ARTICLE

The Evolution and Jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review

Laura K. Donohue[*]

[*] Professor of Law, Anne Fleming Research Professor, and Director, Center on National Security and the Law, Georgetown Law. All FISC/FISCR opinions and orders cited in the Article have been declassified and released. They are available at the Foreign Intelligence Law Collection, which was built by the author, Jeremy McCabe, and Leah Prescott, and is hosted by Georgetown Law Library at https://repository.library.georgetown.edu/handle/10822/1052698 [https://perma.cc/68BH-AWZS]. I am grateful to Jeremy McCabe, at the Georgetown Law Library, for his help in cite checking the Article and to Judge James E. Boasberg for his comments on an earlier draft.

Abstract

The past eight years have witnessed an explosion in the number of publicly-available opinions and orders issued by the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review. From only six opinions in the public domain 1978–2012, by early 2021, eighty-eight opinions had been released. The sharp departure is even more pronounced in relation to orders: from only one order declassified during 1978–2012, since 2013, 288 have been formally released. These documents highlight how the courts' roles have evolved since 2004 and reveal four key areas that dominate the courts' jurisprudence: its position as a specialized, Article III court; the effort to understand the existing statutory language in light of new and emerging technologies; the tension among constitutional rights, the need for information, and the implications of increasingly broad surveillance programs; and the court's growing role in conducting oversight and having to respond to Executive Branch errors, noncompliance, and misrepresentations. This Article details these tensions in light of the courts' jurisprudence, noting the areas where we are likely to continue to see concerns in the implementation of the Foreign Intelligence Surveillance Act going forward.

Table of Contents

I. Introduction

In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA) to govern domestic electronic intercepts undertaken for foreign intelligence purposes.[1] The statute represented the culmination of years of hearings directed to understanding the scope of surveillance programs conducted with little to no oversight that had resulted in the collection of significant amounts of information on U.S. citizens.[2] It also reflected the U.S. Supreme Court's determination that the Fourth Amendment prohibited the government from undertaking surveillance for domestic security purposes absent independent judicial oversight.[3]

The statute created two specialized Article III courts: the Foreign Intelligence Surveillance Court (FISC) and the (appellate) Foreign Intelligence Court of Review (FISCR).[4] The FISC's role was to review applications for electronic surveillance to determine whether probable cause existed that the target to be placed under surveillance was a foreign power or an agent of a foreign power, and whether the individual was likely to use the facility to be placed under surveillance, prior to issuing orders.[5]

During the first two years that FISA operated, the Department of Justice (DOJ) conducted warrantless physical searches outside of the statutory framing. But in 1980, it adopted a new approach, in which it applied to the FISC for orders to approve nonconsensual physical searches of personal (not real) property.[6] In each case, the Justice Department asserted that the search in question would have required a warrant in a law enforcement context.[7] The court issued the orders without any accompanying opinions. In October of that year, however, the

---

[1] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C.A. §§ 1801–85c (West)).

[2] *See e.g.*, *Intelligence Activities: S. Res. 21: Hearing Before the S. Select Comm. to Study Governmental Operations with Respect to Intelligence Activities of the United States*, 94th Cong., vol. 5, at 1 (1975); 124 CONG. REC. 34,845 (1978) (statement of Sen. Kennedy); S. REP. NO. 94-755 (1976) (the Church Committee reports, divided into six books); THE UNEXPURGATED PIKE REPORT: REPORT OF THE HOUSE SELECT COMMITTEE ON INTELLIGENCE, 1976 (Gregory Andrade Diamond ed., 1992), https://archive.org/details/PikeCommitteeReportFull/page/n103/mode/2up [https://perma.cc/3ZCJ-UWJ3]; Laura K. Donohue, *Bulk Metadata Collection: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 767–83 (discussing the history leading to heightened protections afforded to domestic collection of U.S. citizens' information) (2014).

[3] *See* United States v. U.S. Dist. Ct., 407 U.S. 297, 317–22 (1972) (finding government's security concerns did not justify departure from requirement of judicial approval prior to a search or surveillance).

[4] 50 U.S.C.A. § 1803(a)–(b); *see also In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00127, at 6 (FISA Ct. Jan. 25, 2017) (Collyer, J.); *In re* Sealed Case, 310 F.3d 717, 731, GID.CA.00001, at 731 (FISA Ct. Rev. 2002) (per curiam); United States v. Cavanaugh, 807 F.2d 787, 792 (9th Cir. 1987); *In re* Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985), *aff'd*, 788 F.2d 566 (9th Cir. 1986).

[5] 50 U.S.C.A. § 1805(a); 124 CONG. REC. 35,389 (statement of Sen. Mathias).

[6] S. REP. NO. 97-280 (1981), at 3.

[7] *Id.*

Presiding Judge of the FISC submitted a memorandum that the Court's Legal Adviser had prepared, concluding that the FISC had no authority to issue orders approving a physical search or the opening of mail.[8]

In 1981, the Justice Department, now under the Reagan Administration, submitted an application to the FISC to issue an order approving physical search of nonresidential premises under the direction and control of a foreign power as well as personal property of agents of a foreign power located on the premises.[9] The government simultaneously submitted a memorandum of law explaining that the court lacked jurisdiction over the request.[10] Assuming that the court denied the application, if Congress wanted to bring such searches within FISA, it would have to amend the statute. Otherwise, the Executive Branch could proceed on the basis of its own, independent authority. The court, as expected, declined to issue an order approving the application on the grounds that it lacked any statutory, implied, or inherent authority or jurisdiction to issue orders approving for physical search or mail opening.[11] The full court concurred in the judgment.[12] It did not address the merits of the government's claim that it had the independent authority to undertake such actions. Although the Senate in 1981 considered amending the statute to take account of physical search, it did not do so.[13]

Thirteen years later, the Federal Bureau of Investigation (FBI) arrested Aldrich Hazen Ames, a Central Intelligence Agency counterintelligence officer suspected of being a KGB agent.[14] The Attorney General, citing national security, approved a warrantless search of his home outside of either FISA or ordinary criminal provisions. Ames pled guilty before the case went to trial, but the Clinton Administration was sufficiently concerned about the legality of the search as to seek to amend the statute.

The 1995 Intelligence Authorization Act, accordingly, altered FISA to allow for warrantless, covert physical searches when targeting "premises, information, material, or property used exclusively by, or under the open and exclusive control of, a foreign power or powers."[15] For property not under exclusive

---

[8] Letter from Hon. George L. Hart, Jr., presiding judge, U.S. Foreign Intelligence Surveillance Court, Oct. 31, 1980, cited in S. REP. NO. 97-280 (1981), at 3, n. 3.
[9] S. REP. NO. 97-280 (1981), at 4.
[10] *Id.*
[11] *In re* Application of the United States for an Ord. Authorizing the Physical Search of Nonresidential Premises and Pers. Prop., at 16-19 GID.C.00001 (FISA Ct. June 11, 1981) (Hart, J.), *reprinted in* S. REP. NO. 97-280 (1981).
[12] *Id.*
[13] S. REP. NO. 97-280 (1981), at 8. It continued to keep the matter under advisement. *See* S. REP. NO. 98-660 (1984), at 24.
[14] *See* Complaint, United States v. Ames, No. 94-cr-00166 (E.D. Va. Feb. 21, 1994), https://cryptome.org/jya/ames.htm [https://perma.cc/KP6U-VR69].
[15] Intelligence Authorization Act for Fiscal Year 1995, Pub L. No. 103-359, sec. 807(a)(3), § 302(a)(1)(A)(i), 108 Stat. 3423, 3444 (1994) (codified at 50 U.S.C.A. § 1822(a)(1)(A)(i)). There must be no substantial likelihood that the facilities targeted are the property of a U.S. person. *Id.* § 1822(a)(1)(A)(ii).

control of foreign powers, the statute requires an application to the FISC. The requirements parallel those for electronic surveillance, including the probable cause requirements.[16] In February 1995, President Bill Clinton issued an Executive Order extending certification authority in support of physical search applications submitted to the FISC to the Secretary of State, Secretary of Defense, and the Director of Central Intelligence, as well as their deputies and the Director of the FBI.[17]

Congress subsequently added two more types of foreign intelligence collection to what has come to be known as "Traditional FISA." In 1998, Congress provided for the first by authorizing the acquisition of pen register and trap and trace (PRTT) data for foreign intelligence or international terrorism investigations.[18] In 2001, Congress extended PRTT beyond telephone numbers to empower the government to obtain any "dialing, routing, addressing, or signaling information" identifying the source or end point of a communication—including those that travel via email or through the internet.[19] Further changes in 2006 allowed the government to obtain subscriber records relating to past calls, as well as real-time information.[20]

The second additional type of collection stemmed from the 1995 Oklahoma City bombing. During the investigation, it was unclear whether the FBI had the authority to obtain business records related to a Ryder truck and a storage locker in Arizona that Timothy McVeigh, the Oklahoma City bomber, had rented. So in 1998, Congress expanded FISA to allow the government to obtain records from "a common carrier, public accommodation facility, physical storage facility, or vehicle rental facility."[21] The Director of the FBI, or a designated high-ranking official, had to state that the records are sought for an "investigation to gather foreign intelligence information for . . . international terrorism."[22] The application also had to include "specific and articulable facts" as to why the person to whom the records pertain are a foreign power or an agent thereof[23] (these last two requirements no longer apply).

---

[16] *Id.* § 1823.
[17] Exec. Order No. 12,949, 60 Fed. Reg. 8169 (Feb. 9, 1995).
[18] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, §§ 601–02, 112 Stat. 2396, 2404–12 (1998) (codified as amended at 50 U.S.C.A. §§ 1841–46, 1861–64). Previously, although the Government could request (and the court could issue) orders authorizing pen register and trap and trace devices (PRTT), it could only do so by going through the application procedures that enabled the government to obtain electronic content. *See* Donohue, *supra* note 2, at 793.
[19] USA PATRIOT ACT of 2001, Pub. L. No. 107-56, § 216, 115 Stat. 272, 290 (codified as amended at 18 U.S.C.A. § 3127).
[20] USA PATRIOT Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, § 128(a), 120 Stat. 192, 228 (2006) (codified at 50 U.S.C.A. § 1842(d)).
[21] Intelligence Authorization Act for Fiscal Year 1999 sec. 602, § 502, 112 Stat. at 2411.
[22] *Id.*
[23] *Id.* Just two months before the Oklahoma City attack, President William J. Clinton issued Executive Order 12,949, which expanded the use of FISA for physical searches. *See* Exec. Order No. 12,949, 60 Fed. Reg. 8169 (Feb. 9, 1995).

Under Traditional FISA, from 1978 to 2001, the FISC essentially functioned as a warrant-granting body, issuing more than 14,000 orders and just one public opinion.[24] Applications were sealed and procedures conducted *in camera* and *ex parte*.[25] No additional opinions—and no orders—ever saw light of day. The Oklahoma City-derived provision, for its part, saw little use: between 1998 and 2001, the FBI only obtained one FISA order for business records. But following the attacks of 9/11, that all changed.

