4 "Incidental" Foreign Intelligence Surveillance and the Fourth Amendment

Jennifer Daskal* & Stephen I. Vladeck†

The United States' foreign intelligence surveillance scheme permits broad-based collection of foreigner data, based largely on the presumption that such foreigners lack Fourth Amendment rights – and that the acquisition of such data is therefore freed from the strictures of the Constitution. For technological reasons, however, such broad-based collection necessarily sweeps in hundreds of millions of U.S.-person communications – those of U.S. citizens and legal permanent residents, and others residing in the United States – which are protected by the Fourth Amendment. This chapter argues for a three-pronged reformulation of Fourth Amendment doctrine to take these interests into account, and thus better serve the interests the Fourth Amendment is meant to protect. First, it calls for a presumptive Fourth Amendment, pursuant to which the Fourth Amendment is generally understood to govern the acquisition of data, regardless of the location or identity of the target. While this does not mean that all such acquisitions are subject to the warrant requirement (we support, with some caveats, the foreign intelligence exception to this requirement), such acquisitions must at least satisfy the Fourth Amendment's reasonableness test. Second, it argues that the Fourth Amendment reasonableness of such large-scale collection of data depends in significant part on the existence and effective implementation of postacquisition limits on the use, retention, and dissemination of incidentally collected U.S.-person data. And, third, it argues that law enforcement querying of that data for U.S.-person information should be understood as a separate Fourth Amendment event that is independently required to meet the applicable constitutional requirements.

Introduction

Section 702 of the Foreign Intelligence Surveillance Act (FISA) Amendments Act of 2008[1] is held out by commentators across the political spectrum as a critically important surveillance tool – one that has helped the nation respond to (and avert) planned

* Associate Professor of Law, American University Washington College of Law.
† Professor of Law, University of Texas School of Law. Our sincere thanks to David Gray and Stephen Henderson for inviting us to contribute to this volume, and for their indefatigable (if not infinite) patience with us thereafter.

1 *See* Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FISA Amendments Act of 2008), Pub. L. No. 110–261, § 101(a), 122 Stat. 2436, 2438–48 (2008) (codified as amended at 50 U.S.C. § 1881a).

attacks.[2] Yet, it is also controversial. The provision, which was the centerpiece of the 2008 amendments to FISA, authorizes "programmatic" surveillance of noncitizens reasonably believed to be located outside the United States whose communications nevertheless cross through U.S. servers, nodes, or other electronic infrastructure.[3] Even by conservative estimates, the government collects hundreds of millions of communications under Section 702 on an annual basis.[4] Included in that figure are millions of emails and other communications by U.S. persons (defined here as citizens and lawful permanent resident aliens).[5] This occurs despite the fact that Section 702 forbids the direct "targeting" of such communications.[6] Such so-called incidental collection nevertheless occurs when a U.S. person is in communication with foreign targets, or when a U.S. person's communications are bundled with a foreign target's communications, and the government has no way to acquire the targeted communication without also scooping up the nontargeted communications with which it is bundled.[7] As a result, this extremely valuable foreign intelligence surveillance program is predictably collecting large quantities of data about U.S. persons that would *not* be permitted if the U.S. persons whose data is being collected were the direct targets of the surveillance.

Such surveillance has thus far been held to be constitutional because of the intersection of at least three different strands of Fourth Amendment jurisprudence: first, most noncitizens located outside the United States do not enjoy Fourth Amendment protections;[8] second, the incidental collection of the communications of persons protected by the Fourth Amendment generally does not make an otherwise lawful search unlawful;[9] and third, even if the Fourth Amendment might otherwise apply, Section 702

2 *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 9–10 (2014) [hereinafter PCLOB 702 REPORT], http://www.pclob.gov/library/702-Report.pdf.

3 *Id.* at 111–113.

4 *See* [Caption Redacted], [Docket No. Redacted], 2011 WL 10945618, at *9, *25 (FISA Ct. Oct. 3, 2011) [hereinafter *October 2011 Bates Opinion*] (referring to the fact that the NSA acquires "more than two hundred fifty million Internet communications each year pursuant to Section 702").

5 Even if only 5 percent of these communications were from U.S. persons, that would add up to more than 12 million U.S.-person communications.

6 *See* 50 U.S.C. §§ 1801(i), 1881a(b) (2012).

7 *See infra* text accompanying note 46. Previously, significant quantities of U.S. person communications were also collected through what was known as "about" collection" – in situations when a U.S. person was communicating "about " a foreign target. As this chapter went to press, however, the NSA announced that it would no longer engage in "about" communications, after concerns were raised by both the FISC and some members of Congress. *See* Nat'l Security Agency, NSA Stops Certain Section 702 "Upstream" Activities (Apr. 28, 2017), https://www.nsa.gov/news-features/press-room/statements/2017-04-28-702-statement.shtml.

8 *See, e.g.*, *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990). As discussed later, the Supreme Court recently heard arguments in a case that may provide an opportunity for clarifying the scope of *Verdugo-Urquidez*. *See infra* note 22.

9 *See, e.g.*, *In re Directives* [Redacted Text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008) [hereinafter *In re Directives*] (concluding that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful"); *United States v. Bin Laden*, 126 F. Supp. 2d 264, 280 (S.D.N.Y. 2000) ("Incidental interception of a person's conversations during an otherwise lawful surveillance is not violative of the Fourth Amendment"); *see also United States v. Kahn*, 415 U.S. 143, 157–58 (1974).

surveillance falls within a "foreign intelligence surveillance" exception to the Warrant Clause(and the searches are otherwise deemed reasonable).[10]

Section 702 capitalizes upon these threads by authorizing the large-scale collection of Internet communications (including communications to and from U.S. persons) when the government is *targeting* noncitizens abroad, *i.e.*, those who have no constitutional expectation of privacy in such communications. So framed, Section 702 may raise privacy concerns, along with diplomatic and foreign relations hackles, but it seems at least outwardly drawn so as not to implicate the Constitution.

In this chapter, we challenge this understanding, arguing that the scope of incidental collection of U.S. persons' communications pursuant to programmatic foreign intelligence surveillance triggers the Fourth Amendment – not only with respect to how the government *uses* what it incidentally collects, but at the point of acquisition itself. Specifically, we urge three key shifts in doctrine.

First, we argue for the adoption of a *presumptive* Fourth Amendment, pursuant to which Fourth Amendment protections are applied to the acquisition of *all* communications that are anticipated to include a U.S. person's data, regardless of whether the U.S. person is the direct target of the search. To be clear, we are not saying that a warrant is required for all such collection. Rather we support the premise of a foreign intelligence exception (appropriately circumscribed) to the warrant requirement. But we do argue that any such collection, even if it does not require a warrant, must satisfy a reasonableness test to be constitutional.

