017), *available at* https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml ("NSA previously reported that, because of the limits of its current technology, it is unable to completely eliminate 'about' communications from its upstream 702 collection without also excluding some of the relevant communications directly 'to or from' its foreign intelligence targets. That limitation remains even today. Nonetheless, NSA has determined that in light of the factors noted, this change is a responsible and careful approach at this time.").

conditions is met: (1) the query term is associated with someone reasonably believed to be a foreigner overseas, or (2) the government has obtained the required warrant or FISA Court order.

Some have suggested that agencies should be free to run U.S. person queries of Section 702 metadata, with heightened requirements in place only if the agency wishes to review content. Legal scholars and judges, however, have begun to recognize that metadata can be every bit as revealing as content, enabling the government to piece together individuals' beliefs, associations, habits, and other highly sensitive information.[122] Even if one takes the position that metadata is less deserving of protection, the Electronic Communications Privacy Act and Section 215 of the USA PATRIOT Act still require the government to follow certain procedures and to meet certain substantive standards in order to access Americans' telephone and Internet metadata.[123] Allowing unfettered access to metadata collected under Section 702 subverts those requirements, just as allowing the unfettered review of content subverts the requirement of a warrant or FISA Title I order.

Second, Congress should limit the permissible uses of Section 702 data about Americans, even in cases where a warrant is obtained or the government comes across the information without having performed a backdoor search. It is a basic tenet of privacy protection, enshrined in the "widely accepted" Fair Information Practice Principles that are themselves "at the core of the Privacy Act of 1974," that the use of personal information should be limited to the purposes for which it was collected.[124] This principle has even more force when the government could not legally have collected the information in the first place for reasons other than the stated purpose. Obtaining evidence for use against Americans in legal proceedings unrelated to national security or foreign intelligence is not a permissible purpose for collecting communications under Section 702. It therefore should not be a permissible use of those communications.

Third, Congress should add specificity to its definition of "minimization." In the absence of objective statutory criteria, there has been a predictable steady slide toward wider sharing of raw data, greater access to the data by agency personnel, and more exceptions to retention limits. On retention in particular, Congress should clarify that keeping Americans' information for five years, and for even longer in cases where that information has been reviewed and no determination of its status has been made, is not "minimization." Congress should specify that all information not subject to a "litigation hold" shall be destroyed within three years of the authorization for the acquisition, unless it has been reviewed and determined to be foreign intelligence or evidence of a crime (where the use of that evidence would comply with applicable use limitations).

---

[122] *See, e.g.,* Steven M. Bellovin, Matt Blaze, Susan Landau, & Stephanie K. Pell, *It's Too Complicated: How the Internet Upends Katz, Smith, and Electronic Surveillance Law*, 30 HARV. J.L. & TECH. 1, *8 (2016) (noting that "[t]he application of traditional content/non-content distinctions leads to inconsistent and anomalous results"); *Riley*, 134 S. Ct. at 2490 ("Data on a cell phone can also reveal where a person has been. Historic location information is a standard feature on many smart phones and can reconstruct someone's specific movements down to the minute, not only around town but also within a particular building.").

[123] *See* 18 U.S.C. § 2703; 50 U.S.C. § 1861.

[124] Memorandum from Hugo Teufel III, Chief Privacy Officer, Dep't of Homeland Sec., regarding The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 29, 2008), *available at* https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

C. Increasing Transparency and Accountability

A range of other reforms would increase the transparency and accountability of Section 702 surveillance. For example, *all* agencies that are authorized to perform U.S. person queries, including the FBI, should be required to report how often they use U.S. person identifiers to query databases containing Section 702 data. This obligation should remain in place even if Congress enacts a warrant requirement for U.S. person queries. Lawmakers and the public need this information to understand and evaluate the impact on Americans of a surveillance authority that is nominally targeted at foreigners overseas.

Congress also should address the artificial barriers that are blocking legal challenges to Section 702 surveillance. Even though Congress clearly intended for defendants to be able to challenge the use of Section 702-derived evidence in criminal cases, the government's notification policies are thwarting this intent. Congress should clarify that evidence is "derived" from Section 702 surveillance, for purposes of triggering the notification requirement, if the government would not otherwise have possessed this evidence. It should also specify that a person has standing to bring a civil lawsuit if she has a reasonable basis to believe her information has been (or will be) acquired, and if she has expended (or will expend) time or resources in an attempt to avoid acquisition.

An important caveat is in order. While reforms that promote transparency and accountability are critical, they are not a substitute for limiting the scope of Section 702 surveillance and shoring up privacy protections for Americans whose communications are "incidentally" collected. The most stringent of oversight provisions cannot justify amassing the personal data of ordinary, law-abiding private citizens. Nor can they legitimize the warrantless searching of Americans' phone calls and e-mails. Procedural protections are only as good as the substantive rights and limitations they enforce. That is why Congress should reform Section 702 to bolster those rights and limitations while preserving the core of the statute: warrantless surveillance of foreigners who pose a threat to our nation.

Thank you again for this opportunity to testify.