The 2001 USA PATRIOT Act altered FISA in several ways: in addition to amending PRTT, it introduced temporary provisions to allow for roving wiretaps; changed the duration of certain orders; increased the number of judges; and amended the definition of "electronic surveillance."[26] By far, the most significant alterations though were the expansion of the business records provision in Section 215 to incorporate requests for *any* tangible goods, as well as the insertion of the word "significant" into the purpose for which FISA's electronic intercepts could be sought.[27] The latter, together with a provision that authorized coordination between intelligence and law enforcement—and a prominent case that came before the FISCR in 2002—brought down the wall that had previously existed within the Department of Justice between foreign intelligence collection and criminal investigations.[28] In 2004, Congress further amended the statute to incorporate temporary "lone wolf" powers, permitting the surveillance of non-U.S. persons engaged in international terrorism, without requiring evidence linking those persons to an identifiable foreign power or terrorist organization.[29]

---

[24] FISA Annual Reports to Congress, 1979–2002, *Foreign Intelligence Surveillance Act*, FED'N AM. SCIENTISTS, https://fas.org/irp/agency/doj/fisa/ [https://perma.cc/Z4QH-73A3] (last updated July 28, 2020); *In re* Application of the United States for an Order Authorizing the Physical Search of Nonresidential Premises and Pers. Prop., GID.C.00001 (FISA Ct. June 11, 1981) (Hart, J.), *reprinted in* S. REP. NO. 97-280, at 16-19 (1981).

[25] *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 488 n.12, GID.C.00021, at 6 n.12 (FISA Ct. 2007) (Bates, J.). The law provides special protections for U.S. persons, who can only be considered an "agent of a foreign power" when the government has evidence of some level of criminality on a par with criminal law. 50 U.S.C.A. § 1801(b)(2); *see also* Donohue, *supra* note 2, at 789–90. Even then, further minimization procedures apply. 50 U.S.C.A. § 1801(h)(2). Where special non-judicial procedures targeting non-US persons are used, the Attorney General can only authorize collection where there is "no substantial likelihood" that citizens' communications will be obtained or that the search will involve the "premises, information, material, or property of a" U.S. person. 50 U.S.C.A. § 1822(a)(1)(A)(ii). In the event that a citizen's communications or property *are* involved, the government must obtain a court order within 72 hours before the information or property in question can be "disclosed, disseminated, or used for any purpose." 50 U.S.C.A. § 1801(h)(4) (electronic surveillance); *id.* § 1821(4)(D) (physical search).

[26] USA PATRIOT ACT of 2001, Pub. L. No. 107-56, §§ 206–08, 214, 504, 1003, 115 Stat. 272, 282-83, 286-87, 291, 364–65, 392 (§§ 206 (roving wiretaps), 207 (duration of orders for non-US persons), 208 (expanding FISC to 11 judges), 214 (amending PRTT), 504 (authorizing coordination), 1003 (amending the definition)).

[27] *Id.* §§ 215, 218, 115 Stat. at 287–88, 291.

[28] *In re* Sealed Case, 310 F.3d 717, GID.CA.00001 (FISA Ct. Rev. 2002) (per curiam).

[29] Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, § 6001, 118 Stat. 3638, 3742.

Despite Congress's explicit direction in 1978 that FISA be the sole means for conducting domestic surveillance for foreign intelligence purposes, following 9/11, the Bush Administration instituted a program entirely outside the FISA framework. STELLARWIND intercepted the contents of certain domestic and international telephone calls and Internet communications, as well as telephony and Internet metadata. Starting in 2004 with Jack Goldsmith's arrival at the Office of Legal Counsel, the Justice Department began to try to shoehorn some of the existing intelligence collection into the FISA framing. The statute, though, had been designed to ensure that surveillance could only be undertaken with particular targets in mind. Even with the USA PATRIOT Act changes, it took creative legal interpretations to find a way to bring parts of the program within FISA.[30]

The ill-fitting nature of bulk collection programs in the existing statutory framing prompted further statutory revision and ushered in what is colloquially referred to as "modernized FISA." The 2008 FISA Amendments Act (FAA) added a new provision (Section 704), which provided for the acquisition of the communications of U.S. persons located outside the United States—a category that previously fell within the guidelines set by Executive Order 12333. Simultaneously, two other provisions liberalized the FISA rules for targeting individuals outside the United States, with Section 702 providing for the domestic collection for non-U.S. persons, and Section 703 for U.S. persons, reasonably believed to be outside the United States.[31] The statute empowered the Attorney General and the Director of National Intelligence to jointly authorize (without court approval), for up to one year, the targets of such intercepts.[32]

These changes significantly altered the courts' role. Instead of just issuing orders targeted at particular individuals inside the U.S., the FISC and FISCR now monitor programmatic collection of international electronic communications.[33] The courts tackle questions related to jurisdiction, separation of powers, and the rule of law. They wrestle with how to understand new technologies in light of old statutory language, and they engage in complex analysis to apply the fourteen statutes that now constitute FISA.[34] The courts routinely confront difficult First, Fourth, and Fifth Amendment questions that impact the lives of every person in the United States, as well as certain individuals overseas.[35] And they have to police an

---

[30] *See generally* LAURA K. DONOHUE, THE FUTURE OF FOREIGN INTELLIGENCE: PRIVACY AND SURVEILLANCE IN A DIGITAL AGE (2016).

[31] FISA Amendments Act of 2008, Pub. L. No. 110-261, §§ 702–04, 122 Stat. 2436, 2438–57 (codified as amended at 50 U.S.C.A. §§ 1881a–c (West)).

[32] Certain restrictions apply. *See id.*

[33] The courts also became enmeshed in considering bulk collection of domestic and international communications, until subsequent statutory changes prohibited such collection for telephony metadata. *See* Donohue, *Bulk Metadata Collection*, *supra* note 2.

[34] *See, e.g.*, Supplemental Opinion, *In re* Prod. of Tangible Things, No. BR 08-13, GID.C.00033 (FISA Ct. Dec. 12, 2008) (Walton, J.).

[35] *See, e.g.*, *In re* Proc. Required by Section 702(i) of the FISA Amends. Act of 2008, No. Misc 08-01, GID.C.00028, 2008 WL 9487946 (FISA Ct. Aug. 27, 2008) (McLaughlin, J.) (First and Fourth Amendments); Opinion on Motion for Disclosure of Prior Decisions, [REDACTED], No. [REDACTED], GID.C.00112 (FISA Ct. 2014) (Collyer, J.) (Fifth Amendment); Memorandum, *In*

Executive that makes technical errors, fails to comply with court orders, omits critical information, and makes misrepresentations to the court.[36] Instead of just issuing orders approving applications, the FISC routinely issues opinions, which the Executive Branch, *amici*, non-specialized Article III judges (and their clerks and parties before them), cite to as precedent.[37] This is not the role that Congress envisioned for the FISC/FISCR in 1978.

An important and robust body of law is now emerging from a court that, for decades, has been largely shielded from public inspection. As shown in Figures 1

---

re Application of the Federal Bureau of Investigation for an Order Requiring Production of Tangible Things from [REDACTED], No. BR 13-158, GID.C.00086 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.) (First and Fourth Amendments); *In re Sealed Case*, 310 F.3d 717, GID.CA.00001 (Fourth Amendment).

[36] *See, e.g.*, Supplemental Opinion and Order, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things [REDACTED], No. BR 09-15, GID.C.00048, at 3–4 (FISA Ct. Nov. 5, 2009) (Walton, J.) (NSA sent query results to email list of 189 analysts, "only 53 of whom had received the required training"); [REDACTED], No. [REDACTED], GID.C.00073, at 15–18, 78–80, 2011 WL 10945618, at *5–6, *28 (FISA Ct. Oct. 3, 2011) (Bates, J.) (NSA misled Court, violating FISA and the Fourth Amendment); Memorandum Opinion, [REDACTED], No. [REDACTED], GID.C.00092, at 3, 18, 100–05 (FISA Ct.) (Bates, J.) ("NSA exceeded the scope of authorized acquisition continuously during the more than [REDACTED] years of acquisition"; FBI, CIA, and NCTC "accessed unminimized U.S. person information"; NSA disseminated "reports containing U.S. person information"; government requested permission to violate law); Memorandum Opinion, [REDACTED], No. [REDACTED], GID.C.00078, at 26–27 (FISA Ct. Sept. 25, 2012) (NSA misrepresented upstream collection, acquiring U.S. person domestic communications).

[37] For FISC/FISCR reference to prior opinions as precedent, see, e.g., *In re* Directives to Yahoo! Inc. Pursuant to Sec. 105B of Foreign Intel. Surveillance Act, 551 F.3d 1004, 1010, GID.CA.00002, at 13, 15 (FISA Ct. Rev. 2008) (Selya, J.); Memorandum, *In re* Application of the FBI, No. BR 13-158, GID.C.00086, at 4–5 (analyzing Judge Eagan's constitutional analysis in the context of the Supreme Court's recent decision in *United States v. Jones*); *see also* Memorandum Opinion, [REDACTED], No. [REDACTED], GID.C.00092, at 6, 74–75; Memorandum Opinion, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things from [REDACTED], No. BR 14-96, GID.C.00103, at 2–3 (FISA Ct. June 19, 2014) (Zagel, J.); Amended Memorandum Opinion, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-109, GID.C.00083, at 19–20 (FISA Ct. Aug. 29, 2013) (Eagan, J.). For similar references by the U.S. Department of Justice, see, e.g., Defendants' Memorandum of Law in Opposition to Plaintiffs' Motion for a Preliminary Injunction at 16, Am. C.L. Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013), *aff'd in part, vacated in part, remanded*, 785 F.3d 787 (2d Cir. 2015), 2013 WL 5744828 ("[S]ince May 2006, fourteen separate judges of the FISC have concluded on thirty-four occasions that the FBI satisfied this requirement, finding 'reasonable grounds to believe' that the telephony metadata . . . 'are relevant to authorized investigations.'") (citation and quotation omitted); United States' Legal Brief to the En Banc Court in Response to the Court's Order of March 22, 2017 at 1, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08 (FISA Ct. Apr. 17, 2017), https://repository.library.georgetown.edu/bitstream/handle/10822/1056062/Misc%252013-08%2520United%2520States%2527%2520Legal%2520Brief%2520to%2520the%2520En%2520Banc%2520Court.pdf [https://perma.cc/WKA5-CT8P] ("It is well-settled that there is no First Amendment public right of access to the proceedings, records, and rulings of this Court," citing to four FISC opinions and orders in support.)

and 2, nearly ninety declassified FISC/FISCR opinions and 290 orders are now in the public domain, as are hundreds of FISC/FISCR filings.[38]

Previously Classified FISC/FISCR Opinions
by month of declassification and release

Month	Pre-2013	2013	2014	2015	2016	2017	2018	2019	2020
	6								
January						1	6		
February									1
March				2			1		2
April			7		3	2			1
May						1			
June			1	1		12			
July				1					
August		3	3		1		7		
September		3	4	1		1			6
October		1						3	
November		2				1			1
December			2	1					
Total	6	9	17	6	4	18	14	3	11

Figure 1

Previously Classified FISC/FISCR Orders
by month of declassification and release

Month	Pre-2013	2013	2014	2015	2016	2017	2018	2019	2020
	1								
January			24			2	12		4
February			1		1		1		6
March			1	4	1	4			5
April			51		16	5		1	4
May			2			2	2		
June			3	2		18			1
July		1	3	2					2
August		2	7	1	1		28		
September		8	11	2		14			5
October		3	1	1		1		3	1
November		2	1						1
December			8	1				3	1
Total	1	16	113	13	19	46	43	7	30

Figure 2

The timing and pattern of the declassification of the courts' opinions and orders illustrate the suddenness with which the courts have found themselves in the public eye.