Second, we argue that an assessment of the postacquisition "use" constraints – namely, retention and dissemination limits – is central to the front-end reasonableness inquiry. This has already been recognized implicitly, if not explicitly, by both Congress and certain courts. The Wiretap Act, for example, requires that law enforcement officials "minimize the interception of communications not otherwise subject to interception" when they conduct Title III wiretaps.[11] In computer search cases, some courts have required specific protocols regarding access, retention, and dissemination of collected data.[12] Section 702 itself requires the executive branch to adopt, and the Foreign Intelligence Surveillance Court (FISC) to approve, so-called minimization procedures, which are

10 *See, e.g.*, *In re Directives*, 551 F.3d at 1012; *United States v. Hasbajrami*, 2016 WL 1029500, at *10–13 (E.D.N.Y. Feb. 18, 2016); *United States v. Mohamud*, No. 3:10-CR-475-KI-1, 2014 WL 2866749, at *16–18 (D. Or. June 24, 2014).

11 18 U.S.C. § 2518(5) (2012).

12 *See, e.g.*, *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1180 (9th Cir. 2010) (en banc) (Kozinski, J., concurring) (suggesting, albeit as guidance, the use of detailed computer search protocols); *United States v. Bonner*, No. 12–3429, 2013 WL 3829404, at *19 (S.D. Cal. July 23, 2013); *In re Search of 3817 W. West End*, 321 F. Supp. 2d 953, 955 (N.D. Ill. 2004) (requiring use of detailed search protocol); *In re Appeal of Application for Search Warrant*, 71 A.3d 1158 (Vt. 2012) (upholding ex ante requirements that personnel segregated from the investigators review the data and prohibitions on the use of certain search tools). *But see United States v. Burgess*, 576 F.3d 1078, 1094 (10th Cir. 2009) (noting that it would be "folly for a search warrant to attempt to structure the mechanics of the search because imposing such limits would unduly restrict legitimate search objectives"); *United States v. Grimmett*, 439 F.3d 1263, 1270 (10th Cir. 2006) ("[A] computer search 'may be as extensive as reasonably required to locate the items described on the warrant.'") (quoting *United States v. Wuagneux*, 683 F.2d 1343, 1352 (11th Cir. 1982)); *State v. Bizewski*, No. UWYCR110144340, 2013 WL 1849282, at *13 (Conn. Super. Ct. Apr. 10, 2013).

designed, among other things, to limit the retention and dissemination of U.S. person information.[13] A recent Foreign Intelligence Surveillance Court of Review (FISCR) opinion relied on "steps taken by the government to minimize the dissemination of" certain acquired information as a factor in its reasonableness assessment.[14] Other rulings by the FISC have adopted similar analyses.[15] In sum, both Congress and the courts are increasingly recognizing the importance of postacquisition limits on the retention, dissemination, and use of collected data in determining the lawfulness of proposed surveillance programs.[16] In our view, this is the right approach; the existence and robustness of such postacquisition limits are – and should be – an explicit part of the Fourth Amendment assessment into the reasonableness of the collection.[17]

Third, in addition to and independent of the reasonableness assessment, we argue that subsequent law enforcement *queries* of surveillance databases for information about a U.S. person are themselves Fourth Amendment events. The queries themselves must independently satisfy the Fourth Amendment's requirements.[18]

This chapter proceeds in three parts. Part I provides the relevant background – elucidating the current doctrine, the rise of the current foreign intelligence surveillance regime, and the scope of incidental collection that results. Part II explains why, given the scope and anticipated nature of the incidental collection that occurs, Section 702 (as well as the separate collection that takes place pursuant to Executive Order 12333) should be understood to implicate the Fourth Amendment insofar as it inevitably leads to the collection of significant quantities of U.S. persons' communications. Finally, we close in Part III by laying out the shifts in doctrine and policy that we think are needed. With Section 702 due to expire at the end of 2017,[19] our hope is that Congress will take seriously the unique constitutional problems posed by incidental collection in this context as it debates reauthorization – and that the courts will as well.

[13] *See* 50 U.S.C. §§ 1801(h), 1881a(e).

[14] *See In re Certified Question of Law*, No. 16–01, slip op. at 31 (FISA Ct. Rev. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.

[15] *See, e.g., In re Directives*, *supra* note 9, at 1015 (noting that the existence of "effective minimization procedures" supports the reasonableness of governmental surveillance); *October 2011 Bates Opinion*, *supra* note 4, at *27 (noting that both the FISC and FISCR "have recognized that procedures governing retention, use, and dissemination have a bearing on the reasonableness under the Fourth Amendment of a program for collecting foreign intelligence information").

[16] *See In re Certified Question of Law*, *supra* note 14, at 7 ("FISC review of targeting and minimization procedures under Section 702 is not limited to the procedures as written; rather, the Court examines how the procedures have been and will be implemented").

[17] For a parallel argument made in the context of "Big Data" surveillance programs, see David Gray, THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017). *See also* Stephen E. Henderson, *Fourth Amendment Time Machines (And What They Might Say about Police Body Cameras)*, 18 U. PA. J. CONST. L. 933, 972 (2016) (emphasizing the importance of "access, use, and dissemination restrictions for our privacy").

[18] *See* David Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SEC. L. & POL'Y 377, 399 (2016) (noting the "interesting" but unresolved question as to whether querying should be seen as a "separate Fourth Amendment event" or best seen as part of the "overall Fourth Amendment event described by the FAA").

[19] *See* FISA Amendments Act of 2008, Pub. L. No. 110–261, § 403(b)(1), 122 Stat. 2436, 2474 (2008), *amended by* FISA Amendments Act Reauthorization Act of 2012, Pub. L. 112–238, § 2(a)(1), 126 Stat. 1631 (2012).

I The Fourth Amendment, Foreign Intelligence Surveillance, and Incidental Collection

A *The Doctrine*

1 The Fourth Amendment's Territorial Limits

In the 1990 case of *United States v. Verdugo-Urquidez*, Chief Justice William Rehnquist concluded that only citizens and those with substantial voluntary connections to the United States are entitled to Fourth Amendment rights.[20] As Rehnquist put it (writing for himself and Justices White, O'Connor, and Scalia), "'the people' protected by the Fourth Amendment ... refers to a class of persons who are part of a national community or who have otherwise developed sufficient connection with this country to be considered part of that community."[21] Whatever its merits, this understanding of the Fourth Amendment's reach appears to be entrenched, at least for the time being.[22] Citizens, persons with sufficient connections to the United States (such as legal permanent residents), and other persons located in the United States are widely understood to be protected by the Fourth Amendment. By contrast, noncitizens located outside the United States who lack sufficient connections to the United States have no constitutional protection from warrantless or otherwise unreasonable searches and seizures carried out by the U.S. government.

This government relies on this doctrine to justify surveillance of noncitizen targets located outside the United States under laxer standards than those required for the targeting of citizens, legal permanent residents, and others residing in the United States.

2 Incidental Collection Permitted

The Supreme Court has long held that only the person whose premises, property, person, or effects have been searched or seized has cognizable Fourth Amendment rights vis-à-vis the government – the so-called personal-rights approach to the Fourth Amendment.[23] Thus, a criminal defendant has no grounds to challenge an illegal search of a third party,

20 494 U.S. 259 (1990).

