University of Richmond Law Review

Volume 51
Issue 3 *National Security in the Information Age: Are We Heading Toward Big Brother? Symposium Issue 2017*

Article 4

3-1-2017

Next Generation Foreign Intelligence Surveillance Law: Renewing 702

William C. Banks
Syracuse University College of Law

NEXT GENERATION FOREIGN INTELLIGENCE SURVEILLANCE LAW: RENEWING 702

William C. Banks *

Sometime before the end of 2017, Congress has to decide whether and then on what basis to renew the FISA Amendments Act ("FAA"),[1] a cornerstone authority for foreign intelligence surveillance that sunsets at the end of December 2017. The Privacy and Civil Liberties Oversight Board ("PCLOB") reported in 2015 that more than one quarter of the National Security Agency (the "NSA") reports on terrorist activities are derived, in whole or in part, from surveillance authorized by section 702 of the FAA, and that the percentage has increased every year since the enactment of the FAA.[2] Although the bulk warrantless collection of communications content enabled by the FAA was viewed as a scandalous overreach when the Bush Administration's then-secret program's existence was revealed by the *New York Times* in December 2005,[3] Congress approved substantially the same program on a temporary basis in 2007.[4] Congress codified it in 2008,[5] extended it in 2012,[6] and is almost certain to renew it next year.

---

* Board of Advisers Distinguished Professor, Syracuse University College of Law; Director, Institute for National Security and Counterterrorism; Professor, Public and International Affairs, Maxwell School of Citizenship & Public Affairs, Syracuse University. The author thanks Taylor Henry, Syracuse University College of Law, J.D. 2018, for excellent research assistance.

1. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. §§ 1881–1881g (2012 & Supp. 2015)).

2. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 10 (2014) [hereinafter PCLOB 702 REPORT], https://www.pclob.gov/library/702-Report.pdf.

3. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html?_r=0.

4. Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

5. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

6. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631 (codified at 50 U.S.C. 1801 (2012 & Supp. 2015)).

My objectives in this article are to explain how and why the FAA and its authorization of bulk collection of content in section 702 came about, predict the main issues that will be considered in its renewal, and recommend reforms, for consideration in 2017 and beyond, that will better assure that bulk content collection does not undermine fundamental freedoms. Finally, I will remind us that the renewal and reform of the FAA only temporarily delays the need to confront the foundational and structural flaw in FISA and foreign intelligence surveillance law in general—that technological developments make it virtually impossible, in real time, to verify the location or nationality of a surveillance target.

I. FROM RETAIL TO WHOLESALE ELECTRONIC SURVEILLANCE

The FAA is part of the Foreign Intelligence Surveillance Act ("FISA"),[7] which has authorized the means for electronic collection of foreign intelligence since 1978. For a long time FISA served the intelligence community well. The basic idea was simple. Government may conduct intrusive electronic surveillance of Americans or others lawfully in the United States without traditional probable cause to believe that they had committed a crime if it could demonstrate to a special Article III court—the Foreign Intelligence Surveillance Court ("FISC")[8]—that it had a different kind of probable cause: reason to believe that targets of surveillance were acting on behalf of foreign powers or international terrorist groups.[9]

The FISA procedures were effective in regulating surveillance of known intelligence targets.[10] Foreign intelligence collection pursuant to FISA was always limited, however. As originally structured, FISA assumed that intelligence officials knew where the target was and what facilities the target would use for his communications.[11] Being able to assert these facts in an application to the FISC enabled the government to demonstrate the re-

7. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 178 (codified at 50 U.S.C. §§ 1801–1885c (2012)).

8. *Id.* § 103(a), 92 Stat. at 1788.

9. *Id.* § 105(a), 92 Stat. at 1790.

10. *See* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1233–39 (2007) (detailing the operation of FISA between 1978 and the early 1990s) [hereinafter Banks, *Death of FISA*].

11. *See id.* at 1231–32.

quired probable cause to obtain a surveillance order.[12] Throughout this period FISA did *not* authorize intelligence collection for the purpose of *identifying* the targets of surveillance. Nor did it permit the government to collect aggregate communications traffic and then identify the surveillance target.[13] Traditional FISA envisioned case-specific surveillance, not a bulk surveillance operation, and its mechanisms were geared to specific, narrowly targeted applications.[14] FISA was also based on the recognition that persons lawfully *in* the United States have constitutional privacy and free expression rights that stand in the way of unfettered government surveillance.[15]

The explosive growth of internet-based communications eventually undermined the basic FISA plan. First, the internet broadened the scope of communications governed by FISA in unanticipated ways. It had long been the case that foreign-to-foreign communications and even foreign to domestic communications that originated outside the United States were collected for foreign intelligence purposes pursuant to more flexible standards in an executive order.[16] FISA and its more elaborate procedures were thus inapplicable to a wide swath of foreign intelligence collection. Yet over time the pervasiveness of United States telecom-switching technology meant that even foreign-to-foreign communications as well as foreign to domestic messages are often routed through the United States, making their collection subject to FISA procedures and requirements and thus more burdensome for the government.[17] Second, the basic prerequisite for applying

12. *Id.* at 1260.

13. *Id.* at 1276.

14. *Id.*

15. *See Foreign Intelligence Surveillance Act of 1978: Hearing Before the Subcomm. on Criminal Laws and Procedures of the S. Comm. on the Judiciary*, 95th Cong. 13, 23 (1977).

16. *See* Exec. Order No. 12,333, 46 Fed. Reg. 59, 941 (Dec. 4, 1981).

17. *See* William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1638–39 (2010) [hereinafter Banks, *Programmatic Surveillance*]. FISA defines "electronic surveillance" as:

> (1) the acquisition by an electronic . . . device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;
> (2) the acquisition by an electronic . . . device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs within the United States . . . ;
> (3) the intentional acquisition by an electronic . . . device of the contents of

FISA regulation—knowing the physical location of the surveillance target—became problematic. The rapid and widespread growth of web-based e-mail meant that it was often difficult to determine the location of one or both parties to a communication.[18] Further complicating matters, our domestic communications, like foreign-to-foreign communications, traverse the globe instantaneously as packets of information.[19] These packets—some containing information content and others including information about the Internet Protocol ("IP") addresses of the sender and recipient, for example—are routed for speed and efficiency and may cross multiple international borders before they reach their destination. Wholly domestic messages may thus be routed through international servers.[20] As such, targeting an individual or group for electronic surveillance at their known location and known communications facilities in the United States became a less effective means for collecting foreign intelligence.[21]

Yet, as the value of traditional location-based FISA surveillance of foreign intelligence targets identified in advance decreased, it became possible to reach those targets in other ways. Throughout the period of rapid internet growth, powerful data mining and analytic techniques enabled intelligence officials to search collected communications in bulk and then select intelligence targets from enormous electronic databases.[22] In other words, instead of the individualized FISA surveillance process—think of it as retail surveillance—officials could build toward an individual FISA application by developing leads on individuals through the use of algorithms that search millions of collected communications for indications of suspicious activities—

---

any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

(4) the installation or use of an electronic . . . device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f) (2012).

18. *See* Banks, *Programmatic Surveillance*, *supra* note 17, at 1639.

19. *Id.*

20. *Id.*

21. *Id.*

22. *Id.* at 1634.

wholesale surveillance followed by individualized surveillance target collection.[23]

The problem was that FISA did not authorize wholesale surveillance. Clearly the authorization and regulation of foreign intelligence surveillance had to be changed, but the solution was not obvious. From the beginning, FISA was designed as a compromise. The traditional protections that the Fourth Amendment affords citizens against unreasonable searches and seizures and the presumption of a warrant issued by a judge were put to one side in this special set of circumstances—including collection in pursuit of foreign intelligence where the target was reasonably believed to be a foreign power or agent of a foreign power.[24] Americans could be targeted, but only following individualized procedures tailored to finding foreign agency. The implementation of wholesale surveillance—collection of international communications content that is undeniably necessary to protect our national security—involves a distinctively different set of tradeoffs and raises a new set of legal challenges.