[38] More than two decades after its 1981 opinion, the Court issued two opinions. *In re Sealed Case*, 310 F.3d 717, GID.CA.00001; *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, GID.C.00002 (FISA Ct. 2002), *rev'd by In re Sealed Case*, 310 F.3d 717, GID.CA.00001. It published two more opinions between 2007 and 2008. *In re* Directives to Yahoo!, Inc Pursuant to Sec. 105B of Foreign Intel. Surveillance Act, 551 F.3d 1004, GID.CA.00002 (FISA Ct. Rev. 2008) (Selya, J.); *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, GID.C.00021 (FISA Ct. 2007) (Bates, J.).

It would be hard to overstate the importance of the documents leaked by Edward Snowden in June 2013 in driving this phenomenon. They took the study of foreign intelligence from a niche, classified legal specialization to a matter of public discourse. By the end of the year, nine new opinions and sixteen orders had been formally declassified and released by the government, in sharp contrast to just six opinions and one order that had been released over the previous 35 years of the statute's existence. Similarly, from zero public filings prior to June 2013, within five months of the Snowden leaks, the FISC's public docket had exploded.[39] These filings put the courts in the position of having to determine a range of difficult questions, including under what conditions its opinions would be made public. Like some of the other roles assumed by the court, this was not a function envisioned by Congress in 1978.

As the FISC/FISCR have been forced to wrestle with difficult constitutional and statutory questions, non-specialized Article III courts increasingly have had to take account of their jurisprudence. In part this also has to do with changed conditions regarding standing. In *Clapper v. Amnesty International*, the Solicitor General represented to the Supreme Court that the Justice Department would inform criminal defendants if FISA-derived information was used against them.[40] It was not until a *New York Times* article revealed in 2013 that the government was not in the practice of doing so, however, that the policy changed.[41] The definition

---

[39] Four days after the first articles appeared in *The Guardian* and *Washington Post*, for instance, on June 10, 2013 the ACLU and Yale Media Freedom Information Access Clinic (MFIAC) filed a motion to obtain all FISC opinions evaluating the meaning, scope, and constitutionality of bulk collection. Four days later, Yahoo! moved under FISC Rule 62(a) to request the Court to order publication of an opinion from 2008, which had been appealed to FISCR and referenced in *In re* Directives, 551 F.3d 1004, GID.CA.00002. On June 19, Microsoft requested permission to disclose the aggregate information related to FISC orders with which it had been served. Google, Facebook, and LinkedIn soon filed parallel requests. On June 28, sixteen members of the U.S. House of Representatives filed an amicus brief in support of the ACLU/MFIAC motion—a move followed on July 8 by the First Amendment Coalition, the Center for Democracy and Technology, the Electronic Frontier Foundation, and on July 15 by a formidable media conglomerate: the Reporters' Committee, ABC News, the Associated Press, Bloomberg News, Dow Jones, the *Los Angeles Times*, National Public Radio, Reuters, the *New Yorker*, *Newsweek*, the *Washington Post*, and others. By mid-November 2013, further motions for judicial records had been filed by the Center for National Security Studies and ProPublica. For further discussion, see discussion in Part II.E, Standing, *infra*.

[40] *See* Clapper v. Amnesty Int'l, 568 U.S. 398, 421–22 (2013).

[41] *See* Nina Totenberg, *Government Takes a U-Turn on Warrantless Wiretaps*, NPR (Oct. 23, 2013), https://www.npr.org/2013/10/23/240163063/government-changes-policy-on-warrantless-wiretap-defendants [https://perma.cc/ZBA2-THYX]; Eric Schmidt et al., *Administration Says Mining Data Is Crucial to Fight Terrorism*, N.Y. TIMES (June 7, 2013), https://www.nytimes.com/2013/06/08/us/mining-of-data-is-called-crucial-to-fight-terror.html?module=inline [https://perma.cc/TH3B-G3CY]; Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N.Y. TIMES (July 15, 2013), https://www.nytimes.com/2013/07/16/us/double-secret-surveillance.html [https://perma.cc/PLH6-JADQ]; Charlie Savage, *Federal Prosecutors, in a Policy Shift, Cite Warrantless Wiretaps as Evidence*, N.Y. TIMES (Oct. 26, 2013), https://www.nytimes.com/2013/10/27/us/federal-prosecutors-in-a-policy-shift-cite-warrantless-wiretaps-as-evidence.html [https://perma.cc/B9MB-HPQJ].

of "derived from" remains classified. Nevertheless, an increasing number of defendants are being informed that evidence against them derives from FISA. Simultaneously, dozens of Freedom of Information Act (FOIA) suits over the past decade have sought access to FISC opinions and orders.[42] A number have been successful in contributing to the material in the public domain.[43]

There are now more than 180 FISA-related cases in regular Article III courts—approximately twice the total number of FISC/FISCR cases that have been made publicly available by the courts, Office of the Director National Intelligence (ODNI), or FOIA litigation.[44] The specialized Article III courts (FISC/FISCR) and the non-specialized, geographic Article III courts (i.e., District Courts and Courts of Appeal) are increasingly in dialogue as the caselaw evolves, making it all the more important to address the scope of FISC/FISCR jurisprudence.

This Article suggests that the bulk of the issues that come before the courts derive from four key areas. Each can be explained by tensions inherent in the FISC/FISCR current role and the structure developed by Congress in 1978. Understanding these areas can help to clarify questions before the courts by placing them in their broader context and provide a framework for how to think about any future legislative changes. The goal is to ensure a deeper theoretical grasp of the role of the courts in foreign intelligence law.

The first area of tension arises from the courts' statutory jurisdiction, Article III status, and the specialized nature of the cases that they consider. Somewhat surprisingly, there is almost no attention paid in the Federal Courts scholarship to the role of specialized Article III entities in contrast to non-specialized, geographic courts—much less their distinction from the myriad other types of federal courts in

---

[42] *See, e.g.*, ACLU v. ODNI, Not Reported in F.Supp.2d, 2011 WL 5563520 (Nov. 15, 2011); New York Times Co. v. U.S. Dep't of Justice, 872 F.Supp.2d 309 (S.D.N.Y. 2012); Elec. Frontier Found. v. Dep't of Justice, 892 F.Supp.2d 95 (D.D.C. 2012); Elec. Frontier Found. v. Dep't of Justice, U.S. Ct. of Appeals for D.C., 739 F.3d 1, Jan. 3, 2014; cert. denied Elec. Frontier Found. v. Dep't of Justice, 135 S.Ct. 356 (2014); *Elec. Privacy Info. Ctr. v. DOJ*, No. 13cv1961, 2016 WL 447426 (D.D.C. Feb. 4, 2016).

[43] *See, e.g.*, ACLU v. ODNI, Not Reported in F.Supp.2d, 2011 WL 5563520 (Nov. 15, 2011); Elec. Frontier Found. v. DOJ, No.: 4:11-cv-05221-YGR, 2014 WL 3945646 (N.D. Cal. Aug. 11, 2014).

[44] Despite the increasing importance of the courts' jurisprudence, FISC/FISCR opinions and orders have not hitherto been easily accessible. Less than two dozen declassified and redacted opinions are available on the court's web site. Some opinions are only available through the Office of the Director of National Intelligence (ODNI). Others are only available from individuals who have submitted Freedom of Information Act requests or engaged in litigation with the Department of Justice to obtain the materials—and decided to place them online. Neither Westlaw nor Lexis, moreover, carry most of the opinions, despite FISA issues regularly now appearing in ordinary Article III courts. No site has all of the declassified and redacted court filings available. Accordingly, Jeremy McCabe, Leah Prescott, and I have created a text-searchable database at Georgetown Law Library with all of the formally released (and often redacted) FISC/FISCR opinions and orders, along with all of the publicly available guidelines. *Foreign Intelligence Law Collection*, DIGITAL GEO., https://repository.library.georgetown.edu/handle/10822/1052698 [https://perma.cc/NQ4B-CQYN] (last updated Mar. 17, 2021).

existence.[45] Yet the associated questions are foundational and particularly important for the FISC/FISCR. Separation of powers, issues related to the standing of third parties and the public, the scope of the courts' subject-matter jurisdiction, and the relationship between specialized and non-specialized courts have all played a central role in the courts' jurisprudence. The cases also reveal efforts by the Executive to classify judicial opinions that reveal Executive Branch malfeasance—raising further concern about efforts by Article II to undermine the constitutional powers and responsibilities of an Article III entity.

The second cluster finds root in the tension between new technologies and old statutory language—i.e., text drafted with very different technologies in mind. Here, the FISC has repeatedly had to return to questions about *what*, precisely, constitutes "electronic surveillance," how to understand "electronic communications," and what is included in the definition of a "facility." So, too, has it wrestled with the line between intercepts and searches in the mobile digital world. Distinguishing between "content" versus "non-content" in relation to PRTT, and how to handle technologies like the use of post-cut-through-dialed-digits provide just a few examples. Further issues arise in relation to business records, bulk collection, and Section 702 acquisition.

The third cluster centers on constitutional rights, wherein the tension between secrecy (as statutorily required or as demanded by the Executive Branch), surveillance, and individual rights comes to the fore. The courts have had to wrestle here with matters related to the First Amendment right of access that derives from the right to petition the government, as well as, to a lesser extent, associational rights. Equally important have been Fourth Amendment concerns—particularly in relation to third party data and the reasonableness requirement. The Fifth Amendment has appeared around the edges in the context of due process protections.

The fourth and final cluster centers on process and compliance, where tension marks the frontier between public and private accountability. Innumerable instances of noncompliance, coupled with blatant misrepresentations to the court, have put the FISC in the position of having to conduct ongoing oversight of the intelligence community. Irregularities in regard to special as well as standard minimization procedures (SMPs), targeting, and querying procedures have repeatedly presented. The court has had to address inaccurate, materially omitted, erroneous, and false statements. Some opinions further call attention to the problem of overcollection and what could be termed the "data dilemma": i.e., what to do with information obtained outside statutory or judicial restrictions.

---

[45] For scholarship on the distinction between Article III specialized and geographic courts, as well as the full panoply of federal courts, see Laura K. Donahue & Jeremy M. McCabe, *Federal Courts: Art. III(1), Art. I(8), Art. IV(3)(2), Art. II(2)/I(8)(3), and Art. II(1)*, 71 CATH. U. L. REV. ___ (forthcoming 2021).

Having examined each of these areas, the Article concludes by underscoring some of the trends that we are now seeing, as well as areas where we might expect to see more concentration in the future, based on the structural pressures.

II. Cluster 1: The FISC/FISCR as Specialized, Article III Courts

One of the most important tensions to which the FISC/FISCR has had to return repeatedly is how to understand its status as a specialized Article III court. To some extent the questions that mark this area reflect a dearth in the scholarship: surprisingly little has been written on the range of federal courts and their distinguishing characteristics. Nevertheless, what is clear from statutory language, legislative history, and jurisprudence of both specialized and non-specialized, geographic Article III courts, is that the FISC and FISCR find their constitutional nexus in Article III(1) and thus carry with them the inherent powers of such entities. The FISC, accordingly, has exercised some ancillary powers even as it has wrestled with the scope of its jurisdiction.