21 *Id.* at 265. Although Justice Kennedy, providing the fifth vote, joined Rehnquist's opinion in full, his reasoning called into question the core of Rehnquist's logic, *i.e.*, that the term "the people" in the Fourth Amendment restricted its application to U.S. citizens and others with sufficient voluntary connections to the United States. *See id.* at 276 (Kennedy, J., concurring) ("Given the history of our Nation's concern over warrantless and unreasonable searches, explicit recognition of 'the right of the people' to Fourth Amendment protection may be interpreted to underscore the importance of the right, rather than to restrict the category of persons who may assert it.").

22 For a critique of and suggested limits to the ruling, see Jennifer Daskal, *Transnational Seizures: The Constitution and Criminal Procedure Abroad*, *in* CONSTITUTIONALISM ACROSS BORDERS IN THE STRUGGLE AGAINST TERRORISM 191 (Federico Fabbrini & Vicki Jackson eds., 2016). In February 2017, the Supreme Court heard arguments in a case in which one of the three questions presented is whether the extraterritorial application of the Fourth Amendment to noncitizens should be resolved on more functional terms, such as those suggested by Justice Kennedy in his *Verdugo-Urquidez* concurrence. As of this writing, the opinion has not yet been handed down. *See Hernandez v. Mesa*, No. 15–118, 2016 WL 5897576 (U.S. Oct. 11, 2016). By way of disclosure, one of us (Vladeck) is co-counsel to the Petitioners in *Hernandez*.

23 *See, e.g.*, *Minnesota v. Carter*, 525 U.S. 83, 88 (1998) ("In order to claim the protection of the Fourth Amendment, a defendant must demonstrate that he *personally* has an expectation of privacy in the place searched, and that his expectation is reasonable") (emphasis added); *id.* (The Fourth Amendment is a personal right that must be invoked by an individual"). For a critique of this view *see* David Gray,

even if that search yields information that is used against the defendant in the criminal proceedings. As the Court put it in *Rakas v. Illinois*:

> A person who is aggrieved by an illegal search and seizure only through the introduction of damaging evidence secured by a search of a third person's premises or property *has not had any of his Fourth Amendment rights infringed.* And since the exclusionary rule is an attempt to effectuate the guarantees of the Fourth Amendment, it is proper to permit only defendants whose Fourth Amendment rights have been violated to benefit from the rule's protection.[24]

This is not just a prudential rule of standing, but reflects an understanding of the Fourth Amendment's limits. If John puts evidence of a crime in his friend Jane's purse, and the police then unlawfully search that purse, only Jane – not John – has suffered a Fourth Amendment injury.

This analysis also carries over to information – not just physical property – voluntarily conveyed to others. The "misplaced trust" doctrine, for example, tells us that individuals do not have a reasonable expectation of privacy in information conveyed to an informant or undercover agent. This is so even if the informant or agent both records and instantaneously transmits the target's conversations to law enforcement officials; after all, the target loses control over the information once it has been transmitted to another. As a plurality of the Supreme Court characterized it, "The law gives no protection to the wrongdoer whose trusted accomplice is or becomes a police agent."[25]

In the context of Section 702 collection, the government relies on the misplaced trust doctrine to argue that

> once a non-U.S. person located outside the United States receives information, the sender loses any cognizable Fourth Amendment rights with respect to that information. That is true even if the sender is a U.S. person protected by the Fourth Amendment, because he assumes the risk that the foreign recipient will give the information to others, leave the information freely accessible to others, or that the U.S. government (or a foreign government) will obtain the information.[26]

Taken to its logical conclusion, this means that all persons lose their reasonable expectation of privacy – and thus any Fourth Amendment protection – in communications transmitted to others. And while the Department of Justice seems to have backed off this extreme position (and separately seems to acknowledge that the use of such shared information can raise Fourth Amendment concerns),[27] the government maintains – as

THE FOURTH AMENDMENT IN AN AGE OF SURVEILLANCE (2017) and David Gray, *Dangerous Dicta*, 72 WASH. & LEE L. REV. 1181 (2015).

24 *Rakas v. Illinois*, 439 U.S. 128, 425 (1978) (emphasis added) (citations omitted); *id.* at 426 (emphasizing that "persons who [are] not parties to unlawfully overheard conversations or who did not own the premises on which such conversations took place [do] not have standing to contest the legality of the surveillance, regardless of whether or not they [are] the 'targets' of the surveillance").

25 *United States v. White*, 401 U.S. 745, 752 (1971); *see also Lewis v. United States*, 385 U.S. 206 (1966); *Hoffa v. United States*, 385 U.S. 293 (1966); *Lopez v. United States*, 373 U.S. 427 (1963).

26 *See* Gov't Unclassified Response to Defendant's Alt. Motion for Suppression of Evidence & a New Trial at 48, *United States v. Mohamud*, No. 3:10-cr-475-KI, 2014 WL 2866749 (D. Or. June 24, 2014). For a thoughtful analysis of the misplaced trust doctrine, *see* Kiel Brennan-Marquez, *Fourth Amendment Fiduciaries*, 84 FORDHAM L. REV. 611 (2015).

27 Notably, the above-quoted passage referring to the misplaced trust doctrine was dropped in the appellate brief in the same case, even though much of the rest of the brief tracks the earlier lower court filing. *See* Answering

supported by several courts – that the incidental collection of U.S. (or other protected) persons' communications does not render an otherwise valid search unlawful.[28]

In some isolated cases, courts have nevertheless imposed limits. As Judge John Bates, then presiding judge of the FISC, stated, "There surely are circumstances in which incidental intrusions can be so substantial as to [both trigger the Fourth Amendment and] render a search or seizure unreasonable."[29] Moreover, courts and the government also have recognized that U.S. persons have Fourth Amendment rights with respect to how information collected incidentally is ultimately *used* – hence the focus on minimization.[30] But, in general, the government has been free from the strictures of the Fourth Amendment when it engages in the *acquisition* of non-U.S. persons' data located outside the United States, despite the anticipated incidental collection of U.S. persons' data.[31] To the extent that the Fourth Amendment is triggered, the prevailing assumption is that it is implicated only by what is *done* with a U.S. person's data that has been obtained, not at the point of acquisition itself.

3 Foreign Intelligence Exception

In the context of foreign intelligence collection, this doctrine also intersects with yet another strand of Fourth Amendment jurisprudence: the idea of a foreign intelligence exception to the Fourth Amendment's warrant requirement. Pursuant to this doctrine, searches of foreign powers or agents of foreign powers reasonably believed to be located outside the United States are subject to a "reasonableness" test only, *even* if the direct target of the search is a U.S. person.[32]

B *Foreign Intelligence Surveillance*

1 Section 702 of the FISA Amendments Act

As the now-familiar story goes, the FISA Amendments Act of 2008 (FAA) was a response to a May 2007 ruling by the FISC that prohibited the warrantless targeting of foreigners'

Brief of Plaintiff-Appellee, *United States v. Mohamud*, No. 14–3027 (9th Cir. Dec. 7, 2015); *see also* Robert Litt, *The Fourth Amendment in a Digital Age*, 126 YALE L.J. F. 8 (2016), http://www.yalelawjournal.org/forum/fourth-amendment-information-age (describing it as "significant that the government did not argue in *Jewel* [another case challenging the constitutionality of 702 collection] that the plaintiffs had no reasonable expectation of privacy in the content of the communications even though that content was exposed to a third party").