In addition, in enacting FISA in 1978, Congress was explicitly determined not to regulate surveillance abroad, of United States persons or others.[25] Any surveillance abroad was conducted under the President's constitutional authority, and such surveillance of American citizens as existed was limited only by executive order.[26] Years later, wholesale foreign intelligence surveillance was first implemented in secret and was hidden from Congress and the American people. Only days after 9/11, President George W. Bush ordered a program of wholesale electronic surveillance by the NSA that simply bypassed or ignored FISA procedures and requirements.[27] Code-named *Stellar Wind*, the secret NSA program collected e-mail and telephone communications of persons inside the United States where one end of the communication was outside the United States and where there were reasonable grounds to believe that a party to the international communication was affiliated with al Qaeda or a related organization.[28] Note

23. *Id.*

24. *Id.* at 1636.

25. *See* Banks, *Death of FISA*, *supra* note 10, at 1230 (explaining that in 2008 the definition of electronic surveillance excluded surveillance taking place abroad).

26. Exec. Order No. 12,333, 49 Fed. Reg. 59,941 § 2.5 (Dec. 4, 1981).

27. *See* Banks, *Death of FISA*, *supra* note 10, at 1254.

28. LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND

that no court was involved in approving targeting or reviewing targeting criteria. NSA selected the surveillance targets on its own. Although *Stellar Wind* was operating in violation of FISA (FISA states that its procedures provided the exclusive means for conducting foreign intelligence surveillance in the United States),[29] the program continued even after the *New York Times* revealed its existence in December 2005[30] and until Congress enacted a version of it in temporary legislation in 2007[31] and then as a codified part of FISA in the 2008 FISA Amendments Act.[32]

The temporary Protect America Act ("PAA") was challenged by an internet service provider ("ISP") following a directive it had received ordering it to assist in surveillance by the NSA.[33] The ISP invoked the Fourth Amendment privacy rights of its customers, and argued that the wholesale bulk collection of content authorized by the PAA could not occur without a warrant.[34] Following its 2002 decision implicitly recognizing a foreign intelligence exception to the warrant requirement in the context of retail individual FISA requests for surveillance,[35] in its 2008 *In re Directives* decision the Foreign Intelligence Surveillance Court of Review ("FISCR") formally recognized a foreign intelligence exception to the warrant requirement based on a "special needs" exception[36] that had been found in other contexts to excuse obtaining a warrant when the purpose of the governmental action went beyond routine law enforcement and the warrant process would materially interfere with the accomplishment of that purpose.[37] The FISCR agreed that acquiring foreign intelligence falls within the "special needs" exception, and that requiring a warrant would interfere with collecting important national security information in time-sensitive circumstances.[38] The court concluded by finding

---

SURVEILLANCE IN A DIGITAL AGE 18–19 (Geoffrey R. Stone ed., 2016).

29. 18 U.S.C. § 2511(2)(e)–(f) (2012).

30. Risen & Lichtblau, *supra* note 3.

31. Protect America Act of 2007, 50 U.S.C. § 1805(a)–(c) (2012).

32. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended at 50 U.S.C. §§ 1881–1881g (2012 & Supp. 2015)).

33. *In re* Directives [redacted] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1017 (FISA Ct. Rev. 2008).

34. *Id.* at 1006.

35. *In re* Sealed Case, 310 F.3d 717, 737–39 (FISA Ct. Rev. 2002).

36. In re *Directives* [redacted] *Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d at 1011–12.

37. Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995).

38. In re *Directives* [redacted] *Pursuant to Section 105B of the Foreign Intelligence*

that the collection program authorized by the PAA met Fourth Amendment reasonableness based on the importance of the government's interest and the protections against abuse contained in the PAA.[39] Under the circumstances, no prior judicial review of directives or applications for surveillance was required.[40]

In the 2008 legislation, Congress opened the collection aperture even further than the Bush administration had in *Stellar Wind*. The FAA subtitle of FISA section 702 enables the Attorney General and Director of National Intelligence ("DNI") to authorize the "targeting" (collection of content of communications) of non-United States persons "reasonably believed to be located outside the United States to acquire foreign intelligence information."[41] The FAA does not require that the targets are suspected of terrorist activities or criminal law violations. The FISC does not review individualized surveillance applications, and it does not supervise implementation of the program.[42] While the FAA does prohibit the government from "intentionally target[ing] any person known at the time of acquisition to be located in the United States,"[43] nonetheless, the government may not reliably know a target's location or identity at the time of targeting. The "reasonably believed" standard accommodates this operational challenge.[44] These uncertainties, combined with the fact that the targeted person may communicate with an innocent United States person, mean that the authorized collection may include the international or even domestic communications of United States citizens and lawful residents as an incidental by-product of foreign intelligence collection involving non-United States persons.

This so-called 702 collection works this way: the Attorney General and DNI submit a certification to the FISC listing foreign intelligence topics that will be pursued in the 702 collection. The certification also attests that acquisitions conducted under the program meet the program targeting objectives (the collection of foreign intelligence from non-United States persons reasonably

---

Surveillance Act, 551 F.3d at 1011.

39. *Id.* at 1013.

40. *Id.*

41. 50 U.S.C. § 1881a(a) (2012).

42. *Id.* § 1881a(c)(4).

43. *Id.* § 1881a(b)(1).

44. *Id.* § 1881a(a).

believed to be outside the United States through "selectors," such as e-mail addresses, phone numbers, and other communications facilities) and satisfy traditional FISA minimization procedures (to protect against dissemination and retention of incidentally collected communications contents from United States persons).[45] The FAA requires a supporting affidavit stating that the Attorney General has adopted "guidelines" to ensure that statutory procedures have been complied with, that the targeting and minimization procedures and guidelines are consistent with the Fourth Amendment, and that a significant purpose of the collection is to obtain foreign intelligence information.[46]

The FAA does not limit the government to surveillance of particular, known persons reasonably believed to be outside the United States (i.e., retail surveillance) but instead authorizes bulk collection of content within the topics certified for collection for surveillance and eventual data mining (i.e., wholesale surveillance). In addition, non-United States person targets do not have to be suspected of being an agent of a foreign power nor, for that matter, do they have to be suspected of terrorism or any national security or other criminal offense, so long as the collection of foreign intelligence is a significant purpose of the surveillance.[47] That the targets may be communicating with innocent persons inside the United States is not a barrier to surveillance.

Additional details concerning the implementation of the FAA 702 program were not available until after the Edward Snowden leaks in 2013.[48] We now know that a FISC judge approves the program features, including targeting procedures that contain a non-exclusive list of factors that the NSA may consider in assessing whether a target may possess foreign intelligence information.[49] Although the current targeting procedures remain classified, leaked 2009 targeting procedures from the NSA state that foreignness and location determinations are made based on the "totality of the circumstances," including information from leads,

45. The requirements for minimization in the review of individualized applications for FISA surveillance are codified in 50 U.S.C. §§ 1801(h), 1821(4). Both sections direct the Attorney General to promulgate detailed minimization procedures. *Id.* §§ 1801(h), 1821(4).

46. 50 U.S.C. § 1881a(g)(1–2).

47. *Id.* § 1804(a)(6)(B).

48. *New Snowden Leak Shows How the NSA Gets Away with Domestic Spying*, RT AMERICA (Aug. 8, 2013), http://www.rt.com/usa/guardian-showden-702-loophole-304/.

49. SHEDD ET AL., THE HERITAGE FOUND., NO. 3122, MAINTAINING AMERICA'S ABILITY TO COLLECT FOREIGN INTELLIGENCE: THE SECTION 702 PROGRAM 2–4 (2016).

information from agency databases that may be relevant to location, and "technical analyses" of the facility from which it expects to acquire intelligence.[50] In addition, the NSA maintains a database of phone numbers and e-mail addresses that it has reason to believe are used by United States persons and are thus off-limits.[51] NSA procedures require that the analyst examine the target's e-mail address, phone number, or other selector associated with the target and then obtain the approval of senior NSA analysts before the person may be targeted for collection.[52] NSA officials then authorize the surveillance and issue directives requesting (or, through an additional court order, compelling) communications carriers to assist with the collection.[53]

Section 702 content is received by the NSA from service providers through two programs. PRISM is the larger program, and it involves the government relying on information about a particular e-mail address, phone number, or other information about a person, linking it or him to a foreign intelligence objective.[54] That address or name becomes a "selector" and provides the basis for sifting through vast quantities of collected content.[55] The Attorney General and DNI certify the selector as relating to a non-United States person who is reasonably believed to be outside the United States and in possession of foreign intelligence.[56] The NSA then sends a query about that selector to an ISP, which in turn hands over to the government any communications that were sent to or from the selector.[57] The NSA receives the data and may make portions available to the CIA and FBI, subject to minimization, reviewed below.[58] Think of PRISM as downstream collection. United

50. PROCEDURES USED BY THE NATIONAL SECURITY AGENCY FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 1 (2009) [hereinafter NSA 2009 TARGETING PROCEDURES], https://s3.amazonaws.com/s3.documentcloud.org/documents/716665/exhibit-a.pdf; Benjamin Wittes, *The Minimization and Targeting Procedures: An Analysis*, LAWFARE (June 23, 2013), https://lawfareblog.com/minimization-and-targeting-procedures-analysis.