A. *Constitutional Grounding*

Article III(1) non-specialized courts are those entities that enter the mind when envisioning federal courts: i.e., the U.S. Supreme Court, the Courts of Appeal, and the District Courts. With the exception of the Supreme Court, each is brought into being by Congress. They are provided with broad subject-matter jurisdiction and designated as the courts of record for distinct geographic regions.[46]

Less well-known are the specialized Article III(1) courts. Over the course of U.S. history, there have been at least a dozen such entities, five of which are still in existence.[47] Distinguishing between the two categories by referring to the narrower subject matter of specialized tribunals, though, is somewhat of a misnomer: all federal Article III(1) courts are courts of limited jurisdiction.[48] As the Supreme Court explained in 1812, "[T]he power which congress possess to create Courts of inferior jurisdiction, necessarily implies the power to limit the

---

[46] *See* Judiciary Act of 1789, ch. 20, §§ 9, 11, 1 Stat. 73, 76–77, 78–79 (district and defunct circuit courts); Judiciary Act of 1891, ch. 517, §§ 2, 6, 26 Stat. 826, 826–27, 828 (circuit courts of appeals).

[47] Past Article III specialized courts include: the Customs Court (replaced by U.S. Court of International Trade); Court of Customs and Patent Appeals; Emergency Court of Appeals (WWII challenges to Price Administration regulations); Temporary Emergency Court of Appeals; Commerce Court; Special Railroad Court; Court of Claims; and Courts of the District of Columbia (which are now considered Article I entities). The current specialized courts include the FISC and FISCR, Alien Terrorist Removal Court, the U.S. Court of Appeals for the Federal Circuit, and the U.S. Court of International Trade. For more discussion of each of these entities, and their designation, see Donohue & McCabe, *supra* note 45.

[48] *See* Patchak v. Zinke, 138 S. Ct. 897, 906–07 (2018); Gunn v. Minton, 568 U.S. 251, 256–58 (2013); Bender v. Williamsport Area Sch. Dist., 475 U.S. 534, 541 (1986); Owen Equip. & Erection Co. v. Kroger, 437 U.S. 365, 374 (1978); Owen Equip. & Kline v. Burke Constr. Co., 260 U.S. 226, 234 (1922); Marbury v. Madison, 5 U.S. (1 Cranch) 137, 173-80 (1803); Turner v. Bank of N. Am., 4 U.S. (4 Dall.) 8, 10 (1799).

jurisdiction of those Courts to particular objects."[49] The legislature merely grants geographic Article III(1) courts the authority to hear more types of cases.

Whether a court falls within Article III of the Constitution turns in part on whether it satisfies structural requirements: i.e., unity, supremacy, and inferiority within the Judicial Branch. The composition and operation of the court also must comply with the constitutional requirements of tenure of office during good behavior and undiminished compensation, as well as the case-or-controversy stipulations.

Courts that do not meet these requirements are considered alternately (and misleadingly)[50] "non-constitutional," "legislative," or "Article I" courts—i.e., tribunals "created by Congress in the exertion of *other* powers."[51] They "are not . . . [c]ourts, in which *the judicial power* conferred by the Constitution on the general government, can be deposited."[52] Instead, they arise out of other constitutional provisions, such as Congress's tax powers,[53] commerce, bankruptcy, and citizenship authorities,[54] copyrights and patents,[55] control of the military,[56] governance over Washington, D.C.,[57] or regulation of the territories.[58] *Pari passu*, consular courts, and certain adjudicatory bodies find their locus in the Executive Branch and do not constitute the Judicial Branch of government.[59]

The distinction matters: these other courts do not exercise the judicial power of the United States. Article III(1) constitutional courts, like the FISC and FISCR, do.[60] They have the authority to enter final, binding judgments relating to constitutional law and common law. As the Supreme Court put it in 1888, "The whole work done by the judges constitutes the authentic exposition and interpretation of the law."[61] It is thus within the purview of Article III courts to dispose of cases, applying law to the facts, before rendering a final, binding judgment.

As a matter of separation of powers, once this process is put into motion,

---

[49] United States v Hudson, 11 U.S. (7 Cranch) 32, 33 (1812).
[50] All federal courts derive from a constitutional nexus. Some non-Article III entities, moreover, are created by legislation, but others are not. Further, while some tribunals derive from provisions in Article I, others stem from Article IV or Article II. For more detailed discussion of the myriad federal courts introduced over the course of U.S. history, see Donohue & McCabe, *supra* note 45.
[51] *Ex parte* Bakelite Corp., 279 U.S. 438, 449 (1929) (emphasis added).
[52] Am. Ins. Co. v. 365 Bales of Cotton (Canter), 26 U.S. (1 Pet.) 511, 546 (1828) (emphasis added).
[53] U.S. CONST. art. I, § 8, cl. 1.
[54] *Id.* art. I, § 8, cls. 3, 4.
[55] *Id.* art. I, § 8, cl. 8.
[56] *Id.* art. I, § 8, cl. 14, 16.
[57] *Id.* art. I, § 8, cl. 17.
[58] *Id.* art. IV.
[59] *See generally* Donohue & McCabe, *supra* note 45.
[60] *See* Stern v. Marshall, 564 U.S. 462, 494–95 (2011).
[61] Banks v. Manchester, 128 U.S. 244, 253 (1888).

Congress and the Executive cannot interfere.[62] Nor can they insert themselves into the process after the fact—a principle famously recognized in *Hayburn's Case*.[63] If the political branches *could* interfere (for instance, by overturning the court's final judgment or stripping the court of authority over their own opinions), it would render the independence of the judiciary of no consequence. It would not matter what the court said or did. All the courts *have* is their judgment as to matters of law.

B. *FISC/FISCR Article III Status*

Every Article III court—specialized and non-specialized—that has considered the question of whether the FISC and FISCR are Article III courts has answered in the affirmative.[64] As FISC Judge John Bates explained in 2007, "Notwithstanding the esoteric nature of its caseload, the FISC is an inferior federal court established by Congress under Article III."[65] Efforts to question their status on the grounds of the judges' seven-year tenure have been roundly defeated.[66] As a Ninth Circuit District Court explained in 1985, "The FISA court is wholly composed of United States District Court judges, who have been appointed for life by the President, with the advice and consent of the Senate, and whose salaries cannot be reduced."[67] The constitutional requirement of tenure of office is thus satisfied, as is the protection against diminished compensation.

The statutorily-required *in camera*, *ex parte* procedures do not remove the FISC/FISCR from the ambit of Article III. The legislative design in 1978 laid out a process not dissimilar from ordinary warrant procedures—an approach that made sense in light of the courts' initially limited role in granting or denying applications for surveillance. Giving such powers to the court did not amount to an unconstitutional delegation of authority. As the FISCR reflected in 2002, "In light of *Morrison v. Olson* and *Mistretta v. United States*, we do not think there is much left to an argument made by an opponent of FISA in 1978 that the statutory

---

[62] *See* United States v. Klein, 80 U.S. (13 Wall.) 128, 145-48 (1871).

[63] Hayburn's Case, 2 U.S. (2 Dall.) 409, 410 n.† (1892); *see also* Plaut v. Spendthrift Farm, Inc., 514 U.S. 211, 217–18 (1995).

[64] *See, e.g.*, United States v. Cavanagh, 807 F.2d 787, 791 (9th Cir. 1987); United States v. Megahey, 553 F. Supp. 1180, 1197 (E.D.N.Y. 1982), *aff'd*, 727 F.2d 1444 (2d Cir. 1983); United States v. Falvey, 540 F. Supp. 1306, 1313 n.16 (E.D.N.Y. 1982); *In re* Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985) (district court judges retain "Article III status" when acting as members of the FISC), *aff d*, 788 F.2d 566 (9th Cir. 1986); Opinion and Order, *In re Ords. of this Ct. Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, GID.C.00085, at 4 (FISA Ct. Sept. 13, 2013) (Saylor IV, J.) ("The FISC is an Article III Court."); *In re* Sealed Case, 310 F.3d 717, 731, GID.CA.00001, at 731 (FISA Ct. Rev. 2002) (per curiam) (applying to the FISC "the constitutional bounds that restrict an Article III court.").

[65] *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 486, GID.C.00021, at 3 (FISA Ct. 2007) (Bates, J.).

[66] *Cavanagh*, 807 F.2d at 791 ("[Appellant] . . . appears to suggest that the FISA court is not properly constituted under [A]rticle III because the statute does not provide for life tenure on the FISA court. This argument has been raised in a number of cases and has been rejected by the courts. We reject it as well.") (citations omitted).

[67] *Kevork*, 634 F. Supp. at 1014.

responsibilities of the FISA court are inconsistent with Article III case and controversy responsibilities of federal judges because of the secret, non-adversary process."[68]

Nor does limited subject matter jurisdiction impact the courts' status. In 1982, the FISC explained, "[a]s an inferior court established by Congress pursuant to Article III of the Constitution," the court is limited to "only such jurisdiction as the FISA confers upon it and such ancillary authority as may fairly be implied from the powers expressly granted to it."[69] All federal courts, in this sense, are courts of limited jurisdiction. More recently, in 2018, the court stated, "the FISC's authority and inherent secrecy is cabined by—and consistent with —Article III of the Constitution."[70] The FISC therefore acts with the understanding that its "jurisdiction is governed by Article III, section 2, of the Constitution."[71]

C. *Inherent Powers*

Owing to their constitutional status within the third branch of government, the FISC and FISCR carry with them the same inherent powers of all Article III courts.[72] FISA acknowledges, "Nothing in this chapter shall be construed to reduce or contravene the inherent authority of a court established under this section to determine or enforce compliance with an order or a rule of such court or with a procedure approved by such court."[73] FISC Presiding Judge John Bates later attributed the source of the court's inherent authorities to its Article III status.[74]

Inherent powers incorporate a range of powers central to the courts's role in administering justice, foremost amongst which is the importance of being able to ensure fairness in the course of adjudication. This includes, *inter alia*, the exercise of equitable remedies, as established by Article III, which extends the judicial power "to all Cases, in Law and Equity, arising under" federal law.[75] Article III entities, accordingly, can appoint auditors, special masters, and commissioners to undertake investigations.[76] Like its sistren, the foreign

---

[68] *In re Sealed Case*, 310 F.3d at 732 n.19, GID.CA.00001, at 732 n.19 (citation omitted).
[69] *In re* Application of the United States for an Ord. Authorizing the Physical Search of Nonresidential Premises & Pers. Prop., GID.C.00001 (FISA Ct. June 11, 1981) (Hart, J.), *reprinted in* S. REP. NO. 97-280 at 16 (1981).
[70] *In re* Certification of Questions of L. to the Foreign Intel. Surveillance Ct. of Rev., GID.CA.00006, at 8 (FISA Ct. Rev. Mar. 16, 2018).
[71] *Id.*
[72] For more detailed discussion of Article III courts' inherent powers, see Donohue & McCabe, *supra* note 45.
[73] 50 U.S.C.A. § 1803(h) (West).
[74] *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 486, GID.C.00021, at 3 (FISA Ct. 2007) (Bates, J.).
[75] U.S. CONST., Art. III, Sec. 2, cl. 1.
[76] *See In re* Peterson, 253 U.S. 300, 304-07, 312-14 (1920); Ruiz v. Estelle, 679 F.2d 1115, 1161 (5th Cir. 1982), *amended in part and vacated in part on other grounds*, 688 F.2d 266 (5th Cir. 1982); Schwimmer v. United States, 232 F.2d 855, 865 (8th Cir. 1956); Heckers v. Fowler, 69 U.S. (2 Wall.) 123, 127–29 (1864).