28 *See, e.g., United States v. Hasbajrami*, 2016 WL 1029500, at *9 (E.D.N.Y. Feb. 18, 2016) ("When surveillance is lawful in the first place – whether it is the domestic surveillance of U.S. persons pursuant to a warrant, or the warrantless surveillance of non-U.S. persons who are abroad – the incidental interception of non-targeted U.S. persons' communications with the targeted persons is also lawful"); *Mohamud*, 2014 WL 2866749, at *16 ("The § 702 acquisition targeting a non-U.S. person overseas is constitutionally permissible, so, under the general rule, the incidental collection of defendant's communications with the extraterritorial target would be lawful"); *In re Directives*, 551 F.3d at 1015; *see also United States v. Kahn*, 415 U.S. 143, 157–58 (1974).

29 *October 2011 Bates Opinion*, *supra* note 4, at *26.

30 *Id.* at *27.

31 There is, however, a statutory prohibition on reverse targeting – targeting a person located outside the United States with the *purpose* of targeting a particular, known person reasonably believed to be in the United States. *See* 50 U.S.C. § 1881a(b)(2) (2012).

32 *See In re Directives*, 551 F.3d at 1012; see also *October 2011 Bates Opinion*, supra note 4, at *24; *Mohamud*, 2014 WL 2866749, at *15–18. The definition of "foreign power" and "agent of a foreign power" can be found at 50 U.S.C. § 1801(a) & (b).

communications transiting through U.S. infrastructure. Whereas prior FISC court judges had approved such searches, Judge Roger Vinson interpreted FISA's requirements of an individualized, court-approved finding of probable cause to apply – regardless of the location or nationality of the target (or the other participants).[33] Claiming that a warrant requirement would kneecap its ability to track and prevent threats, the Bush administration persuaded Congress to enact the temporary Protect America Act of 2007 (PAA),[34] which permitted warrantless foreign surveillance on targets believed to be outside the United States; this included the authority to engage in the warrantless surveillance of U.S.-person targets. In 2008, the PAA was replaced with the (somewhat-more) permanent FAA, the heart of which is Section 702.[35]

While Section 702 does not permit the direct targeting of U.S. persons, it does permit broad-based collection of non-U.S.-person data in ways that lead to *incidental* collection of vast quantities of U.S.-person data. Section 702 gives the government wide latitude to target any non-U.S. person "reasonably believed" to be outside the United States in order to acquire specified categories of foreign intelligence information.[36] There is no probable cause determination, or even a required finding of reasonable articulable suspicion that the target is an agent of a foreign power or in possession of foreign intelligence information. And there is no court review of the specific targeting decisions. Rather, the government applies to the FISC, on an annual basis, for an "authorization" to target, for specified purposes, the communications of noncitizens reasonably believed to be outside the United States.[37] The FISC reviews the authorization application to ensure compliance with the applicable statutory provisions and the Fourth Amendment. In other words, the FISC's job is to oversee the programmatic procedures, not individual applications for, or specific instances of, surveillance. Electronic communication providers are required to assist in these collection efforts; specifically, they must "immediately provide the Government with all information, facilities, or assistance necessary to accomplish the acquisition" that is being sought.[38]

As far as is publicly known, there are two separate foreign intelligence surveillance programs operated under Section 702: what is known as the PRISM program and upstream collection.[39] Pursuant to PRISM, the government sends approved "selectors" (e.g., email addresses) to electronic communication service providers, such as Internet service providers, who then are required to turn over all communications sent over their networks to or from the selector.[40] The PRISM program accounts for approximately 90 percent of communications collected under 702 – yielding upward of 225 million communications each year.[41]

33 *See In re Certified Question of Law*, No. 16–01 (FISA Ct. Rev. Apr. 14, 2016), https://www.dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.

34 Protect America Act of 2007 (PAA), Pub. L. No. 110–55, 121 Stat. 552 (formerly codified at 50 U.S.C. §§ 1805a–c), *repealed by* FISA Amendments Act of 2008, Pub. L. No. 110–261, § 403(a), 122 Stat. 2437, 2473–2474.

35 *See supra* note 1.

36 *Id.*

37 50 U.S.C. § 1881a(a).

38 *Id.* § 1881a(h)(1).

39 PCLOB 702 REPORT, *supra* note 2, at 7.

40 *Id.*

41 *October 2011 Bates Opinion*, *supra* note 4, at *9, *25 (referring to the fact that the NSA acquires "more than two hundred fifty million Internet communications each year pursuant to Section 702," and that

The remaining 10 percent is collected via upstream collection – this time with the aid of the Internet and telecommunications companies that control the fiber optic lines over which Internet communications travel "upstream" of the U.S. Internet service providers.[42] Because of the way the technology operates, such upstream collection yields so-called Internet transactions.[43] Sometimes, such transactions include discrete communications, but oftentimes they include multiple communications bundled together – meaning that totally unrelated communications may be acquired because they are bundled with communications that are to or from the target.[44]

Section 702 thus yields incidental collection of U.S. persons' data in two key ways: (1) when a U.S. person is in direct communication with a targeted non-U.S. person; and (2) when, also as part of upstream collection, the government collects bundled communication transactions that include discrete communications of U.S. persons.[45]

2 Minimization Procedures

To help ameliorate the privacy concerns raised by such collection, Section 702 requires the attorney general, in consultation with the director of national Intelligence, to adopt "minimization procedures."[46] Broadly speaking, they require the attorney general to minimize the acquisition, retention, and dissemination of non–publicly available information concerning nonconsenting U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[47] Dissemination of non–publicly available, non–foreign intelligence information that identifies a nonconsenting U.S. person is prohibited "unless such person's identity is necessary to understand foreign intelligence information or assess its importance."[48]

Importantly, the requirements include an exception for law enforcement purposes: notwithstanding the otherwise-applicable prohibitions on retention and dissemination of U.S.-person information, information that is "evidence of a crime which has been, is being, or is about to be committed" can be retained and disseminated for law enforcement purposes.[49]

The existence of such "minimization" procedures is hardly unique to FISA. Congress, for example, has prescribed the application of minimization procedures as part of the Wiretap Act, which governs law enforcement's real-time collection of electronic and wire communications.[50] But, as stated previously, the minimization procedures required under the FAA differ from what is required under the Wiretap Act or pursuant to the specific court orders

approximately 91 percent of these communications are acquired directly from Internet Service Providers (ISPs) through the PRISM program); PCLOB 702 Report, *supra* note 2, at 33–34.

42 PCLOB 702 Report, *supra* note 2, at 8.

43 *October 2011 Bates Opinion*, *supra* note 4, at *5; PCLOB 702 Report, *supra* note 2, at 7.

44 PCLOB 702 Report, *supra* note 2, at 39–41; *October 2011 Bates Opinion*, *supra* note 4, at *26.

45 For a more in-depth discussion of the kinds of incidental collection that result from both Section 702 and other surveillance programs, see Jennifer Daskal, *The Un-Territoriality of Data*, 125 Yale L.J. 326, 348–54 (2015).

46 50 U.S.C. § 1881a(e).

47 *See id.* §§ 1881a(e), 1801(h)(1).

48 *Id.* § 1801(h)(2).