51. NSA 2009 TARGETING PROCEDURES, *supra* note 50, at 3; Wittes, *supra* note 50.

52. NSA 2009 TARGETING PROCEDURES, *supra* note 50, at 3.

53. PCLOB 702 REPORT, *supra* note 2, at 33, 35

54. *Id.* at 33.

55. *Id.*

56. 50 U.S.C. § 1881a(e) (2012).

57. PCLOB 702 REPORT, *supra* note 2, at 34.

58. *Id.*

States persons (citizens and lawfully resident aliens) are subject to surveillance in downstream collection whenever they talk or correspond with foreign targets.

About 10 percent of 702 collection occurs through so-called "upstream" collection. In contrast to the PRISM program, upstream surveillance is conducted directly by the NSA and involves bulk interception, copying, and searching of international internet communications.[59] These e-mails and web-browsing traffic travel through internet hubs between sender and receiver on the internet "backbone"—at switching stations, routers, and high-capacity cables owned by major telecoms—while those communications are in transit and before they come to rest with an ISP.[60] In upstream collection, NSA tasks or searches using keyword selectors such as e-mail addresses, phone numbers, or other identifiers associated with targets. If a given stream of internet packets contains the selector, NSA will preserve and store for later use the entire transaction of which the selector was a part.[61] Employing the broadest possible selector, NSA can search the contents of the hundreds of millions of annual communications for a match with tens of thousands of foreign intelligence-related search terms that are on the government list.[62]

One unique aspect of the way NSA conducts upstream collection involves an "about" communication, where the selector of a targeted person is found within a communication, but the targeted person is not a participant.[63] In other words, the communication is not to or from the targeted person, but may be "about" him, or mention him in some way. Similarly, some internet transactions contain multiple discreet communications ("MCTs"). If any communication within a MCT or "about" communication involves a selector, the entire transaction is collected.[64] Through this indirect targeting, there is an even greater likelihood that communications of United States persons will be collected.[65]

Upstream collection is a virtual dragnet, working backwards toward targeted collection. In upstream collection, NSA comput-

59. *Id.* at 35.
60. *Id.* at 37.
61. *See id.* at 37; DONOHUE, *supra* note 28, at 60.
62. PCLOB 702 REPORT, *supra* note 2, at 37.
63. *Id.*
64. *Id.* at 41.
65. *Id.*

ers scan the contents of all of the communications that pass through the internet transit point and then justify the collection based on the presence of one or more selectors after the scan is complete.[66] Viewing 702 collection in the aggregate, considerable incidental acquisition of the communications of United States persons inside the United States inevitably occurs due to the difficulty of ascertaining a target's location, because targets abroad may communicate with innocent United States persons, and because upstream collection captures such a broad swath of internet communications.

II. MINIMIZATION

Once their communications are collected incidentally, intelligence agencies are supposed to protect the privacy and civil liberties of United States persons through minimization procedures that control the retention, dissemination, and use of nonpublic, non-consenting United States person information.[67] Minimization procedures have been part of FISA since 1978 and are unique to each collection agency and program.[68] At a high level of generality, the 702 minimization procedures are designed to balance privacy and national security objectives of the collecting agency in setting standards for acquisition and retention of United States person information. They also control use and dissemination of collected information about United States persons.[69] For example, NSA minimization procedures require that any wholly domestic communications that have been collected must be promptly destroyed unless the NSA Director determines that the sender *or* recipient has been lawfully targeted, and that the communication is reasonably believed to contain: significant foreign intelligence information, evidence of a crime; information indicating an imminent threat of serious harm to life or property; or technical information for signals exploitation.[70] Considerable United States per-

66. David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y 377, 394 (2016) (quoting DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 17.5 (2d ed. 2012) (Supp. 2016)).

67. 50 U.S.C. § 1801(h) (2012).

68. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 50 U.S.C. § 1801h (codified as amended in scattered sections of 50 U.S.C.).

69. PCLOB 702 REPORT, *supra* note 2, at 7–8.

70. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NATIONAL SECURITY AGENCY IN CONNECTION WITH ACQUISITIONS OF FOREIGN

son information may thus be retained even after complying with the standards.

Internally, the minimization procedures serve as controls on how analysts inside the agency can access and use the collected information. Once collected information is held by the NSA, an analyst can analyze and query the information, similar to the process of conducting an internet search.[71] Minimization procedures are supposed to assure that querying does not violate privacy or other protected freedoms.[72] In general, NSA procedures require that all telephone and internet transactions obtained under 702 be destroyed within five years if not subject to immediate destruction when collected.[73] Transactions may be retained beyond the five year period if the NSA determines that the information is essential for maintaining technical databases, is evidence of a crime, or otherwise could be disseminated under NSA rules.[74]

NSA minimization procedures were amended in 2011 after the FISC ruled that proposed NSA minimization procedures implementing 702 collection were insufficient on statutory and constitutional grounds.[75] Judge John Bates found that the proposed minimization procedures focused "almost exclusively" on the information sought to be used by the analyst and not much on the aggregate content collected.[76] Because the default rule was that all collected information could be retained for five years, content known to be unrelated to a target, including domestic communications, could be retained without the agency taking steps to minimize retention. Applying the Fourth Amendment, Judge Bates accepted application of the foreign intelligence exception, but found that the minimization procedures as proposed failed the reasonableness standard.[77] Revised procedures approved by the

---

INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 12–13 (2015) [hereinafter NSA 2015 MINIMIZATION PROCEDURES], https://www.dni.gov/files/documents/2015NSAMinimization Procedures_Redacted.pdf.

71. PCLOB 702 REPORT, *supra* note 2, at 8.

72. *See id.*

73. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 7.

74. *See id.* at 13–15.

75. [Redacted], 2011 U.S. Dist. LEXIS 157706, at *1, *110–12 (FISA Ct., Oct. 3, 2011).

76. *Id.* at *81–82, *109.

77. *Id.* at *109–11.

FISC on November 30, 2011 required that the NSA segregate the collected content most likely to contain unrelated or wholly domestic communications, require special handling and markings for communications that could not be segregated, and reduced the upstream collection retention period from five years to two.[78]

More recently, the 2015 minimization procedures for the NSA, Central Intelligence Agencies ("CIA"), Federal Bureau of Investigation ("FBI"), and National Counterrorism Center ("NCTC") were partially declassified and released in August 2016.[79] The NSA procedures treat United States person communications as "foreign communications" subject to retention, use, and dissemination if one participant to the collected communication is outside the United States.[80] In addition, United States person information is minimized only when the communications in question are known to belong to or concern United States persons.[81] In other words, collected information is presumed to be foreign communications, and much United States person content is not minimized.[82]

The 2015 NSA minimization procedures indicate that analysts may not use United States person identifiers to query 702 up-

78. [Redacted], 2011 U.S. Dist. LEXIS 157705, at *5–6, *9 (FISA Ct., Nov. 30, 2011).

79. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 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 (2015) [hereinafter CIA 2015 MINIMIZATION PROCEDURES], https://www.dni.gov/files/documents/2015CIAMinimizationProcedures_Redacted.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, 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 (2015) [hereinafter FBI 2015 MINIMIZATION PROCEDURES], https://www.dni.gov/files/documents/2015FBIMinimization_Procedures.pdf; OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, MINIMIZATION PROCEDURES USED BY THE NATIONAL COUNTERTERRORISM CENTER IN CONNECTION WITH INFORMATION ACQUIRED BY THE FEDERAL BUREAU OF INVESTIGATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED (2005) [hereinafter NCTC 2015 MINIMIZATION PROCEDURES], https://www.dni.gov/files/documents/2015NCTCMinimizationProcedures_Redacted.pdf; NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70.

80. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 1–2.

81. *See id.* at 3.

82. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 347 (2015) [hereinafter Daskal, *The Un-Territoriality of Data*]; Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 165 (2015); PCLOB 702 REPORT, *supra* note 2, at 129 ("[A]lthough a communication must be 'destroyed upon recognition' when an NSA analyst recognizes that it involves a U.S. person . . . in reality this rarely happens.").

stream collection of Internet transactions, but upstream telephone collection and downstream PRISM data may be queried using United States person identifiers if approved internally by the NSA.[83] These searches of collected communications are permitted by NSA and CIA minimization procedures, once analysts create a "statement of facts establishing that the use of any such identifier as a selection term is reasonably likely to return foreign intelligence information."[84] Note that the procedures do not require that obtaining foreign intelligence be *the* purpose of querying the data. The FBI procedures are more permissive, where agents may query 702 data for United States person information pursuant to a routine law enforcement investigation.[85] While the NSA normally redacts identifying details about the United States person in such circumstances, the receiving agency may request that the NSA remove the redaction if they legitimately require the information to pursue their investigation, for example, or if the communication is "reasonably believed to contain evidence that a crime has been, is being, or is about to be committed."[86]

III. AFTER SNOWDEN

In February 2013, the Supreme Court declined to rule on the lawfulness of 702 collection when it found that non-profit organizations that challenged the FAA soon after enactment lacked standing to sue.[87] However, at least in part due to the Snowden leaks and subsequent release of additional details about the 702 program by the government, some changes were made to 702 collection and minimization between 2014 and the present.[88] In broad strokes, the Obama administration determined to do more to protect individual liberties in its foreign intelligence surveillance activities after the Snowden leaks, and to make those activities more transparent.[89] These new trends were evidenced when President Obama promulgated Presidential Decision Directive 28

83. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 7.

84. *Id.*

85. FBI 2015 MINIMIZATION PROCEDURES, *supra* note 79, at 11, 11 n.3.

86. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 14–15.

87. Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1144, 1146, 1155 (2013).

88. *See generally* Directive on Signals Intelligence Activities, 2014 DAILY COMP. PRES. DOC. 4–5 (Jan. 17, 2014).

89. *See, e.g., id.*

("PPD-28") on January 17, 2014.[90] President Obama proclaimed that

> [a]ll persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and all persons have legitimate privacy interests in the handling of their personal information. U.S. signals intelligence activities must, therefore, include appropriate safeguards for the personal information of all individuals, regardless of the nationality of the individual to whom the information pertains or where that individual resides.[91]

Potentially, PPD-28 would lift the thumb that had long been on the scale of foreign intelligence in favor of collection. Like many such directives, however, PPD-28 states that its policies and procedures apply only "[t]o the maximum extent feasible consistent with the national security," apparently leaving it to executive officials in the Intelligence Community to determine how to treat "all persons . . . with dignity and respect."[92] Similarly, PPD-28 extends minimization procedures to include non-United States persons except to the extent that dissemination or retention of comparable information concerning United States persons could occur.[93] So understood, United States policy remains that foreign intelligence information may be retained or disseminated, whatever its source.

The Obama administration also committed to introduce outside lawyer advocates in the judicial process of the FISC in settings unrelated to 702 collection, and to enhance United States person protections through more stringent minimization procedures for information collected under section 702.[94] Meanwhile, as the United States was moving toward limiting surveillance and imbuing its programs with greater openness, the Europeans were, by and large, moving in the opposite direction. Buffeted by the rise of ISIS, concerns about foreign terrorist fighters, and significant terrorist attacks in France and Belgium, surveillance authorities expanded in France, Germany, Austria, the Netherlands, Finland, and the United Kingdom.[95]

---

90. *Id.*

91. *Id.*

92. *Id.*

93. *Id.* at 5.

94. Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 5–6 (Jan. 17, 2014).

95. Kris, *supra* note 66, at 390.

On this side of the Atlantic, the PCLOB, an independent, bipartisan agency within the executive branch created by Congress in 2007,[96] began in July 2013 to examine the 702 program, among other aspects of intelligence collection impacting privacy and civil liberties.[97] After months of meetings with intelligence officials, public hearings, and meetings with congressional staff and public interest groups the PCLOB issued a report on 702 in 2014 which found that the program was "authorized by Congress, reasonable under the Fourth Amendment, and an extremely valuable and effective intelligence tool."[98] The PCLOB so concluded even though "the applicable rules potentially allow a great deal of private information about U.S. persons to be acquired by the government."[99] Nonetheless, the PCLOB made a series of recommendations which it asserted would better protect privacy and civil liberties without jeopardizing the success of the 702 program.[100] Recommendations focused on transparency (making minimization procedures public), documenting the justifications for querying using United States person identifiers, and limiting some types of collection.[101] Between mid-2014 and early 2016, according to PCLOB Recommendations Assessment Reports, ten recommendations have been implemented in whole or in part.[102]

Meanwhile, a provision in FISA that requires the Justice Department to notify criminal defendants that it intends to enter into evidence or otherwise use or disclose information "derived from" FISA-derived electronic surveillance[103] has resulted in several suppression motions by defendants who argue that any such evidence in their cases was unlawfully acquired because of the unconstitutionality of 702.[104] In addition to the Fourth Amend-

96. *About the Board*, PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, https://www.pclob.gov/about-us.html (last visited Feb. 13, 2017).

97. PCLOB 702 REPORT *supra* note 2, at 1.

98. *Id.* at 161.

99. *Id.* at 11.

100. *See id.* at 134–48.

101. *Id.*

102. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., FACT SHEET: PCLOB RECOMMENDATIONS IMPLEMENTED BY THE GOVERNMENT (2016) [hereinafter PCLOB FACT SHEET].

103. 50 U.S.C. §§ 1806(c), 1881a(e) (2012).

104. *See* United States v. Hasbajrami, No. 11-cr-623, 2016 U.S. Dist. LEXIS 30613, at *1, *22 (E.D.N.Y. Feb. 18, 2016); United States v. Muhtorov, No. 12-cr-00033, 2015 U.S. Dist. LEXIS 184312, at *1–3 (D. Colo. Nov. 19, 2015); United States v. Mohamud, No. 3:10-cr-00475, 2014 U.S. Dist. LEXIS 85452, at *10, *30 (D. Or. June 24, 2014), *aff'd*, 843 F.3d 420 (9th Cir. 2016). The attorney for Yahya Farooq Mohammad and Aws Mohammed

ment privacy challenge, the criminal defendants allege that the arrangement authorized by Congress in 702 violates Article III of the Constitution because the FISC is required to evaluate the lawfulness of the targeting and minimization procedures in the abstract, without regard to any specific surveillance operation or action. In effect, the argument goes, the FISC is rendering advisory opinions rather than adjudicating cases.[105] In the challenges decided so far, the criminal defendants' motions to suppress have been denied.[106] The courts have held that 702 does not violate Article III because judicial decisions have upheld federal courts performing other non-adjudicative functions in various settings, akin to those required by the FAA.[107] On the Fourth Amendment, the courts have followed the FISCR decisions, sometimes applying the foreign intelligence exception and/or have found the 702 procedures reasonable.[108]

In December 2016, the Ninth Circuit Court of Appeals rejected a challenge to the constitutionality of 702 surveillance on appeal of a criminal conviction based on "derived from" 702 evidence and concluded that the government did not need a warrant when it incidentally collected some e-mails of United States citizen Mohamed Osman Mohamud in the course of targeting a non-citizen located outside the United States in pursuit of foreign intelligence.[109] The decision is noteworthy for a few reasons. First, the court expressly limited its decision to the particular facts before it, including that the collection was part of the PRISM program, not upstream collection.[110] Nor had the government queried Mohamud's e-mails after storage in a database.[111] The Ninth Circuit recognized that its analysis of the Fourth Amendment may be different in upstream collection or following a database search. Se-

---

Younis Al-Jayab, who both have cases currently pending in federal court, said that he will be moving to suppress the FISA-derived evidence. Charlie Savage, *Warrantless Surveillance in Terror Case Raises Constitutional Challenge*, N.Y. TIMES (Apr. 26, 2016), http://www.nytimes.com/2016/04/27/us/warrantless-surveillance-in-terror-case-raises-constitutional-challenge.html?_r=1.

105. *See, e.g.*, *Muhtorov*, 2015 U.S. Dist. LEXIS 184312, at *21–22, *34.

106. *Hasbajrami*, 2016 U.S. Dist. LEXIS 30613, at *46; *Muhtorov*, 2015 U.S. Dist. LEXIS 184312, at *5; *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *12.