intelligence courts can require the production of statements and parties to attend hearings.[77] To ensure matters of law are addressed, they can require additional legal memoranda and briefing,[78] appoint counsel to serve standby,[79] and designate *amici curiae*.[80] This the court has done on a number of occasions—including prior to the USA FREEDOM Act, which explicitly allowed for the appointment of *amici*. In 2013, Judge Mary A. McLaughlin, relying on non-specialized Article III caselaw, determined that the FISC had the inherent power to allow *amicus curiae* to brief the court.[81] Because of their constitutional status, the FISC and FISCR also retain "all the inherent powers that any court has when considering a warrant. There is no delegation of judicial power to the Executive Branch."[82]

In addition to ensuring fairness and justice, Article III courts have broad authority to facilitate the efficient use of resources, which translates into an ability to manage their own affairs.[83] Thus, while dockets themselves may include mandatory elements, *how* that docket is handled falls within the courts' purview.[84] This includes, amongst other instruments, setting the order in which issues will be addressed,[85] as well as consolidating cases.[86]

The FISC has exercised these powers as well as other ancillary authorities that go to efficiency, such as comity and the first-to-file rule—both of which are considered classic inherent powers. In 2013, for example, Judge Dennis Saylor found standing on First Amendment grounds for an American Civil Liberties Union (ACLU) motion for the release of Section 215-related opinions, but then stayed the case on the grounds that a substantially similar one was moving through the Southern District of New York pursuant to FOIA.[87] The court wrote, "As a matter of comity, and in order to conserve judicial resources and avoid inconsistent judgments, federal courts do not engage in parallel adjudications involving the

---

[77] *See* Jencks v. United States, 353 U.S. 657, 668–69 (1957); Brockton Sav. Bank v. Peat, Marwick, Mitchell & Co., 771 F.2d 5, 11–12 (1st Cir. 1985).
[78] Alameda v. Sec'y of Health, Educ. & Welfare, 622 F.2d 1044, 1047 (1st Cir. 1980).
[79] United States v. Bertoli, 994 F.2d 1002, 1018 (3d Cir. 1993).
[80] *In re* Utils. Power & Light Corp., 90 F.2d 798, 800 (7th Cir. 1937).
[81] The Court applies previous Article III case precedent to the FISC to conclude it has the inherent authority to allow "*amicus curiae* briefs within the context of the statutory provisions that set out the *ex parte* and classified nature of proceedings under the . . . . Section 215." Order and Memorandum Opinion, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things, No. BR 13-158, GID.C.00090, at 5 (FISA Ct. Dec. 18, 2013) (McLaughlin, J.).
[82] *In re* Kevork, 634 F. Supp. 1002, 1014 (C.D. Cal. 1985).
[83] Goodyear Tire & Rubber Co. v. Haegar, 137 S. Ct. 1178, 1186 (2017) (quoting Link v. Wabash R.R., 370 U.S. 626, 630-31 (1962)); *In re* Atl. Pipe Corp., 304 F.3d 135, 143 (1st Cir. 2002); Arthur Pierson & Co., v. Provimi Veal Corp., 887 F.2d 837, 839 (7th Cir. 1989).
[84] *See* Daniel J. Meador, *Inherent Judicial Authority in the Conduct of Civil Litigation*, 73 TEX. L. REV. 1805, 1805 (1995)).
[85] Marinechance Shipping, Ltd. v. Sebastian, 143 F.3d 216, 218 (5th Cir. 1998).
[86] *See* MacAlister v. Guterma, 263 F.2d 65, 68 (2d Cir. 1958).
[87] Opinion and Order, *In re* Ords. of this Ct. Interpreting Section 215 of the Patriot Act, No. Misc. 13-02, GID.C.00085, at 1–2 (FISA Ct. Sept. 13, 2013) (Saylor IV, J.) (referencing Am. C.L. Union v. FBI, 2015 WL 1566775, No. 11cv7562 (S.D.N.Y. Mar. 31, 2015)).

same parties and issues."[88] Similarly, in 2015, FISC Judge Michael Mosman denied Ken Cuccinelli and FreedomWorks a motion to intervene in a suit under the first-to-file rule. The parties and issues involved, as well as the relief sought, "extensively overlap[ped] with a suit previously commenced in the United States District Court for the District of Columbia."[89] The judge noted the risk of "duplicative effort and risk of inconsistent outcomes."[90] The movants, as plaintiffs in the other suit suing brought against largely the same individuals, presented the same standing questions present in the non-specialized, Article III entity.

The final category of inherent powers within the purview of Article III stems from the courts' ability to protect their own integrity, independence and reputation. These powers are well-recognized in the non-specialized, geographic courts, where they assume a range of powers to prevent fraud on the court, such as launching their own investigations,[91] or setting aside decisions if they are later determined to be based on fraudulent representations.[92] As addressed in Part V below, the FISC has had to implement a number of steps in this category to respond to government misrepresentation. Like all Article III courts, the FISC can sanction contumacious behavior and impose penalties on individuals who act in bad faith.[93] It has had occasion to do so, such as its March 2020 opinion forbidding not just Kevin Clinesmith, the attorney who made a deliberate, material misrepresentation to the court from appearing before it, but also *any* attorney under disciplinary or criminal investigation for their work before the FISC.[94]

D. *Control of Judicial Records*

Tension between the courts' Article III status and the specialized nature of their proceedings forcefully presents the problem who controls the courts' records. The issue stems from the subject matter before the court. The classification regime, which is designed to protect sensitive national security information, exists by

---

[88] *Id.* at 13.

[89] Opinion and Order, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things, No. BR 15-75, GID.C.00117, at 4 (FISA Ct. June 29, 2015) (Mosman, J.).

[90] *Id.* at 6.

[91] Universal Oil Prod. Co. v. Root Refin. Co., 328 U.S. 575, 580 (1946).

[92] As the Supreme court explained, the "historic power of equity to set aside fraudulently begotten judgments" is central to judicial integrity because "tampering with the administration of justice in [this] manner . . . involves far more than an injury to a single litigant. It is a wrong against the institutions set up to protect and safeguard the public." Hazel-Atlas Glass Co. v. Harford-Empire Co., 322 U.S. 238, 245, 246 (1946); *see also Universal Oil Prods. Co*, 328 U.S. at 580 (citing *Hazel-Atlas*, 322 U.S. 238); Chambers v. NASCO, Inc., 501 U.S. 32, 44 (1991) (quoting *Hazel-Atlas*, 322 U.S. at 245, 246).

[93] *See* Link v. Wabash R.R., 370 U.S. 626, 630–31 (1962); *Chambers*, 501 U.S. at 44 (citing *Link*, 370 U.S. at 630–31); *Ex parte* Burr, 22 U.S. (9 Wheat.) 529, 531 (1824); Roadway Express, Inc. v. Piper, 447 U.S. 752, 765–66 (1980); Goodyear Tire & Rubber Co. v. Haegar, 137 S. Ct. 1178, 1183–84 (2017) (holding that federal courts have inherent authority to sanction bad-faith conduct); Alyeska Pipeline Serv. Co. v. Wilderness Soc'y, 421 U.S. 240, 258–59 (1975) (quoting F.D. Rich Co. v. United States *ex rel.* Indus. Lumber Co., 417 U.S. 116, 129 (1974)).

[94] Corrected Opinion and Order, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00272, at 18 (FISA Ct. Mar. 5, 2020) (Boasberg, J.).

executive fiat and is thus part and parcel of the Executive Branch.[95] So, what happens when the third branch of government uses classified information as a basis for their work product? Although the government has become increasingly strident in its arguments, the FISC, for the most part, has guarded its constitutional authority while taking steps to protect against the unwitting release of harmful information.

1. Non-specialized Courts

The ability to decide a case lies at the heart of Article III authority: as the Supreme Court observed in 1825, "The judicial department is invested with jurisdiction in certain specified cases, in all of which it has the power to render judgment."[96] Neither the Executive Branch nor Congress can dictate to the courts how to decide cases or require a court to issue—or stop the court from issuing—a decision.

Article III(1) courts, accordingly, recognize their inherent authority "to protect their proceedings and judgments in the course of discharging their traditional responsibilities."[97] They have the power "to command respect for the court's orders, judgments, procedures, and authority"[98] Article III courts thus have supervisory power over their own records and files.[99] They can issue opinions, and they can seal, unseal, revoke, or rescind orders.[100] Courts routinely exercise jurisdiction over third party requests for records, as well as motions for common law or First Amendment right of access.[101] This ranges from applications for warrants to judicial opinions.[102] The tipping point is whether the records are

---

[95] *See* Exec. Order No. 13,526, 69 Fed. Reg. 53,599 (Aug. 27, 2004).

[96] Wayman v. Southard, 23 U.S. (10 Wheat.) 1, 22 (1825); *see also* Doe v. Apfel, No. 98-CV-182, 1999 WL 182669, at *3 (E.D.N.Y. Mar. 22, 1999) ("Courts have recognized that a judicial opinion deciding a case lies at the heart of the exercise of Article III powers.")

[97] Degen v. United States, 517 U.S. 820, 823 (1996).

[98] *In re* Stone, 986 F.2d 898, 902 (1996).

[99] Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 598 (1978). *See also* Gambale v. Deutsche Bank AG, 377 F.3d 133, 140–41 (2d Cir. 2004); Brown & Williamson Tobacco Corp. v. Fed. Trade Comm'n, 710 F.2d 1165, 1177 (6th Cir. 1983). In *Nixon*, SCOTUS held that neither the common law right of access nor the First Amendment, nor the Sixth Amendment guarantee of a public trial compelled the release of tapes from the custody of the District Court. *Nixon*, 435 U.S. at 609–11.

[100] *See, e.g.*, Fernandez v. United States, 81 S. Ct. 642, 644 (1961).

[101] *See, e.g.*, Douglas Oil v. Petrol Stops Nw., 441 U.S. 211 (1979); United States v. Bus. of Custer Battlefield Museum & Store, 658 F.3d 1188, 1192–96 (9th Cir. 2011); Chi. Trib. Co. v. Bridgestone/Firestone Inc., 263 F.3d 1304, 1310–13 (11th Cir. 2001); *In re* Nat'l Sec. Archive, No. 08 Civ. 6599, 2008 WL 8985358, at *1 (S.D.N.Y. Aug. 26, 2008); *In re* Am. Hist. Ass'n, 49 F. Supp. 2d 274, 295 (S.D.N.Y. 1999).

[102] *See, e.g.*, Doe v. Pub. Citizen, 749 F.3d 246, 265–68 (4th Cir. 2014); *Nixon*, 435 U.S. at 597; United States v. Kravetz, 706 F.3d 47, 56-59 (1st Cir. 2013); Lugosch v. Pyramid Co. of Onondaga, 435 F.3d 110, 119–24, 126 (2d Cir. 2006); *In re* Providence J. Co., 293 F.3d 1, 9–13 (1st Cir. 2002); United States v. Corbitt, 879 F.2d 224, 228 (7th Cir. 1989); *In re* Wash. Post Co., 807 F.2d 383, 390 (4th Cir. 1986); United States v. Smith, 776 F.2d 1104, 1107–13 (3d Cir. 1985); Belo Broad. Corp. v. Clark, 654 F.2d 423, 429–30 (5th Cir. 1981); United States v. Myers *(In re* Nat'l Broad. Co.*)*, 635 F.2d 945, 947–48 (2d Cir. 1980).