49 *Id.* § 1801(h)(3).

50 *See* 18 U.S.C. § 2518(5).

issued in a handful of computer search cases. Wiretap orders and computer search protocols are signed off on and reviewed by a judge. The minimization requirements are tailored to the specific needs of the case. Under the FAA, the FISC signs off on the programmatic *procedures*, but does not review or oversee their application in any individual case. The applicable minimization procedures are thus written, implemented, and overseen on a case-by-case basis exclusively by the executive branch.

3 Executive Order 12333

The executive branch also engages in a range of extraterritorial surveillance activities targeted at non-U.S. persons located outside the United States that are not regulated by Section 702 or any statute, but instead governed by Executive Order 12333. Reports suggest that electronic surveillance pursuant to EO 12333 accounts for an even greater share of electronic surveillance activities than any equivalent surveillance conducted under traditional FISA or the FAA.[51] Of note, collection under EO 12333 reportedly includes "vacuum cleaner" or "bulk" collection, pursuant to which the executive sweeps in all communications that transit a particular cable without using a selector or other search term to limit the scope of the acquired data.[52] Reports suggest that bulk collection has included, among other things, Internet metadata,[53] Web cam chats,[54] cell phone location data,[55] and email address books.[56] Such bulk collection is not deemed to target anyone, thus avoiding the prohibition on targeting U.S. persons. Other collection falls outside the prohibition on targeting U.S. persons on the basis of a largely unreviewable executive branch determination that such collection would not require a warrant if done for law enforcement

51 *See, e.g.*, Alvaro Bedoya, *Executive Order 12333 and the Golden Number*, JUST SECURITY (Oct. 9, 2014, 10:14 AM), http://justsecurity.org/16157/executive-order-12333-golden-number/ [http://perma.cc/Q8ZH-NM6G]; John Napier Tye, *Meet Executive Order 12333: The Reagan Rule that lets the NSA Spy on Americans*, WASH. POST, July 18, 2014, http://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html [http://perma.cc/6DHP-TNES].

52 *See* Presidential Policy Directive – Signals Intelligence Activities § 2 (Jan. 17, 2014) [hereinafter *PPD-28*], http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities (referencing signals intelligence collected in "bulk" and defining "bulk" collection to mean "the authorized collection of large quantities of signals intelligence data which, due to technical or operational considerations, is acquired without the use of discriminants (e.g., specific identifiers, selection terms, etc.)" for specified purposes).

53 *See* Tye, *supra* note 52.

54 Spencer Ackerman & James Ball, *Optic Nerve: Millions of Yahoo Webcam Images Intercepted by GCHQ*, GUARDIAN (Feb. 28, 2014), http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo/ [http://perma.cc/KN9D-76HM].

55 *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Locations Worldwide, Snowden Documents Show*, WASH. POST (Dec. 3, 2013), http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html. Though the NSA denies that it is "intentionally collecting bulk cellphone location information about cellphones in the United States," such bulk collection of cell phone location information outside the United States inevitably sweeps in millions of U.S. mobile phone users who travel abroad every year. *Id.*

56 *See* Barton Gellman & Ashkan Soltani, *NSA Collects Millions of E-mail Address Books Globally*, WASH. POST (Oct. 14, 2013), http://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html [http://perma.cc/FS9J-2LKY].

purposes in the United States.[57] There is no FISC or other judicial review of such programs, and virtually no statutory limits on how such data can be subsequently used.

II Incidental Collection as a Fourth Amendment Search

There are three separate – but interrelated – reasons why incidental collection should trigger the Fourth Amendment – not just with respect to how the data is ultimately used, but at the point of collection in the first place.

First, and most importantly, in the context of foreign intelligence surveillance under Section 702 and Executive Order 12333, the *scale* of U.S.- person communications being "incidentally" intercepted raises novel Fourth Amendment concerns. As Judge Bates expressed it, "There surely are circumstances in which incidental intrusions can be so substantial as to [both trigger the Fourth Amendment and] render a search or seizure unreasonable."[58] Even by conservative estimates, the government collects millions of communications under Section 702 on an annual basis. Such collection is estimated to include thousands of communications per year in which *both* the sender and all the recipients are among the "people" covered by the Fourth Amendment;[59] it likely yields millions more in which *either* the sender or the recipient is a U.S. person or a person located in the United States.[60] We do not think that Fourth Amendment doctrine ever considered – or can survive – a scenario when incidental collection is on such a massive scale.

Second, the incidental collection doctrine is premised at least in part on the notion that the government "accidentally" intercepts the communication at issue – where it could not reasonably have expected that the surveillance of the target would yield information about a third party wholly unrelated to the target. Whatever the merits of that premise, there are reasons why courts (and the Constitution) should not be as forgiving when the government *knows* that its surveillance will produce information about third parties. As Judge Leonard Sand explained in 2000, it "is significantly more problematic" when the government *anticipates* that lawful surveillance of one target will produce evidence of a nontarget's culpability.[61] Several FISC judges also seem to recognize the need to address anticipated collection of U.S.-person data in evaluating the constitutionality of 702 and related surveillance programs; hence the focus on minimization procedures as an element of assessing Fourth Amendment reasonableness.[62] In fact, in many ways, we are simply seeking to make explicit an understanding of incidental collection and the Fourth Amendment that at least some of the FISC's judges have implicitly adopted.

57 *See* 50 U.S.C. § 1881c(a)(2) (2012) ("No element of the intelligence community may intentionally target, for the purpose of acquiring foreign intelligence information, a United States person reasonably believed to be located outside the United States under circumstances *in which the targeted United States person has a reasonable expectation of privacy and a warrant would be required if the acquisition were conducted inside the United States for law enforcement purposes* [without a FISC-approved order or an Attorney General–issued emergency exception]") (emphasis added).

58 *October 2011 Bates Opinion*, *supra* note 4, at *26.

59 *Id.* at *11.

60 *See supra* notes 4–5.

61 *United States v. Bin Laden*, 126 F. Supp. 3d 264, 281 (S.D.N.Y. 2000).

62 *See, e.g.*, *In re Certified Question of Law*, No. 16–01, slip op. at 37–44 (FISA Ct. Rev. Apr. 14, 2016); *In re Directives*, 551 F.3d at 1015; *October 2011 Bates Opinion*, *supra* note 4, at *27.

Third, the prototypical incidental collection case involves surveillance that is separately covered by the Fourth Amendment. After all, U.S. law enforcement generally lacks jurisdiction to investigate unilaterally outside the U.S. territorial borders; as a result, targets of most searches are either U.S. citizens, legal permanent residents, or people located in the United States. At least someone – even if not the third party implicated by the search – has standing to challenge an illegal search.[63]

Thus, at least in the prototypical case, there is a meaningful judicial check on both the front and back end of the collection. Judges sign off on each aspect of the underlying surveillance – applying the Fourth Amendment's substantive and procedural standards, including individualized judicial review. And in most cases the person whose property is being searched or seized can raise a Fourth Amendment claim, even if the third party whose data is incidentally collected cannot. In contrast, programmatic surveillance under Section 702 or EO 12333 does *not* involve any individualized judicial review. Given that the targets are noncitizens located outside the United States, they have no Fourth Amendment rights to adjudicate on either the front or back end of the surveillance. As a result, the data is being collected pursuant to much *laxer* standards than those that would apply if the U.S. person, whose data is incidentally collected, were the direct target of the search or seizure.