107. *See, e.g.*, *Muhtorov*, 2015 U.S. Dist. LEXIS 184312, at *22–25.

108. *Hasbajrami*, 2016 U.S. Dist. LEXIS 30613, at *7–9, *36–40; *Muhtorov*, 2015 U.S. Dist. LEXIS 184312, at *10–11, *27–35; *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *32–53.

109. United States v. Mohamud, 843 F.3d 420, 438–41, 444 (9th Cir. 2016).

110. *Id.* at 438.

111. *Id.*

cond, the court found the scope of incidental collection "troubling,"[112] and emphasized the importance of effective minimization, particularly when the FAA does not provide for judicial review of the implementation of 702 orders.[113] Nonetheless, the court found that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful."[114]

The court also acknowledged that Mohamud had some Fourth Amendment privacy expectations in his sent and received e-mails.[115] The defense and amici argued that the collection of Mohamud's e-mails was not truly incidental "because the monitoring of communications between foreign targets and U.S. persons was specifically contemplated and to some degree desired."[116] However, to the extent collection on United States persons was an intended purpose, the government would have engaged in forbidden reverse targeting.[117] In short, if there had been any suspicion that Mohamud was targeted using 702 procedures as an end-run of traditional FISA requirements, the result would have unconstitutional bootstrapping and the court would have suppressed the evidence in his criminal case.[118]

Given the bipartisan support for the program in 2008 and the PCLOB bottom line that the program has been effective and lawful, there is little doubt that Congress will renew the FAA before it expires in December 2017. Less clear is the extent to which Congress and the new administration will give serious consideration to a few important reforms that will improve the 702 programs and enhance the privacy of persons and the transparency of the program implementation.

---

112. *Id.* at 440.

113. *Id.* at 440–43.

114. *Id.* at 439 (quoting *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008)).

115. *Id.* at 442.

116. *Id.* at 440.

117. *See id.* at 443.

118. *See id.* at 444; *see also* Jennifer Daskal, *Ninth Circuit Upholds 702 Foreign Intelligence Surveillance, But Leaves Open Future Challenges*, JUST SECURITY (Dec. 6, 2016), https://www.justsecurity.org/35276/section-702-foreign-surveillance-ruling-ninth-circuit/ (criticizing the court for unanswered questions in its opinion). *But see* April Doss, *Why the 9th Circuit Was Right in Mohamed Mohamud, and a Startling Thing It May Have Gotten Wrong*, LAWFARE (Dec. 9, 2016), https://www.lawfareblog.com/why-9th-circuit-was-right-mohamed-mohamud-and-startling-thing-it-may-have-gotten-wrong (arguing that the Ninth Circuit did reach the correct conclusion).

IV. RENEWAL ISSUES

It is difficult to evaluate independently the success or importance of intelligence tools such as 702 collection. For the most part, the government cannot realistically release information about thwarted plots or surreptitiously apprehended fugitives in the foreign intelligence realm due to the secrecy of the surveillance, the sometimes-ongoing nature of the investigations, and the value to our adversaries of the details of the collection techniques. For the most part, only when a plot is disrupted or an accused terrorist is captured and the alleged perpetrators are identified does the United States reveal the role of intelligence collection and 702 programs in those operations. In general, the Office of the Director of National Intelligence ("ODNI") has asserted and the PCLOB has agreed that the 702 program has been of considerable value in learning about the membership and activities of terrorist organizations, and to discover previously unknown terrorist operatives and their plots.[119] The 702 program also supports members of the intelligence community generally to understand terrorist networks, the individuals who affiliate with them, and coverage of targets as they switch modes of communication.[120]

Technological change has dramatically altered foreign intelligence collection tradecraft. Within the modern era of electronic surveillance, technical capabilities that now drive collection were

119. PCLOB 702 REPORT, *supra* note 2, at 104, 107.

120. *Id.* at 108. In the case of Khalid Ouazzani, the NSA was unaware of his identity until after conducting 702 surveillance of an e-mail address used by an extremist in Yemen. From this surveillance, the NSA discovered a connection between the extremist and an unknown person in Missouri. The FBI identified the unknown person as Khalid Ouazzani, and subsequently discovered that Ouazzani had connections to United States-based al-Qaeda associates who had been part of an abandoned plot to bomb the New York Stock Exchange. Ouazzani eventually pled guilty on material support charges. *Id.* at 108–09. Section 702 surveillance also helped the government to identify Najibullah Zazi. *Id.* In September 2009, the NSA used 702 surveillance to monitor the e-mail address of an al-Qaeda courier in Pakistan. *Id.* at 109. The NSA intercepted e-mails sent to that address from an unknown individual in the United States. *Id.* The sender was seeking advice on how to manufacture explosives. *Id.* After the FBI identified Zazi, it tracked him leaving for New York City, where he was planning to detonate explosives on the subway in Manhattan. Zazi was arrested, and pled guilty. *Id.* In its report, the PCLOB commented that it is possible that traditional FISA might have produced the same intelligence and results. *Id.*; *see also* Bailey Cahall et al., *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, NEW AM. (Jan. 13, 2014), https://www.newamerica.org/internationalsecurity/policypapers/do-nsas-bulk-surveillance-programs-stop-terrorists (concluding that 702 surveillance played a role in only 4.4% of cases in a sample of 225 terrorists, or would-be terrorists, in comparison to the use of traditional FISA in 21% of cases).

unheard of even twenty years ago. While retail surveillance still has an important place in foreign intelligence collection, the sheer power of bulk collection and subsequent filtering with algorithms and related analytic techniques has made wholesale surveillance an integral part of contemporary foreign intelligence collection. In view of the profound differences between the 702 program and the legal regime that applies to individualized foreign intelligence surveillance, it is simply not realistic to superimpose traditional Fourth Amendment criminal law enforcement procedures and a pre-collection judicial warrant requirement on bulk foreign intelligence collection at this initial screening phase.

There is little to gain in rehashing whether there is a foreign intelligence or special needs exception to the warrant requirement. Electronic surveillance, which is intended to protect national security by collecting foreign intelligence in bulk, does not typically implicate criminal law sanctions or our historical fears of overreaching by law enforcement. The objective of the surveillance is to keep tabs on foreign adversaries, sometimes to learn about terrorist plans before they become operational. Meeting the law enforcement probable cause standard and insisting on the issuance of a warrant by a judge is not well suited to the 702 context. Nor can the traditional FISA process, with individualized consideration of foreign agency, be easily adapted to bulk collection. (The fact that evidence of criminal activity may be collected during what was otherwise a foreign intelligence investigation, and that foreign intelligence collection is only required to be "a significant purpose"[121] of a FISA investigation raise different Fourth Amendment issues, mostly unrelated to 702.)[122]

Just as technology has dramatically altered intelligence collection, so has it transformed conceptions of individual privacy. New

121. 50 U.S.C. § 1881a(g)(2)(A)(v) (2012).

122. *See* Banks, *Death of FISA*, *supra* note 10, at 1250–53; William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 MIAMI L. REV. 1147, 1175–76 (2003). I say "mostly unrelated" because the fact that the FBI has access to some 702 content raises concerns about the open-endedness of FBI minimization procedures that permit the use of United States person information collected under 702 programs to be used in prosecution. *See* FBI 2015 MINIMIZATION PROCEDURES, *supra* note 79, at 20 ("The FBI may disclose FISA-acquired information . . . to federal prosecutors and others working at their direction, for all lawful foreign intelligence and law enforcement purposes, including in order to enable the prosecutors to determine whether the information: (1) is evidence of a crime, (2) contains exculpatory or impeachment information; or (3) is otherwise discoverable under the Constitution or applicable federal law.").

technologies have expanded the categories of content—including digitized social networks and locational data—and digitization makes personal ideas, beliefs, and thoughts available to the government through the power of data analytics.[123] Whether the predicate for individual constitutional privacy protection remains the "reasonable expectation of privacy" standard evolved from *Katz v. United States*[124] or something else,[125] the overarching Fourth Amendment principle is reasonableness and it remains the touchstone for assuring that 702 adequately protects individuals. In the foreign intelligence and national security setting, where the purpose of an investigation is to collect foreign intelligence in bulk and then filter with keyword selectors toward identifying targets for retail surveillance for foreign intelligence purposes, our national security legal framework requires an agile, nuanced attention to the specific characteristics and challenges of foreign intelligence surveillance in the twenty-first century.