"judicial documents," understood as materials that go to "the exercise of Article III judicial power."[103] The moment at which they become so, the public has a presumptive right of access through the court in which they were filed.[104]

Article III courts continue to exercise jurisdiction over their records after the conclusion of the matter before the court.[105] They have "the inherent power to correct errors, remedy omissions, and correct clerical errors in its records."[106] They can "modify or lift protective orders that [have been] entered."[107] They can unseal records after the fact.[108] And they can re-open a case.[109] Their jurisdiction "is not exhausted by the rendition of its judgment, but continues."[110] Courts can punish those who might "disregard . . . the product of their functioning, their judgments."[111]

Should courts not be able to control their own determinations, it would undermine their constitutional role. "Courts of record can speak only by or through their records, and what does not so appear does not exist in law."[112] If the other branches could divest the courts of ownership over their records, they could alter the principles of law according to their own interests. They could hide malfeasance, with deep implications for democratic representation and accountability. And they could undermine the judicial branch. The core of judicial power *is* the ability to render decisions.

Like the powers addressed in the prior section, control of judicial records is an inherent power of Article III entities: in none of the cases in which courts have entertained requests for their records has Congress made a statutory grant of power over the records in question. Some courts go so far as to recognize it even when it conflicts with the statutorily-derived rules.[113] In one case, historians filed a motion requesting that a court unseal grand jury transcripts from an Espionage

---

[103] United States v. Amodeo (Amodeo II), 71 F.3d 1044, 1047–48 (2d Cir. 1995).
[104] *See, e.g.*, *Lugosch*, 435 F.3d at 119; *Amodeo II*, 71 F.3d at 1048–52; Stern v. Cosby, 529 F.Supp.2d 417, 420 (S.D.N.Y. 2007).
[105] *See, e.g.*, Doe v. United States, 853 F.3d 792, 798 (5th Cir. 2017) (A court "has the power to manage its records, even though the proceeding that generated those records has concluded."); Qureshi v. United States, 600 F.3d 523, 525 (5th Cir. 2010) ("That the court loses jurisdiction over the litigation does not, however, deprive the district court of its inherent supervisory powers." (citing Cooter & Gell v. Hartmarx Corp., 496 U.S. 384, 395 (1990)).
[106] 20 AM. JUR. 2D *Courts* § 25, Westlaw (database updated Feb. 2021) (citations omitted).
[107] *In re* Agent Orange Prod. Liab. Litig., 821 F.2d 139, 145 (2d Cir. 1987).
[108] *See Doe*, 749 F.3d at 252-53; Oregonion Pub. Co. v. U.S. Dist. Ct., 920 F.2d 1462, 1465–68 (9th Cir. 1990).
[109] United States v. Alcantara, 396 F.3d 189, 201–02 (2d Cir. 2005).
[110] Wayman v. Southard, 23 U.S. (10 Wheat.) 1, 23 (1825).
[111] Young v. United States ex rel. Vuitton et Fils S.A., 481 U.S. 787, 821 (1987) (Scalia, J., concurring) (emphasis omitted).
[112] 20 AM. JUR. 2D *Courts* § 22, Westlaw (database updated Feb. 2021) (citations omitted) ("The court record is the permanent account of that court's proceedings in particular cases, as well as the court's opinion or decision.")
[113] *See, e.g.*, *In re* Craig, 131 F.3d 99, 103 (2d Cir. 1997).

Act case seventy years prior.[114] The district court regarded the request as well within its power.[115] On appeal, the court noted that "Every federal court to consider the issue" has determined that "a district court's limited inherent power to supervise a grand jury includes the power to unseal grand-jury materials when appropriate."[116] The plaintiff "chose the Northern District of Illinois because it was the court that originally had supervisory jurisdiction over the grand jury in question."[117] He argued that this same court has continuing common-law authority over matters pertaining to that grand jury.[118] It did not matter that that the individual himself had no connection to the underlying action.[119] "[R]epresentatives of the press and general public must be given an opportunity to be heard on the question of . . . access to documents."[120] "To hold otherwise would raise First Amendment concerns."[121] The line is the point at which the documents become part of the judicial record. Accordingly, the case law includes materials deep in litigation, all the way up to final judgment.[122]

2. The Foreign Intelligence Courts

The first time this issue came to the FISC appears to have been in 2007, when Judge Bates, following *Warner Communications*, held that the FISC has supervisory jurisdiction over its own documents. He rejected the government's argument that the court lacked jurisdiction over its own opinions, writing, it would be "quite odd if the FISC did not have jurisdiction in the first instance to adjudicate a claim of right to the court's very own records and files."[123] In 2013, Judge Reggie Walton cited back to Bates's opinion to determine that the FISC continues to exercise jurisdiction over records following final determination of the matter before it, as reflected in the FISC Rules of Procedure.[124]

---

[114] Carlson v. United States, 837 F.3d 753, 756–61 (7th Cir. 2016).
[115] *Id.*
[116] *Id.* at 755–56.
[117] *Id.* at 757.
[118] *Id.*
[119] *Id.* at 759.
[120] *Id.* (quoting Jessup v. Luther, 227 F.3d 993, 997 (7th Cir. 2000)).
[121] *Id.*
[122] *See, e.g.*, United States v. Sealed Search Warrants, 868 F.3d 385, 390–96 (5th Cir. 2017) (holding that the district court had jurisdiction to determine whether a common law qualified right of access extended to pre-indictment search materials).
[123] Memorandum Opinion, *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, GID.C.00021, at 4 (FISA Ct. 2007) (Bates, J.). This opinion was also cited favorably in Opinion and Order, *In re* Motion for Consent to Disclosure of Ct. Recs. or, in the Alternative, A Determination of the Effect of the Ct's Rules on Statutory Access Rights, No. 13-01, GID.C.00082, at 2, (FISA Ct. June 12, 2013) (Walton, J).
[124] *In re* Motion, GID.C.00082, at 2–3. In that case, the Government had been trying to play two ends off against the middle: the Electronic Frontier Foundation (EFF) had brought a FOIA request in the District of Columbia for a FISC record. The Justice Department argued to the District Court that the FISC, by operation of Rule 62, had authority and control over copies of the opinion in the Government's possession. The EFF moved to stay and brought a parallel motion before the FISC. Before the specialized court, the Government contended that the FISC did not have jurisdiction because the copies of the opinion were in the Government's possession and EFF was thus asserting

FISC Rule 62 acknowledges the court's control of its records, allowing for the court to determine when to make its opinions public. In 2014, "in the exercise of its discretion,"[125] the FISC determined that it was "appropriate to take steps toward publication of any Section 215 Opinions" that were not subject to parallel FOIA litigation, without reaching the merits of an asserted right of public access under the First Amendment.[126] The court ordered the government to identify which opinions were and were not subject to the FOIA litigation and to "propose a timetable to complete a declassification review and submit to the Court its proposed redactions, if any."[127] The government returned with just one opinion, stating that it should be withheld in full.[128] The court did not accept the government's position.[129] Ordered to provide further documentation, the government determined "upon review and as a discretionary matter . . . that it does not object if this Court determines, pursuant to Rule 62(a), that those portions of the Opinion that are not classified and release of which would not jeopardize" an ongoing investigation be published.[130] Again, the court pushed back, leading to broader publication.[131]

Similarly, in February 2020, the FISC held that it had subject matter jurisdiction over a Motion for the Release of Court Records, and ancillary jurisdiction over the claim. The court recognized jurisdiction following the second prong of *Kokkonen v. Guardian Life Ins. Co. of Am.*, which allows jurisdiction outside of a statutory grant "to enable a court to function successfully, that is, to manage its proceedings, vindicate its authority, and effectuate its decrees."[132] In drafting opinions, an action contemplated by Congress, the FISC has the inherent

---

a statutory, and not a constitutional, right of access against the Executive Branch. The FISC rejected the Government's argument that it therefore lacked jurisdiction. *Id.*

[125] *See* Opinion and Order Directing Declassification of Redacted Opinion, *In re* Ords. of this Ct. Interpreting Section 215 of the Patriot Act, No. Misc. 13-02, GID.C.00104, at 3 (FISA Ct. Aug. 7, 2014) (Saylor IV, J.).

[126] *See In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02 GID.C.00085, at 17, 2013 WL 5460064, at *8 (FISA Ct. Sept. 13, 2013) (Saylor IV, J.).

[127] *Id.* at 18, 2013 WL 546064, at *8.

[128] *In re* Ords. of this Ct., GID.C.00104 at 4 (citing Second Submission of the United States in Response to the Court's Oct. 8, 2013 Order at 2, *In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02 (FISA Ct. Nov. 18, 2013), https://repository.library.georgetown.edu/handle/10822/1055928 [https://perma.cc/Q3TV-W9TR].

[129] Two days later, the court responded, ordering the Government to submit a detailed explanation of why the opinion could not be made public, even in redacted form, and to provide an unclassified explanation, under FISC Rule 7(j) to the two parties in the suit. Order, *In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02, GID.C.00181, at 2 (FISA Ct. Nov. 20, 2013) (Saylor IV, J.).

[130] *In re* Ords. of this Ct., GID.C.00104, at 5.

[131] The court reviewed the First Redaction proposal and questioned its scope. *Id.* at 5–6. On February 6, 2014, the Government submitted a second redaction proposal, which the court accepted and ordered to be published. *Id.* at 6–7.

[132] Opinion, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00267, at 11, 5 (FISA Ct. Feb. 11, 2020) (Collyer, J.) (quoting Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375, 380 (1994)).

power of any Article III court.[133] Thus, the FISCR, even as it decided *not* to exercise jurisdiction over a First Amendment right of access claim, simultaneously stated that it was declining to act on its ancillary authority.[134]

Despite the government's protestations, separation of powers means that the executive cannot bind the court and classify judicial opinions. No more so could it bind Congress—a fact recognized by rules in the Senate and House of Representatives that retain for the legislature the right to declassify material, even over Presidential objection.[135]

3. Mischaracterization of *Dep't of the Navy v. Eagan*

The decisions and underlying briefs that have been made public over the past five years demonstrate that the government has become increasingly strident—and inaccurate—in arguments put forward to support its claim that it has control over FISC opinions as an extension of its classification authority. In doing so, it frequently mischaracterizes *Dep't of the Navy v. Egan* as standing for the proposition that the authority to make national security judgments related to classified material lies solely with the Executive Branch.[136] The Executive Branch

---

[133] *See* 50 U.S.C.A. § 1803(a)(1), (b) (West).

[134] *In re* Ops. & Ords. by the FISC Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, 957 F.3d 1344, 1355–57, GID.CA.00013, at 22-23 (FISA Ct. Rev. 2020) (per curiam).

[135] *See* S. Res. 400, 94th Cong. § 8(a), (b)(1)–(5) (1976) (as amended through S. Res. 470, 113th Cong. (2014)), *reprinted in* S. PRT. NO. 116-4 (2019); Rules of H.R., 116th Cong., Rule X(g)(1) (2019). The Senate Select Committee on Intelligence ("SSCI") controls information in its own records. S. Res. 400 § 10. Members may declassify witness names and make classified material available to Senators and to the public. SSCI R.P., 116th Cong., Rules 8.10, 9.5, 9.7; S. Res. 400, § 8(a). The House Permanent Select Committee on Intelligence ("HPSCI") safeguards sensitive national security information. HPSCI R.P., 116th Cong., Rules 12(a)–(b), 14 (2019). Once the Executive Branch provides classified information, it becomes committee material. *Id.* at Rule 13 (labelling it "executive session material"). HPSCI imposes an oath on Committee members and determines which members of the House gain access to the material. *Id.* at Rule 14(d), (f), (g), (i). It can release classified information to the entire House or to the public. *Id.* at Rule 14(*l*); House Rule X(11)(g). The committee takes into account national defense and "[s]uch other concerns, constitutional or otherwise, as may affect the public interest of the United States." HPSCI R.P., Rule 14(f)(2)(A), (D).