Whether any of these three considerations suffices on its own to demonstrate why incidental collection in the context of foreign intelligence surveillance should trigger Fourth Amendment concerns, they seem to us to support that conclusion when taken together. Foreign intelligence programs yield significant surveillance of U.S. persons on the basis of the much lower standards that apply to the targeting of noncitizens outside the United States. This provides insufficient protection to the very category of persons that the Fourth Amendment is, according to current doctrine, meant to protect.

III Rethinking the Fourth Amendment in Light of Incidental Collection

The rise of the digitalized person, coupled with the scale of foreign intelligence collection, requires a rethinking of Fourth Amendment doctrine. The intermingling of communications, taken together with the scope of contemporary foreign intelligence surveillance, means that the United States is now gathering vast quantities of U.S. persons' communications as it targets non-U.S. persons located outside the United States, but without any of the constraints imposed by the Fourth Amendment. And it is doing so *knowing* that such large-scale incidental collection will occur. As we explain in what follows, this ought to trigger the Fourth Amendment – not just with respect to subsequent questions involving the use of such data, but at the point of collection itself.

In this section, we explore what a reformulated Fourth Amendment doctrine would look like. Specifically, we argue for a presumptive Fourth Amendment that governs the acquisition of data that is anticipated to include U.S. persons' information, regardless of whether a U.S. person is the target of the search. This is justified as a much-needed prophylactic protection for the class of U.S. persons the Fourth Amendment is designed to protect.

We also consider whether and to what extent minimization requirements – in particular limits on retention and dissemination – can independently address Fourth

[63] *See, e.g.*, cases cited *supra* note 12.

Amendment concerns. The U.S. government, after all, acknowledges that U.S. persons are often caught up in foreign intelligence collection, but argues that any privacy concerns are adequately addressed by minimization requirements. We agree that such minimization requirements are essential, and that they need to be evaluated as part of the up-front reasonableness assessment that a presumptive Fourth Amendment requires. But we also think that they have been, in some key respects, insufficient to date.

Finally, we argue that the law enforcement querying of incidentally collected U.S.-person data is itself a Fourth Amendment "event" that must satisfy the applicable constitutional requirements.

A *A Presumptive Fourth Amendment*

In an interconnected, digitalized world, the current myopic focus on the target of the search leaves unprotected the rights of the very "people" the Fourth Amendment is meant to protect. We instead advocate a presumptive Fourth Amendment: one in which the Fourth Amendment is presumed to apply, regardless of the location or identify of the target.[64] Such a presumption could be rebutted if and only if the government establishes that *none* of the parties to the communication or with some kind of ownership interest in a particular document is a U.S. person, *i.e.*, a person protected by the Fourth Amendment.

In practice, this means that bulk collection, wherever it takes place, is subject to Fourth Amendment regulation; communications targeting noncitizens will presumptively be covered by the Fourth Amendment, irrespective of the identity of the particular target; and most foreign intelligence surveillance will also trigger a Fourth Amendment inquiry because it will not be feasible in most cases – at least on the basis of what we know about current technology – to make a showing that none of the parties affected by these programs has Fourth Amendment rights. By contrast, targeted and discrete surveillance, such as programs focusing on North Korean diplomats in North Korea, likely would not trigger the Fourth Amendment – although there may be policy reasons to expand protections across the board, even in those circumstances.[65]

This, of course, is not the same as saying that a warrant is required every time the government searches or seizes electronic communications for foreign intelligence purposes, or that all surveillance necessarily implicates the Fourth Amendment. Both of us are, in fact, persuaded that there should be a foreign intelligence exception to the warrant requirement, although we have concerns about how broadly the exception has been defined – especially insofar as it is being applied even when the collection of foreign intelligence surveillance is not the primary purpose of the search.[66] We also are well aware that there is some surveillance that simply does not trigger the Fourth Amendment,

64 This tracks the approach that one of us has previously recommended. *See* Daskal, *supra* note 46, at 379–87.

65 *See, e.g.*, *PPD-28*, *supra* note 53, § 4(a) (requiring that postacquisition limits on retention and dissemination of data apply "equally to the personal information of all persons, regardless of nationality" to "the maximum extent feasible consistent with the national security").

66 *See, e.g.*, *In re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008) (holding that the foreign intelligence surveillance exception to the Warrant Clause requires only that foreign intelligence gathering be a "significant" purpose of the search).

as well as certain categories of surveillance that do not require a warrant, regardless of the application of the foreign intelligence exception.

But we do think that any reasonableness (or warrant) requirement that does apply should be applied consistently to U.S.-person targets and non-U.S.-person targets alike. This in fact was one of the central insights of the 1978 Congress that first enacted FISA. Notably, it required a warrant for *all* covered foreign intelligence surveillance at the time. As the House Intelligence Committee Report explained, such a requirement was imposed "not ... primarily to protect such persons but rather *to protect U.S. citizens* who may be involved with them and to ensure that the safeguards inherent in a judicial warrant cannot be avoided by a determination as to a person's citizenship."[67]

To reiterate, we are not advocating a return to the 1978 surveillance regime – and a warrant requirement for all foreign intelligence surveillance. But we *do* reject the idea that the acquisition of non-U.S.-person data falls outside the Fourth Amendment's scope, especially in situations when it can reasonably be anticipated that such collection will yield U.S. persons' data. Any such collection that falls outside the warrant requirement must still meet the Fourth Amendment's reasonableness requirement. Otherwise, we are providing only nominal protections to the very people who, even under *Verdugo-Urquidez*, the Fourth Amendment is intended to protect.

B *Back End Protections as Part of the Front End Reasonableness Inquiry*

Any surveillance scheme of globally interconnected digitalized communications is going to yield incidental collection of U.S. persons' information. What makes the scheme reasonable – or not – turns in substantial part on how this incidentally collected information is handled (as well as the scope and purpose of the collection itself). Thus, the existence, application, and robustness of these back end protections for incidentally acquired information are essential components of the *front end* constitutional reasonableness inquiry. This is, in fact, what Congress requires as a matter of statutory law as part of the Wiretap Act and FISA Amendments Act, what the executive branch says it does as a matter of policy, what the Ninth Circuit suggested in its computer search protocol cases, and what several FISC judges have already demanded as part of the Fourth Amendment inquiry. Here, we would seek to make these scattershot approaches categorical rules – making the back end protections an essential element of front end reasonableness.

A recent FISC opinion provides an example of some of what we are suggesting. In evaluating a reauthorization certification pursuant to Section 702, Judge Thomas Hogan engaged in a thorough review of CIA, FBI, and NSA minimization procedures, as well as prior compliance incidents.[68] Although we disagree with some of Judge Hogan's ultimate conclusions, we think he engaged in exactly the kind of front end assessments of back end procedures that the Fourth Amendment demands in these cases.

[67] H.R. Rep. No. 95–1283, pt. 1, at 26 (1978) (emphasis added).