We know that non-United States citizens who lack a substantial connection to the United States are not protected by the Fourth Amendment.[126] The promises made to non-United States persons by President Obama in his 2014 PPD-28 are policy prescriptions, not legally binding commitments. For United States persons, inadvertent 702 collection does burden privacy, no doubt. It is not yet known how much content from how many United States persons is collected or queried in the aggregate under 702, and reasonable people can disagree about the nature and severity of the privacy intrusions. In any case, the realistic constitutional position is to accept the inevitability of bulk collection for foreign intelligence purposes and focus instead on the *uses* of what is collected. Recognizing the certainty of continuing bulk collection of content, sometimes inadvertently including the communications of United States persons does not mean that the surveillance should be unregulated. Indeed, Congress or the ODNI could impose additional administrative controls on the development of the certifications and eventual directives that drive most 702 collection, such as requiring agency staff to attest to the likelihood that

123. *See generally Data, Data Everywhere*, THE ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443 (discussing the massive rise in the amount of data and the concurrent rise in the field of data analytics).

124. 389 U.S. 347, 360–61 (1967) (Harlan, J., concurring).

125. *See* Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 301–02 (2015).

126. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

foreign intelligence will be obtained from the targeted source, or that the information cannot be obtained through a less intrusive means.[127]

Is there collection overbreadth? An October 2011 opinion of the FISC by Judge John Bates, that was declassified in response to a Freedom of Information Act ("FOIA") lawsuit, indicated that by 2011 the NSA was acquiring over 250 million internet transactions annually through 702 collection, more than 90 percent from downstream PRISM collection.[128] Judge Bates noted that, due to the scale of upstream collection, tens of thousands of entirely domestic communications may be collected each year.[129] Based on the information leaked by Snowden, the *Washington Post* reviewed PRISM and upstream collection and estimated that the ratio of targets to United States persons whose information is incidentally collected is about 9:1.[130]

In response to the Snowden leaks and recommendations from the PCLOB, among others, to add transparency to the 702 program, the ODNI and FISC have released some data on the volume and types of communications collected.[131] No data has been released regarding the number of telephone communications acquired where one caller is in the United States, the number of internet communications acquired through upstream collection that originate or terminate in the United States, or the number of communications of or concerning United States persons that the NSA positively identifies. Instead, ODNI reported that there were

127. *See* Banks, *Programmatic Surveillance*, *supra* note 17, at 1656–58; *see also* Adam Klein, Michèle Flournoy & Richard Fontaine, *Surveillance Policy: A Pragmatic Agenda for 2017 and Beyond*, CTR. FOR A NEW AM. SECURITY 1, 36 (Dec. 12, 2016) [hereinafter Klein et al., *Surveillance Policy*].

128. *See* [Redacted], 2011 U.S. Dist. LEXIS 157706, at *36, *36 n.24 (FISA Ct., Oct. 3, 2011).

129. *Id.* at *40.

130. Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html?utm_term=.6b6f50db7485.

131. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2015 5 (2016) [hereinafter ODNI 2015 STATISTICAL REPORT], https://www.dni.gov/files/icotr/ODNI%20CY15%20Statistical%20Transparency%20Report.pdf.

94,368 estimated targets affected in 2015,[132] an increase of about 5000 from 2013.[133] In response to requests for information on how many queries have been performed on collected data that employ United States person identifiers, ODNI reported 4672 queries of content acquired under 702 authority in calendar year 2015, not counting queries from the FBI.[134] In the same period, there were 23,800 queries of metadata, again excluding the FBI.[135]

Is over-collection in 702 encouraged by the breadth and open-endedness of permissible statutory objectives, requiring only that the target be "reasonably believed to be located outside the United States" and that the purpose is "to acquire foreign intelligence information?"[136] As suggested above, Congress or the ODNI, in pursuit of these objectives, could impose stiffer administrative controls on the collectors and thereby potentially shrink over-collection to some extent. Or Congress could change "reasonably believed" to "known" or its equivalent. The subjectivity of the standard underscores the serious operational challenges in making real time judgments about a target's location.

The assumptions made by NSA analysts in targeting—that persons outside the United States or in an unknown location are foreign, and that targets not known to be inside the United States are presumed to be located outside our borders—while accurate in general, are inevitably prone to produce considerable collection of United States persons. In downstream PRISM collection, the NSA minimization procedures presume that a target is located outside our borders unless he is known to be inside the United States.[137] Because the NSA cannot always know the location of a potential surveillance target or his nationality in real time (a cell phone number does not reveal location and possession of a United States cell number does not necessarily indicate the nationality of the owner), the assumption inevitably leads to an over-collection

132. *Id.*

133. *See* OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: ANNUAL STATISTICS FOR CALENDAR YEAR 2013 (2014), https://www.dni.gov/files/tp/National_Security_Authorities_Transparency_Report_CY2013.pdf.

134. ODNI 2015 STATISTICAL REPORT, *supra* note 131, at 5.

135. *Id.*; Letter from Deirdre M. Walsh, Dir. of Legislative Affairs, Office of the Dir. of Nat'l Intelligence, to the Hon. Ron Wyden, U.S. Senate, 1, 3 (June 27, 2014), https://www.wyden.senate.gov/download/?id=184D62F9-4F43-42D2-9841-144BA796C3D3&download=1.

136. 50 U.S.C. § 1881a(a) (2012).

137. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 3.

on United States persons. At the same time, the NSA can make these targeting decisions the way they do because the FAA and NSA procedures do not prescribe criteria for deciding foreignness. Because a phone number or e-mail address does not necessarily reveal location or identity of the user, targeting must be tied to the presumed geolocation of the device and, if possible, other knowledge about the owner or user of the device. Despite these uncertainties, assumptions made by the NSA allow targeting under 702, rather than under the stricter retail collection provisions of FISA and the FAA.

It is unlikely that Congress will have an appetite in the 702 renewal for deliberating the nuances of how the NSA determines foreignness or the location of surveillance targets in its bulk collection. However, improved administrative controls may lessen the subjectivity of targeting and the incidence of over-collection. The FAA does now, and certainly will in the future, require the Attorney General and DNI to adopt targeting procedures in furtherance of the statutory objectives and to certify their lawfulness to the FISC.[138] The declassified NSA 2009 Targeting Procedures[139] included a non-exclusive list of factors that the NSA could consider in assessing whether a target is likely to have foreign intelligence information, including where the United States intelligence community "reasonably believe[s]" the target is communicating or has communicated with someone "associated with" a foreign power or territory.[140] In 2014, the PCLOB urged the NSA to revise its targeting procedures to

> specify criteria for determining the expected foreign intelligence value of a particular target, and . . . require a written explanation of the basis for that determination sufficient to demonstrate that the targeting of each selector is likely to return foreign intelligence information relevant to the subject of one of the certifications approved by the FISA court.[141]

Both of these reforms would add some measure of accountability to NSA foreignness and foreign intelligence determinations. Improved targeting procedures could provide additional guidance to NSA analysts, and a written explanation would assist the analysts in explaining their targeting choices and provide guidance

138. 50 U.S.C. § 1881a(d)(1) (2012).
139. NSA 2009 TARGETING PROCEDURES, *supra* note 50.
140. *Id.* at 4–5.
141. PCLOB 702 REPORT, *supra* note 2, at 11.

for oversight after the fact. Although the targeting procedures, remain classified, the PCLOB reported in February 2016 that revised targeting procedures, that included the written explanation of the foreign intelligence value, were approved by the FISC,[142] and a publicly released FISC opinion by Judge Hogan confirmed that the targeting procedures require that the foreign intelligence purpose of the targeting must be "'particularized and fact-based,'" and that NSA analysts must "'provide a written explanation of the basis for their assessment.'"[143] The PCLOB reported, however, that the revised targeting procedures do not "add or clarify substantive criteria, for determining the expected foreign intelligence value of a particular target."[144] Adding substantive criteria to spell out expected foreign intelligence value, in writing, would improve the efficacy and trustworthiness of NSA decision making. Despite repeated requests, ODNI has not declassified the 702 targeting procedures because they, "as well as an associated list of foreign powers subject to targeting . . . explain in depth how the Intelligence Community decides whether to target a person. . . ."[145] These security concerns are likely to keep the procedures classified. Their sensitivity should not stand in the way of reforms to make the administrative process more accountable.