[136] Dep't. of the Navy v. Egan, 484 U.S. 518 (1988). For examples of the government making this claim before the FISC, *see* United States' Reply Brief at 6, *In re* Certification of Questions of L. to the Foreign Intel. Surveillance Ct. of Rev., No. 18-01 (FISA Ct. Rev. Mar. 5, 2018), https://repository.library.georgetown.edu/handle/10822/1056123 [https://perma.cc/RES3-ET5A]; Opening Brief for the United States at 21–22, *In re* Certification of Questions of L. to the Foreign Intel. Surveillance Ct. of Rev., No. 18-01 (FISA Ct. Rev. Feb. 23, 2018) [hereinafter U.S. Opening Br.], https://repository.library.georgetown.edu/handle/10822/1056118 [https://perma.cc/X8EM-QUSY]; United States' Opposition to the Motion of the ACLU for the Release of Court Records at 11, *In re* Ops. and Ords. of this Ct. Containing Novel or Significant Interpretations of Law, No. Misc. 16-01 (FISA Ct. June 8, 2017) [hereinafter U.S. Opp. to Mot. of ACLU in No. Misc. 16-01], https://repository.library.georgetown.edu/handle/10822/1056116 [https://perma.cc/Y9VH-J622]; United States' Response to Movant's En Banc Opening Brief at 6, *In re* Ops.& Ords. of This Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08 (May 1, 2017), https://repository.library.georgetown.edu/handle/10822/1056064

also uses *Egan* to buttress its claim that the judiciary, unlike the Executive Branch, is ill-suited to make decisions bearing on national security.[137] A parallel trend is appearing in the government's submissions to other Article III courts.[138]

These claims do not square with the facts and holding of the case itself, which focused on a two-track system for an agency to take adverse action against government employees.[139] Under the relevant statute, employees had a right to a hearing through appeal to the Merit Systems Protection Board—a non-Article III tribunal.[140] The court held that the *statute* did not give the *board* control over security clearance determinations.[141] That decision had to be made by the appropriate agency inside the executive branch with the necessary expertise.[142] To the extent that the court looked to the Commander-in-Chief powers, it was as to whether the Executive had the authority to classify information in the first place, as well as to give, or deny, access to that information to individuals hired by the Executive. The court explained: "no one has a 'right' to a security clearance."[143]

Despite the government's effort to credit this case with standing for the

---

[https://perma.cc/GZG4-2SJ8]; United States' Legal Brief to the En Banc Court in Response to the Court's Order of March 22, 2017 at 11 n.4, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08 (FISA Ct. No. Apr. 17, 2017), https://repository.library.georgetown.edu/handle/10822/1056062 [https://perma.cc/3489-4WMV].

[137] *See, e.g.*, U.S. Opening Br., *supra* note 136, at 21 (citing and quoting *Egan*, 484 U.S. at 529, for "holding that predictive judgments related to national security risks 'must be made by those with necessary expertise in protecting classified information.'"); U.S. Opp. to Mot. of ACLU in No. Misc. 16-01, *supra* note 136, at 13 (raising concern that the FISC might err in making the determination as "judges with expertise in national security matters cannot equal [the expertise] of the Executive Branch" (quotation omitted) (citing *Egan*, 484 U.S. at 529)).

[138] It has not always been the case: in the years immediately following *Egan*, the Executive appropriately appealed to it in security clearance or background check cases. *See, e.g.*, Brief for Appellees, Stehney v. Perry, 101 F.3d 925 (3d Cir. 1996) (No. 96-5036); Brief for Appellees at 11–12, Ryan v. Reno, 168 F.3d 520 (D.D.C. Sept. 24, 1998) (No. 98-5036), 1998 WL 35240401. The Department of Justice still uses it in access-related contexts. *See, e.g.*, Brief of Defendant-Appellee at 32, Toy v. Holder, 714 F.3d 881 (5th Cir. Oct. 23, 2012) (No. 12-20471), 2012 WL 5294782, at *32. Over the past decade, however, the government has increasingly begun to claim that the case supports a broad reading of Executive Branch power and expected judicial deference. *See, e.g.*, Brief for the Petitioners at 42, Kerry v. Din, 576 U.S. 86 (Nov. 26, 2014), (No. 13-1402), 2014 WL 6706838, at *42; Brief for the United States at 23, Gen. Dynamics Corp. v. United States, 563 U.S. 478 (Dec. 13, 2010) (Nos. 09- 1298, 09-130), 2010 WL 5099376, at *23; Reply Brief for Defendant-Appellants at 12–13, ACLU v. U.S. Dep't of Def., 901 F.3d 125 (2d Cir. Nov. 3, 2017) (No. 17-779), 2017 WL 5152276, at *12–13; Brief for Respondents-Appellants at 41–42, 48, Dhiab v. Obama, 787 F.3d 563 (D.C. Cir. Mar. 6, 2015) (No. 14-5299), 2015 WL 1004459, at *41–42, *48; Brief of the Plaintiff-Appellee at 115, United States v. Sedaghaty, 728 F.3d 885 (9th Cir. Aug. 3, 2012) (No. 11-30342), 2012 WL 3342732, at *115; Brief for the Appellees at 17, 19, 34, Tenenbaum v. U.S. Dep't of Def., 407 Fed. App'x 4 (6th Cir. Dec. 2, 2009) (No. 09-1992), 2009 WL 4831977; Brief for the Defendants-Appellants at 42–43, John Doe Inc. v. Mukasey, 549 F.3d 861 (2d Cir. Feb. 14, 2008) (No. 07-4943), 2008 WL 6082598, at *42–43.

[139] *See Egan*, 484 U.S. at 526; 5 U.S.C.A. §§ 7511–14, 7531–33 (West).

[140] *See* 5 U.S.C.A. §§ 7513(d), 7532(c).

[141] *Egan*, 484 U.S. at 530–32.

[142] *Id.* at 527.

[143] *Id.* at 528.

broader proposition that the executive has untrammeled authority to classify material—including judicial opinions—the case says nothing of the sort.[144] As the court noted at the beginning of its decision "the narrow question presented by this case."[145] The statute in question did not transfer control over security clearances to the board, as access to classified material within the Executive Branch is overseen by the agency most directly involved in the sensitive areas.[146]

The tension between the FISC as an Article III entity and its handling of classified material, and how it is resolved, has far-reaching implications for the rule of law. It is a foundational tenet in Western democracies that for law to be legitimate, it must be known and promulgated. Some scholars go so far as to suggest that failure to do so may result in something not properly called law at all.[147] To the extent that FISC/FISCR opinions establish law, as they increasingly do, it becomes ever more important for this information to be public. As the foreign intelligence courts are increasingly put into a position of having to conduct oversight of the Executive, moreover, and to respond to Executive Branch malfeasance, there is a deeply democratic concern about whether the government should be able to control who sees judicial opinions that reveal the extent to which the government is acting within the law.

E. *Standing*

The special status of the FISC/FISCR as a specialized court—particularly one that deals with classified material—and its Article III status has also presented issues regarding standing. Statutory provisions require *in camera* and *ex parte* proceedings, as well as the sealing of certain records as they are passed up the chain of review. Yet the courts' decisions create precedent and operate as working law,

---

[144] This problem, while most pronounced in regard to *Egan*, is not limited to that case. Another case frequently cited in support of overbroad Executive Branch authorities is *CIA v. Sims*, 471 U.S. 159 (1985). In that case, individuals were seeking access to the names and institutional affiliations of those working on MKULTRA. *Id.* at 178–79. The Court noted that "Congress did not mandate the withholding of information that may reveal the identity of an intelligence source; it made the Director of Central Intelligence responsible only for protecting against *unauthorized* disclosures." *Id.* at 180. The Court went on to suggest, "[I]t is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process." *Id.* Although the holding was appropriately narrow ("We hold that the Director of Central Intelligence properly invoked § 102(d)(3) of the National Security Act of 1947 to withhold disclosure of the identities of the individual MKULTRA researchers as protected "intelligence sources." *Id.* at 181), the Government looks to the case in support of broad judicial deference to the Executive Branch *whenever* national security matters are on the line. *See, e.g.*, DEP'T OF JUST., GUIDE TO THE FREEDOM OF INFORMATION ACT, EXEMPTION 1, at 15–16 & n.77 (2019), https://www.justice.gov/oip/page/file/1197091/download [https://perma.cc/X8K3-SXVY] (citing *CIA v. Sims* in support of the proposition that the judiciary is and ought to be extremely deferential to the executive when national security matters are on the line).

[145] *Egan*, 484 U.S. at 520.

[146] *Id.* at 530–32.

[147] *See, e.g.*, LON L. FULLER, THE MORALITY OF LAW 39, 47 (1964).

with their contours having a direct impact on the rights of third parties—i.e., individuals who are not part of the application or certification processes. This tension results in numerous questions about who has the right to see the decisions of the court and the information on which those determinations are based.

The question came to the fore on the heels of the predecessor to the 2008 FAA, when Judge Reggie Walton held that Yahoo! could challenge directives under the 2007 Protect America Act (PAA) as violative of its customers' Fourth Amendment rights.[148] The court read the statutory language, which contemplated companies refusing to comply with directives as sufficient to address third party rights.[149] For the court, an unconstitutional directive could not be considered lawful, regardless of whose rights had been violated.[150]

Upon review, FISCR Judge Bruce M. Selya held that the communications service provider had standing to challenge the legality of directives issued pursuant to PAA.[151] The court pointed to the statutory language permitting a provider receiving a directive to challenge the legality of that directive.[152] The provider risked injury by assuming the burden it would have to shoulder to facilitate the government's request—an injury caused by the government and redressable by the court.[153]

Two key developments after those cases profoundly impacted the recent standing questions before the FISC/FISCR: first, the Supreme Court's decision in *Clapper v. Amnesty International*; and, second, the release of the Snowden documents and what they did to demonstrate an injury-in-fact.

Clapper involved a challenge to the constitutionality of Section 702.[154] The plaintiffs admitted to not knowing anything specific about how the targeting practices worked but provided evidence that (a) they had engaged in communications that came within Section 702 purview; (b) the government had a strong motive to intercept the communications because of the subject matter/identities; (c) the government had already intercepted a large number of calls

---

[148] Memorandum Opinion, *In re* Directives to Yahoo!, Inc. Pursuant to Sec. 105B of the Foreign Intel. Surveillance Act, No. 105B(g): 07-01, GID.C.00025, at 43 (FISA Ct. Apr. 25, 2008) (Walton, J.) (GID.C.000238 is the same opinion, but with different redactions).

[149] *Id.* at 54; *see* 50 U.S.C.A. § 1805(b)(g) (West) ("In the case of a failure to comply with a directive . . . [t]he court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful.")

[150] *In re Directives*, GID.C.00025, at 45.