[68] *See In re Certified Question of Law*, No. 16–01 (FISA Ct. Rev. Apr. 14, 2016). Judge Hogan was aided in his review by Amy Jeffress, whom he appointed to act as amica curiae (pursuant to 50 U.S.C. § 1803(i)(2)(B) (2016)) to address the question of whether the minimization procedures met the statutory obligations and were consistent with the Fourth Amendment.

C *Law Enforcement Searches of U.S.-Person Information*

Separate and apart from the required front end inquiry, subsequent law enforcement queries of U.S.-person information should be deemed a search, subject to applicable procedural and substantive protections, and evaluated accordingly. The current rules governing FBI searches of acquired 702 databases fail to provide sufficient protections in this regard. In fact, somewhat ironically given the liberty interests at stake, the rules governing law enforcement searches for U.S. person information are currently *more permissive* than the rules governing intelligence community searches of such data. Under current minimization rules, FBI queries of 702 databases are permitted in order to "find and extract" either "foreign intelligence information" or "evidence of a crime."[69] By comparison, the NSA and CIA are only permitted to query the database using terms "reasonably likely to return foreign intelligence information."[70] The FBI rules thus are more expansive than what is required for the NSA and CIA in two key respects: first, they are not limited by a requirement that the search terms be "reasonably likely" to return the sought-after information; second, they can look for evidence of a crime, in addition to foreign intelligence information.

Moreover, whereas untrained law enforcement personnel are not permitted to access the 702 databases directly, they appear able to ping the database for whatever reason they so choose. If their search term yields a "hit," they can then seek an appropriately trained agent to run an actual query.[71] Both the pings of the database by untrained agents and the official queries can use U.S.-person identifiers or be designed to elicit information about U.S. persons. And whereas both the CIA and NSA are required to document the basis for such requests via a "statement of facts establishing that the use of any [U.S.-person] identifier as a selection term is reasonably designed to return foreign intelligence information as defined in FISA,"[72] no such obligation to document the basis for the query applies to the FBI.[73] Given the Fourth Amendment interests at stake, this is an oversight that, in our opinion, should be corrected.

In a recent FISC opinion, Judge Hogan rejected arguments by one of the FISC's amici curiae, Amy Jeffress, that the FBI queries of the 702 databases should be defined as a "separate action subject to the Fourth Amendment reasonableness test" and were at least in some respects unreasonable. While the court concluded that the querying process was relevant to the *overarching* reasonableness analysis of the program as a whole, it determined that the queries themselves were not separate events that should be independently assessed.

69 *See In re Certified Question of Law*, slip op. at 26–27. The FBI does not receive unminimized information acquired through "upstream collection," but does acquire a "portion" of PRISM collection. *See* PCLOB 702 Report, *supra* note 2, at 7.

70 *See In re Certified Question of Law*, slip op. at 24.

71 Such queries must be approved by both the untrained agent's supervisor and a national security supervisor. *Id.* at 28–29. The untrained agent is generally only permitted to see the results of the query if the information reasonably relates to foreign intelligence information, is necessary to understand foreign intelligence information, or is evidence of a crime. Yet, he or she can review the information if it is "unclear" whether those standards are met so as to help determine whether the information falls into one of those categories. *Id.* at 29. The government claims that the situations in which an untrained agent reviews information prior to a determination that it is foreign intelligence information (FII), relevant to understanding FII, or evidence of a crime are "very rare." *See id.*

72 *Id.* at 25.

73 *Id.* at 39–40 (noting argument that the FBI Minimization Procedures should be amended to require a written justification for each U.S.-person query of the database).

We disagree. The querying process is relevant to the overarching reasonableness analysis *and* is a specific search that should be independently evaluated for Fourth Amendment compliance. This position is supported by, among other cases, the Supreme Court's 2014 decision in *Riley v. California*.[74] In that case, the Supreme Court rejected the claim that law enforcement could engage in the warrantless search of a cell phone seized incident to arrest. Rather, the subsequent search of the cell phone was deemed a separate Fourth Amendment event that will generally require a warrant based upon probable cause.[75]

Congress can and should remedy this situation as part of any reauthorization of Section 702. Specifically, it should consider putting in place standards governing the pinging and querying of the databases for U.S.-person information. Even though the pings do not themselves yield the underlying data, they set in motion the process that does. It thus seems that agents should not be permitted to engage in the standardless pinging of the database for U.S.-person information until they get a positive hit. Rather, agents should be required to demonstrate a reasonable articulable suspicion that the term chosen will yield foreign intelligence information, information necessary to understand foreign intelligence information, or evidence of a crime. Subsequent queries for *metadata* should also be permitted based on a determination that there is a reasonable articulable suspicion that the responsive data is foreign intelligence information, relevant to understanding foreign intelligence information, or evidence of a crime, as approved by a supervisor. The basis for that determination should be documented in writing, so as to ensure transparency and future accountability with respect to such queries.

Queries for *communication content*, however, should only be permitted based on a finding of probable cause as approved by an independent court – either the FISC or an Article III court, depending on the nature of the investigation (*i.e.*, whether the information is being sought for foreign intelligence or ordinary law enforcement purposes). This is, after all, exactly what would be required if the FBI were seeking such information directly from either the target of the investigation or third-party provider that manages the target's data, rather than relying on the fact that it had already been collected pursuant to a separate foreign intelligence collection program. In emergency situations, authorizations can be approved by FBI supervisors, but the FBI should still be required to get post-hoc court approval, as is required with respect to emergency authorization for FISA orders and wiretaps.[76]

Critics are likely to argue that these types of requirements will simply impose additional and inefficient hurdles limiting law enforcement's ability to access potentially critical information. To this concern, we offer three responses: First, we recognize the need sometimes to act quickly and have suggested the application of emergency procedures (properly constrained) to deal with those situations. Second, and more importantly, the U.S. government now acquires millions of U.S. persons' communications every year via warrantless foreign intelligence surveillance programs. If law enforcement sought to access that data directly from either the target of its investigation or the third-party

74 134 S. Ct. 2473 (2014).

75 *Id.* at 2485.

76 *See, e.g.*, 50 U.S.C. § 1811; 18 U.S.C. § 2518(7). We are not the first to suggest a distinction in the standards governing queries of responsive metadata and communications content. *See also* ADAM KLEIN, MICHELE FLUORNEY, AND RICHARD FONTAINE, CTR. FOR A NEW AM. SECURITY, SURVEILLANCE POLICY: A PRAGMATIC AGENDA FOR 2017 AND BEYOND 6, 36, (2017) (suggesting that the FBI be permitted to query 702 databases for U.S. person information but receive responsive metadata only).

company that holds that data, it would need a warrant based on probable cause. Law enforcement should not be able to make an end-run around this requirement simply because the data is already in the government's possession – pursuant to a collection program that does not require probable cause or anything close. Additional limits are needed to protect against the kind of trawling of databases for U.S. persons' information that arguably runs afoul of the framers' fears of general warrants and raises legitimate concerns about a surveillance state.

Third, while we recognize the requirement of probable cause will be hard to meet, at least initially, in certain situations, responsive metadata can be obtained based on a mere reasonable articulable suspicion that the data contains responsive foreign intelligence information or evidence of a crime. The responsive metadata can in turn provide the relevant information needed to meet the probable cause standard.