Regarding the smaller but controversial upstream collection program, there is no dispute that upstream collection of e-mails occurs by first copying all internet traffic that transits certain parts of the internet backbone, storing it briefly, followed by an electronic scan of the contents of those e-mails to determine which communications contain the selectors that have been determined in advance to produce foreign intelligence. Then those communications are retrieved from what was collected and stored while the rest is destroyed. Even though internet transactions are

142. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BD., RECOMMENDATIONS ASSESSMENT REPORT 14–15 (2016), https://www.pclob.gov/library/Recommendations_Assessment_Report_20160205.pdf.

143. [Redacted], slip op. at 11 (FISA Ct., Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf (quoting NSA 2009 TARGETING PROCEDURES, *supra* note 50, at 4.).

144. PCLOB FACT SHEET, *supra* note 102, at 15.

145. Office of the Dir. of Nat'l Intelligence, *Statement by the Office of the Director of National Intelligence and the Department of Justice on the Declassification of Documents Related to Section 702 of the Foreign Intelligence Surveillance Act*, IC ON THE RECORD (Sept. 29, 2015), https://icontherecord.tumblr.com/post/130138039058/statement-by-the-office-of-the-director-of.

supposedly filtered in upstream collection using the best technology to eliminate purely domestic transactions, and then screened to capture only transactions containing a tasked selector, imperfect filters and "about" communications that are not necessarily to or from the e-mail address that was tasked lead to many communications that involve United States persons. The government acknowledges that the technical methods used to prevent acquiring domestic communications through upstream and "about" collection are imperfect.[146]

It is unlikely that most Members of Congress who voted to enact the FAA recognized the government would engage in bulk content collection with significant incidental United States person collection. Whatever the understandings in 2008, it is inevitable that some significant number of United States persons would be communicating with targets for foreign intelligence collection abroad. Those communications would be collected downstream in the PRISM program, with United States person information included. It is also true that upstream collection includes what FISC Judge Thomas Hogan characterized as "substantial quantities of information concerning United States persons."[147] If the administrative reforms mentioned above are prescribed by statute or implemented by ODNI and the NSA, what should the government do with incidentally collected United States person communications?

V. MINIMIZATION AND QUERIES

The minimization requirements that have been part of retail FISA since 1978 were not modified in the FAA in 2008 to accommodate 702 collection. The FAA simply requires that the Attorney General and DNI certify that minimization procedures have been or will be submitted for approval to the FISC.[148] However, the FISC does not review the implementation of minimization procedures or practices following 702 collection, and the FAA permits the government to retain and disseminate information relating to

146. PCLOB FACT SHEET, *supra* note 102, at 21–22.

147. [Redacted], slip op. at 27, 27 n.25 (FISA Ct., Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

148. 50 U.S.C. § 1881a(e) (2012).

United States persons so long as the government determines that it is "foreign intelligence information."[149]

Historically, minimization has served as a backstop to protect individual privacy following incidental collection of United States person information. The backstop role has been centrally important following the first several years of bulk collection pursuant to 702. Bearing in mind that 702 targets are not necessarily terrorist suspects or even wrongdoers of any kind, the baseline proposition in minimization is to protect the privacy of nonconsenting United States persons by "promptly destroy[ing]" domestic communications that were collected in pursuit of foreign intelligence.[150] At the same time, the minimization procedures for 702 must be consistent with the government's need "to obtain, produce, and disseminate foreign intelligence information," and to minimize the retention, and prohibit the dissemination, of evidence of unconsenting United States persons.[151] These oppositional commands have led to continuing uncertainty about minimization of incidental United States person data collected pursuant to 702.

Following a series of PCLOB recommendations, the minimization procedures for the NSA, CIA, FBI, and NCTC were partially declassified in August 2016.[152] NSA minimization procedures prohibit the dissemination of information about United States persons in any NSA report unless that information "is necessary to understand foreign intelligence information or assess its importance,"[153] contains evidence of a crime, or indicates a threat of death or serious bodily injury.[154] If one of those conditions applies, NSA will nonetheless mask the information, including no more United States person information than is necessary.[155] Recipient

149. *Id.* § 1881a(d)(2), (e)(2); NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 12.

150. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 12. Neither FBI nor CIA have similar purging requirements. PCLOB 702 REPORT, *supra* note 2, at 62.

151. 50 U.S.C. § 1801(h)(1) (2012); NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 12.

152. CIA 2015 MINIMIZATION PROCEDURES, *supra* note 79; FBI 2015 MINIMIZATION PROCEDURES, *supra* note 79; NCTC 2015 MINIMIZATION PROCEDURES, *supra* note 79; NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70.

153. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 14.

154. *Id.* at 1, 12, 15.

155. PCLOB 702 REPORT, *supra* note 2, at 64.

agencies may request identifying information about the masked United States person if doing so is "necessary to understand foreign intelligence information or assess its importance. . . ."[156]

Some dismissed the value of minimization when it was learned that the declassified procedures for the NSA, the CIA, and the FBI included a provision stating that "[n]othing in these procedures shall prohibit the retention, processing, or dissemination of information reasonably necessary to comply with specific constitutional, judicial or legislative mandates."[157] In a November 2015 opinion for the FISC, Judge Thomas Hogan supplied a narrowing construction and thus read the provision "to include only those mandates containing language that clearly and specifically requires action in contravention of an otherwise-applicable provision" of the minimization procedures.[158] So limited, the boilerplate override provisions in minimization simply restate the proposition that minimization may be changed by congressional or judicial decision. In a related context, the FISCR publicly released a decision in August 2016, *In re Certified Question of Law*,[159] deciding that FISA-authorized pen register/trap-and-trace devices (that inevitably collect content information in addition to the dialing, routing, signaling, and addressing information that are the objective of the orders) are lawful despite the over-collection *because of* minimization.[160]

One problem with 702 minimization stems from the foreignness assumptions reviewed above—unless the person whose

156. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 14–15; PCLOB 702 REPORT, *supra* note 2, at 64. Unmasking can also follow consent of the United States person, a finding that the United States person is an agent of a foreign power or is engaged in international terrorism, or a finding that the pertinent communication is reasonably believed to contain evidence of a crime. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 14.

157. Jadzia Butler & Jennifer Granick, *Correcting the Record on Section 702: A Prerequisite for Meaningful Surveillance Reform, Part II*, JUST SECURITY (Sept. 22, 2016), https://www.justsecurity.org/33111/correcting-record-section-702-prerequisite-meaningful-surveillance-reform-part-ii/ (citing NSA 2015 MINIMIZATION PROCEDURES, *supra*, note 70, at 1) ("The apparent ability of agencies to deviate from the minimization procedures based on unspecified 'mandates' undermines the anemic privacy safeguards those procedures contain. The FISC cannot ensure that the procedures meet either statutory or constitutional requirements in the face of such a vague exception.").

158. [Redacted], slip op. at 23 (FISA Ct., Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

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

160. *Id.* at 13, 24, 34–35.

communications are received is "known" to be a United States person, minimization presumes that he is foreign until there is contradictory evidence.[161] Given the difficult technological questions that surround determining location and nationality, in practice it will be difficult for domestic communications to be designated as such in many cases.[162] In addition, recall that every 702 decision bearing on specific intelligence targets is made by agency officials and is not subject to review by the FISC or another judge.[163] By contrast, in traditional retail FISA surveillance, minimization is supervised by the FISC during the course of surveillance.[164] In the 702 programs, all of the burden of civil liberties protection is shifted to minimization post-collection, and there is no mechanism in the FAA to demand more than barebones minimization. In renewing 702, Congress should require the NSA to develop algorithms, filters, or other technologies that will enable it to better determine foreignness and thus United States person status at the point of collection or, failing that, after collection but before use. Minimization could also be more United States person-protective if the agencies that possess the collected content use audit trails to hold agency staff accountable if they use data for impermissible purposes.[165]

A different problem concerns agency searches or queries of collected data under 702. Even without reports from the FBI, the NSA and CIA reported 4672 queries in 2015 involving a "known" United States person, more than double the number queried in 2013.[166] Queries use search terms, much like an internet search, but focus on a specific communication facility, such as an e-mail address.[167] Sometimes characterized as the "back door search loophole" because these searches allow government to access information that would otherwise not be available without a war-

161. *See* NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 4.

162. *See* Donohue, *supra* note 82, at 202 (describing how domestic communications can be monitored even when not in direct communication with foreign targets). *See generally* Daskal, *The Un-Territoriality of Data*, *supra* note 82, at 365–76 (describing generally the difficulties of determining where data is located).