In sum, we think that the querying of data collected under Section 702 (and other intelligence databases) for U.S. persons' information triggers the Fourth Amendment; that additional, internal checks on FBI access to these databases are essential, particularly given the incredible power that the FBI holds to affect the liberty interests of U.S. persons; that agents should be required to articulate a reasonable, articulable suspicion that the evidence sought is foreign intelligence information, relevant to understanding foreign intelligence information, or evidence of a crime in order to ping or query the database for responsive metadata; that queries for content should require a finding of probable cause approved by a court; that all such queries should be subject to internal approvals; and that those reasons should be put in writing so as to allow for subsequent review and oversight. Congress should demand each of these requirements as part of any reauthorization of Section 702 – and should consider imposing them on surveillance collected pursuant to Executive Order 12333 as well.

D *Additional Minimization Requirements*

As already stated, we also believe that the applicable use, retention, and dissemination limits should be addressed at the outset as part of the overall reasonableness inquiry. While the question of what *specific* retention, dissemination, and use restrictions ought to apply and how they should be implemented requires a nuanced and particularized assessment on both the programmatic and the individual case level, there are certain common requirements that should aid those assessments. Here, we focus on two: the need for transparency and consistency, and the need for enhanced accountability for and deterrence of error and abuse. We think Congress has erred in failing to require more in these areas. It has a chance to correct these shortcomings in the debate over the renewal of Section 702, currently set to sunset on December 31, 2017.

1 Transparency and Consistency

As the preceding discussion shows, minimization rules vary among agencies. They are often generally classified, although the executive branch has increasingly released unclassified – albeit redacted – versions of such procedures over the last several years. This is critically important. Public disclosure of these rules is needed to allow open and informed debate, particularly given how much is at stake for U.S. persons and their data. In conjunction with Section 702 reauthorization, Congress should require

as a matter of statutory law (not just executive branch discretion) the public disclosure of minimization rules from all of the agencies authorized to review and access data collected under Section 702, namely, the NSA, FBI, and CIA. Redactions should be permitted to protect against disclosure of specific programmatic details or technical means by which data is accessed. But there is no good reason to keep secret the substantive and procedural standards for querying, reviewing, retaining, and disseminating the acquired data.

Moreover, Congress should demand consistency, as much as is practically possible, across the different agencies. There will, of course, be a need for variation. It makes sense, for example, that the FBI should be able to access evidence of a crime, whereas the NSA and CIA cannot. But there does not seem to be any good justification for requiring a written justification for U.S.-person inquiries for the NSA and CIA, but not the FBI. Increased consistency will help with training, oversight, and analysis. As already stated, deviations should be permitted, but they ought to be explained and justified.

2 Accountability and Deterrence

The U.S. government does not publicly release the number of "compliance incidents," meaning those situations when executive branch officials fail to comply with the procedural or substantive requirements that either its own procedures or the FISC has imposed on particular collection methods. But there are enough reports of such incidents over enough different stretches of time to infer that even the most substantively robust minimization requirements will not be completely effective; hence, the need to couple meaningful back end protections with reasonable limits on collection itself.

The fact that so many compliance incidents have come to light suggests, in part, that existing internal oversight mechanisms have indeed been effective in many – if not all – cases. But internal oversight, while important, is not sufficient. Not only does it fail to provide any remedies for individuals affected, but it is also potentially subject to capture. The lack of an external check also fuels a *perception* of capture, even if the perception does not reflect reality. This in turn fosters public distrust of the government's actions. Existing oversight requirements thus should be coupled with three additional statutory requirements.

First, the executive branch should be required, by statute rather than merely court or internal executive branch rules, to report all compliance incidents to both the FISC and the intelligence committees and to release unclassified accounts of such incidents whenever it is possible to do so without jeopardizing national security. Whereas reporting of compliance incidents to the FISC is already required pursuant to the FISC's Rules of Procedure,[77] Congress should make this a statutory requirement, not just a matter of internal court rules. It should also consider the imposition of additional penalties for excessive and/or malicious violations of the minimization rules. The intelligence committees, in turn, should push the executive to make the reports public to the maximum

[77] *See* FISC R. 13(b) (2010).

extent possible and to ensure that compliance incidents are not symptomatic of larger flaws in the minimization requirements.

Second, FISC judges should be required to review and analyze prior compliance incidents and the government's responses as part of their consideration of applications for both new and renewed authorizations under Section 702. Judge Hogan took this step in his 2016 opinion reauthorizing a Section 702 certification, but Congress should make such review a statutory requirement of the certification process. In other words, the certification process should be amended to require the executive branch to describe, and the FISC to review, past compliance incidents within the same or related programs, both to provide a means of ensuring that these incidents are accounted for in subsequent minimization procedures, and, where appropriate, to protect against continued acquisition if such compliance problems have not been resolved.

Third, the suppression remedy for use of unlawfully acquired FISA or FISA-derived information should be expanded explicitly to require the suppression of information obtained or used in any manner that violates the applicable minimization requirements.[78] To give this provision meaning, Congress should require the executive branch to provide a criminal defendant's cleared counsel access to the minimization requirements and to information relevant to assessing compliance as part of any non-frivolous motion to suppress.

Conclusion

The 2017 debate over the reauthorization of Section 702 is – or, at least, ought to be – a pivotal moment for the relationship between incidental foreign intelligence surveillance and the Fourth Amendment. As we have argued, we believe both that courts will increasingly conclude that the Fourth Amendment applies to such government searches and that the reasonableness of the surveillance depends in part on how incidentally collected data is handled. Assuming this to be the case, the more Congress does to ensure both the existence of, and the government's compliance with, robust minimization requirements, including appropriate limits on law enforcement access, the more likely it will be that incidental collection under these programs would – and, in our view, *should* – survive a constitutional challenge.

The reforms we propose here are in many ways quite modest. Specifically, the reforms would require individualized suspicion before law enforcement could access information about U.S.-persons contained in intelligence databases; set additional protections with respect to the FBI accessing of U.S. persons communications content; increase consistency across the various agencies' approach to minimization and facilitate oversight and compliance by mandating judicial review of actual practices and imposing a statutory suppression remedy for compliance breaches. Most of the recommended reforms will require little to change in government practice – so long as the executive branch really is honoring the minimization requirements in the ways it has publicly described. The most significant proposed change is a required warrant based on probable

[78] The statute permits suppression if the "the surveillance was not made in conformity with an order of authorization or approval." 50 U.S.C. § 1806(e)(2) (2012). This provision should be amended explicitly to authorize suppression based on the failure to comply with applicable minimization rules.

cause for FBI accessing of U.S. persons' communications content, albeit with emergency exceptions built in. We think this is necessary to ensure that the existence of vast intelligence databases is not used as an end run around the otherwise applicable rules governing law enforcement searches of American's data and thereby protect the values and interests the Fourth Amendment is meant to serve. Not only do these reforms make good policy sense, but we also think that they (or equivalent protections) should be deemed constitutional requirements, necessary in order to satisfy the requirements of the Fourth Amendment.