163. 50 U.S.C. § 1881a(i)(1)(A) (2012).

164. *Id.* § 1805(a)(3) (2012).

165. *See* MARKLE FOUND., MOBILIZING INFORMATION TO PREVENT TERRORISM 70 (2006).

166. ODNI 2015 STATISTICAL REPORT, *supra* note 131, at 5; PCLOB 702 REPORT, *supra* note 2, at 57–58; Letter from Deidre M. Walsh, *supra* note 135, at 3.

167. *Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties: Hearing Before the S. Judiciary Comm.*, 114th Cong. 4 (2016) (statement of Chairman David Medine).

rant or similar judicial involvement, queries have been the subject of considerable discussion in the PCLOB and elsewhere.[168] Resulting from the PCLOB recommendations, the NSA and CIA minimization procedures now require that the agencies provide a "statement of facts showing that . . . a query . . . is reasonably likely to return foreign intelligence information."[169] This accountability mechanism should improve internal management of 702 collection.

These reforms were not extended to the FBI, where agents can search 702 data for United States person information as part of any law enforcement investigation. Recall that 702 targets need not be suspected terrorists or criminals. They must only be suspected of possessing relevant foreign intelligence. Although the FBI minimization procedures were declassified in part in 2016, portions of them remain controversial. The brunt of the problem concerns the practice of FBI analysts and agents working on non-foreign intelligence crimes who are permitted to query 702 databases, and do so frequently. Although a newly appointed special advocate argued before the FISC that the FBI should not be permitted to query 702 data when investigating a non-foreign intelligence crime, Judge Hogan ruled that so long as a significant purpose of the original collection was pursuit of foreign intelligence, the later use of the data for another purpose does not violate FISA.[170] Judge Hogan also declined to endorse a related argument made by the special advocate that each query by the FBI of 702 data is a "separate action subject to the Fourth Amendment reasonableness test."[171] Judge Hogan agreed with the government that it is the 702 program as a whole and not each part or step that must be subjected to Fourth Amendment review.[172]

Although Judge Hogan's interpretation is plausible, the FBI minimization procedures do not adequately protect the privacy

168. *See Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties: Hearing Before the S. Judiciary Comm.*, 114th Cong. 14 (2016) (statement of Elizabeth Goitein) (internal quotation marks omitted), https://www.judiciary.senate.gov/imo/media/doc/05-10-16%20Goitein%20Testimony.pdf; PCLOB FACT SHEET, *supra* note 102, at 16–17.

169. CIA 2015 MINIMIZATION PROCEDURES, *supra* note 79, at 3; NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 7.

170. [Redacted], slip op. at 40–41 (FISA Ct., Nov. 6, 2015), https://www.dni.gov/files/documents/20151106-702Mem_Opinion_Order_for_Public_Release.pdf.

171. *Id.* at 40 (internal quotation marks omitted).

172. *Id.* at 40–41.

interests of United States persons. Because the FBI may pursue foreign intelligence or evidence of a crime in its investigations, and at the FBI assessments stage of an investigation it may investigate without any evidence of wrongdoing by anyone, Congress should revise 702 when it is reauthorized to require the FBI to request approval from the FISC before using a United States person identifier to query 702 data in connection with non-foreign intelligence crimes, except in exigent circumstances.[173]

More broadly, in its renewal deliberations, Congress should consider inserting the FISC to review requests by *any* intelligence agency that seeks to query United States person data collected pursuant to 702. The FISC could approve agency queries if the applicant demonstrated that a search is "reasonably likely to return foreign intelligence information," or that there is probable cause that foreign intelligence will be returned.[174] Although the volume of queries might be burdensome for the court, special advocates or judicial clerks could review the submissions and prepare recommendations for the court.

In the background of the renewal deliberations should be the recent FISCR opinion in *In re Certified Question of Law*.[175] In addition to emphasizing the importance of minimization in upholding the incidental collection of information content in an other-

173. We recommend that, if the government legally intercepts a communication under section 702 . . . and if the communication either includes a United States person as a participant or reveals information about a United States person . . . the government may not search the contents of communications acquired under section 702 . . . in an effort to identify communications of particular United States persons, except (a) when the information is necessary to prevent a threat of death or serious bodily harm, or (b) when the government obtains a warrant based on probable cause to believe that the United States person is planning or is engaged in acts of international terrorism.

THE WHITE HOUSE, LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 145–46 (Dec. 12, 2013), https://www.obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf; *see also Oversight and Reauthorization of the FISA Amendments Act: The Balance Between National Security, Privacy and Civil Liberties: Hearing Before the S. Judiciary Comm.*, 114th Cong. 3–5 (2016) (statement of Gregory T. Nojeim, Director, Project on Freedom, Security & Technology, Center for Democracy & Technology), https://cdt.org/files/2016/05/CDT-Statement-for-the-Record-Sen-Jud-05.17.16-2.pdf (recommending that Congress amend section 702 to require a finding of probable cause prior to searching through United States person content communications derived from 702 surveillance).

174. NSA 2015 MINIMIZATION PROCEDURES, *supra* note 70, at 3.

175. NO. FISCR 16-01 (FISA Ct. Rev. Apr. 14, 2016), https://dni.gov/files/icotr/FISCR%20Opinion%2016-01.pdf.

wise non-content-based pen register/trap-and-trace order, the FISCR held that the government "is prohibited from making use of any content information that may be collected."[176] Thus, in an admittedly different intelligence context, the court protected the Fourth Amendment interests of persons by going beyond traditional minimization to erect a strict barrier to the use of content. Congress should be similarly solicitous of the privacy interests of United States persons in 702 collection.

VI. UPSTREAM COLLECTION

Even though upstream collection apparently makes up just under ten percent of 702 data, given the magnitude of the collection there is considerable likelihood that innocent persons' communications are captured. In theory, upstream internet transactions are filtered to eliminate likely domestic transactions and to capture only those transactions that contain one of the tasked selectors. However, the filters are imperfect and the selectors do not necessarily screen out domestic users' transactions. Because upstream collection may include communications "about" the tasked selector as well as to or from, it is even more likely to acquire United States person communications.

The United States persons subject to "about" collection have not been targeted in any way by the government for any aspect of their lives. There is no foreign intelligence expectation in their case, and no indication of criminality. Congress should, at a minimum, require NSA to report in a timely fashion on its efforts to improve its technical capabilities to filter upstream collection to avoid domestic communications. Similarly, Congress should require NSA to find technical solutions that can limit or segregate categories of "about" communications.

CONCLUSION

The FAA and section 702 constituted a sea change in electronic surveillance for foreign intelligence collection. From the available evidence, the program appears to be an integral part of contemporary intelligence collection. Yet authorizing collection without

176. *Id.* at 13; *see also* Klein et al., *Surveillance Policy*, *supra* note 127, at 36 (making similar arguments).

any showing of individualized suspicion, even where collection of United States persons communications is the foreseeable consequence of the program orders, should give us all continuing pause. Rather than roll back the authorization, better assurances of protection for individuals can be accomplished with relatively minor changes to the FAA and more extensive administrative reforms that can be required by statute or generated within the executive. Particularly because the FISC has described its role in authorizing and reviewing surveillance conducted pursuant to 702 as "narrowly circumscribed,"[177] the court's lack of involvement in supervising targeting places a premium on efficacious and accountable administrative implementation.

Finally, the renewal and reform of the FAA only temporarily forestalls the need to confront the foundational and structural flaw in FISA—that technological developments make it virtually impossible to verify the location or nationality of a surveillance target in real time. Indeed, NSA analysts engaged in the most scrupulous attention to the "totality of the circumstances" in making a foreignness determination before targeting someone reasonably believed to be a non-United States person outside the United States can be victimized by location-spoofing technology and then obstructed or at least delayed in applying the law before targeting.[178] Our surveillance laws are, by and large, built upon this no longer realistic assumption. A more basic reworking will be essential before too long. Just as security threats and interests transcend border, our individual freedoms are expressed globally. Neither liberty nor security is promoted by continuing to rely on an outmoded basis for authorizing electronic surveillance for foreign intelligence purposes.

177. *In re* Proceedings Required by § 702(i) of the FISA Amendments Act of 2008, No. MISC. 08-01, slip op. at 3 (FISA Ct., Aug. 27, 2008), https://fas.org/irp/agency/doj/fisa/fisc082708.pdf.

178. Kris, *supra* note 66, at 415.

***