[151] *In re* Directives to Yahoo! Inc. Pursuant to Sec. 105B of Foreign Intel. Surveillance Act, 551 F.3d 1004, 1009, GID.CA.00002, at 10 (FISA Ct. Rev. 2008) (Selya, J.).

[152] *See* 50 U.S.C.A. § 1861(f)(2)(A)(i) ("A person receiving a production order may challenge the legality of the production order or any nondisclosure order . . . by filing a petition."); *id.* § 1881a(i)(4)(A) ("An electronic communication service provider receiving a directive . . . may file a petition to modify or set aside such directive with the [FISC], which shall have jurisdiction to review such petition.")

[153] *In re Directives*, 551 F.3d at 1008-09, GID.CA.00002, at 8–10.

[154] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 404 (2013).

and emails involving a person who communicated regularly with the plaintiff; and (d) the government had the capacity to intercept the communications.[155] The Court determined that the plaintiffs' evidence was inadequate to establish standing because they relied on a "highly attenuated chain of possibilities" and displayed "no actual knowledge" as to whether plaintiffs ever specifically targeted.[156]

Less than four months after the Court issued its opinion in *Clapper*, the Snowden documents burst on the scene.[157] On June 6, 2013, the *Guardian* carried the first item: the now-infamous Section 215 secondary order showing that the National Security Agency (NSA) was collecting metadata from millions of Verizon customers, including from calls entirely within the United States.[158] The next day, the *Washington Post* and others reported that the NSA was accessing data through back doors into U.S. internet companies like Google and Facebook via PRISM.[159] The following day, the papers revealed that over a thirty-day period, some 97 billion internet data records and 124 billion telephony data records had been collected.[160] Inside the U.S., some 3 billion data elements were captured over a thirty-day period ending March 2013, giving the NSA more information on Americans inside the United States than Russia had over its citizens. On June 20, 2013, a Section 702 FISC order from 2010 approving targeting procedures, as well as the 2009 minimization procedures appeared, and, a week later, articles reported that the NSA was collecting and storing large quantities of Americans' Internet metadata.[161]

---

[155] *Id.* at 425–30 (Breyer, J., dissenting).

[156] *Id.* at 410–11 (majority opinion).

[157] For a detailed discussion of the documents released by Edward Snowden, the former Booz Allen Hamilton defense contractor at the National Security Agency, see generally BARTON GELLMAN, DARK MIRROR: EDWARD SNOWDEN AND THE AMERICAN SURVEILLANCE STATE (2020); GLENN GREENWALD, NO PLACE TO HIDE: EDWARD SNOWDEN, THE NSA, AND THE U.S. SURVEILLANCE STATE (2014); EDWARD JAY EPSTEIN, HOW AMERICA LOST ITS SECRETS: EDWARD SNOWDEN, THE MAN AND THE THEFT (2017).

[158] *See* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [https://perma.cc/UN4Q-874P].

[159] *See* Barton Gellman, *U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program*, WASH. POST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html [https://perma.cc/97B7-B8UE]; Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [https://perma.cc/E8UE-M28Q].

[160] *See* Glenn Greenwald & Ewan MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, GUARDIAN (June 8, 2013), https://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-datamining [https://perma.cc/AE5C-2PFF].

[161] *See* Glenn Greenwald & James Ball, *The Top Secret Rules that Allow NSA to Use US Data Without a Warrant*, GUARDIAN (June 20, 2013), https://www.theguardian.com/world/2013/jun/20/fisa-court-nsa-without-warrant [https://perma.cc/BZG3-L8C6]; Glenn Greenwald & Spencer Ackerman, *NSA Collected U.S. Email Records in Bulk for More than Two Years Under Obama*, GUARDIAN (June 27, 2013),

Over the following months, the *Washington Post*, *New York Times*, *Guardian*, and others published more information on Section 702 upstream collection, NSA monitoring of Americans' email and text communications into and out of the country, warrantless searches, access to smartphones, monitoring of banking and credit institutions, collection of contact lists, and the augmentation of all of this data with other public and commercial sources to develop sophisticated pictures of citizens' social relationships. When information began to emerge about the extent of surveillance overseas, even America's closest allies began to express alarm.[162]

The political climate shifted, with implications for all three branches of government. Within hours of the first leak, the Director of National Intelligence issued press releases acknowledging the Section 215 and Section 702 programs.[163] Soon thereafter, President Obama ordered the declassification of scores of documents.[164] In August, ODNI launched a Tumblr account, "IC on the Record," to provide more information and to make its case in the intense public debates that ensued.[165] The President simultaneously assembled a Review Group on Intelligence and Communications Technologies, which in December 2013 formally issued forty-six recommendations—including significant reforms of foreign intelligence

---

https://www.theguardian.com/world/2013/jun/27/nsa-data-mining-authorised-obama [https://perma.cc/SL7K-7VTR].

[162] In September 2013, for instance, Brazilian President Dilma Rousseff berated the United States at the United Nations General Assembly: "Meddling in such a manner in the life and affairs of other countries is a breach of international law, and, as such it is an affront to the principles that should otherwise govern relations among countries, especially among friendly nations." *News Wrap: Brazil President Calls U.S. Spying on Allies 'Totally Unacceptable,'* PBS NEWSHOUR (Sept. 24, 2013), https://www.pbs.org/newshour/show/news-wrap-brazil-president-calls-u-s-spying-on-allies-totally-unacceptable [https://perma.cc/H6VX-H844]. The following month, both French President Francois Hollande and German Chancellor Angela Merkel contacted the White House to condemn U.S. surveillance of the private calls and text messages of foreign nationals. Ian Traynor et al., *Angela Merkel's Call to Obama: Are You Bugging My Mobile Phone?*, GUARDIAN (Oct. 24, 2013), https://www.theguardian.com/world/2013/oct/23/us-monitored-angela-merkel-german [https://perma.cc/5HYK-MUGL].

[163] *See* James R. Clapper, *DNI Statement on Activities Authorized Under Section 702 of FISA*, OFF. OF THE DIR. OF NAT'L INTEL. (June 6, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/869-dni-statement-on-activities-authorized-under-section-702-of-fisa [https://perma.cc/5S5S-GSSQ]; James R. Clapper, *DNI Statement on Recent Unauthorized Disclosures of Classified Information*, OFF. OF THE DIR. OF NAT'L INTEL. (June 6, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information [https://perma.cc/8PAQ-DYWU].

[164] *See* The President's News Conference, 2 PUB. PAPERS 916 (Aug. 9, 2013), https://obamawhitehouse.archives.gov/the-press-office/2013/08/09/remarks-president-press-conference [https://perma.cc/384E-BZHK].

[165] *See* Off. of the Dir. of Nat'l Intel., IC ON THE REC., https://icontherecord.tumblr.com/ [https://perma.cc/UEY2-B7Q5] (last visited Feb. 25, 2021). This database is also accessible now via intel.gov. *IC on the Record Database*, INTEL.GOV, https://www.intel.gov/ic-on-the-record-database [https://perma.cc/GSN2-E4Z3] (last visited Feb. 25, 2021); *About*, OFF. OF THE DIR. OF NAT'L INTEL., https://www.dni.gov/index.php/ncsc-features/123-about?start=6 [https://perma.cc/YGN2-ETQK].

surveillance directed at U.S. persons.[166] The Privacy and Civil Liberties Board went from being underfunded and inactive to issuing its first, scathing report, centered on Section 215 collection and operation of the FISC.[167] To assuage the alarm being expressed by allies, Obama issued a new Presidential Policy Directive, underscoring that U.S. signals intelligence activities would henceforth "take into account that all persons should be treated with dignity and respect, regardless of their nationality or wherever they might reside, and that all persons have legitimate privacy interests in the handling of their personal information."[168] Special limitations would apply.

The legislature, too, became swept up in the political fallout. Scores of bills proposing far-reaching reforms suddenly appeared before Congress: from just three bills that had been brought forward the prior year (June 2012–May 2013), when specific clauses in FISA had actually been up for renewal, compared with the twelve months following the leaks, in which forty-two bills were before Congress, calling for everything from the elimination of the FISC/FISCR to a radical overhaul of FISA. Ultimately, Congress settled on the USA FREEDOM Act, which, *inter alia*, prohibited bulk collection under Section 215, FISA pen register/trap and trace authorities, and National Security Letters; required the appointment of at least five *amici* to address novel questions of law; required the Attorney General to submit any FISC/FISCR decision or order with a significant interpretation of FISA to Congress; and required a number of reports related to the operation of FISA authorities.[169]

The judiciary did not remain immune. In non-specialized Article III courts, a slew of cases challenged the constitutionality of the surveillance programs. It started the same day the *Guardian* published the secondary order, with *Klayman I* filed in D.D.C. against Section 215.[170] On June 11, 2013, the American Civil Liberties Union (ACLU) filed in S.D.N.Y., seeking a declaratory judgment that the NSA collection program exceeded the statutory authority and violated both the First

---

[166] *See* PRESIDENT'S REVIEW GRP. ON INTEL. & COMMC'NS TECHS., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES (Dec. 12, 2013). https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [https://perma.cc/6USQ-V634].

[167] *See* PRIVACY & C.L. OVERSIGHT BD., REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT AND ON THE OPERATIONS OF THE FOREIGN INTELLIGENCE SURVEILLANCE COURT (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf [https://perma.cc/K55Q-LFKM].

[168] Directive on Signals Intelligence Activities, Presidential Policy Directive/PPD-28, 2014 DAILY COMP. PRES. DOC. 31 (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/5UR5-MJWV]; *see also* The President's News Conference, *supra* note 164.

[169] *See* USA FREEDOM Act of 2015, Pub. L. No. 114-23, 129 Stat. 268.

[170] Klayman v. Obama, 957 F.Supp.2d 1 (D.C.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015).

and Fourth Amendments.[171] The following day Anna Smith, a neo-natal intensive care nurse in Spokane, filed a complaint in Idaho, requesting that the district court enjoin the NSA from collecting and analyzing her telephone data.[172] In July, EPIC filed in the Supreme Court for a writ of mandamus to demand that the FISC order be vacated,[173] and twenty-two organizations filed suit in the Northern District of California, asserting First Amendment violations.[174]

Like its sistren, the FISC found itself in the middle of a maelstrom. For thirty-five years, there had been no public filings before the FISC. But within days of the first leak, they began. On June 10, 2013, the ACLU and Yale Media Freedom Information Access Clinic (MFIAC) entered a motion to obtain FISC opinions that evaluated the meaning, scope, and/or constitutionality of Section 215.[175] Over the next few weeks, sixteen members of the U.S. House of Representatives filed an amicus brief in support of the motion, as did a number of advocacy organizations, such as the Center for Democracy and Technology (CDT), the EFF, and the First Amendment Coalition.[176] On July 15, 2013, they were joined by a formidable group of media representatives which included, *inter alia*, the Reporters Committee, ABC News, the Associated Press, Bloomberg News, Dow Jones & Company, Reuters, National Public Radio, the *Los Angeles Times*, *The New Yorker*, *Newsweek*, the *Washington Post*, and others.[177]

---

[171] ACLU v. Clapper, 785 F.3d 787, 799 (2d Cir. 2015) (challenged bulk collection).[171]

[172] *See* Smith v. Obama, 24 F. Supp. 3d 1005 (D. Idaho 2014), *vacated and remanded*, 816 F.3d 1239 (9th Cir. 2014).

[173] *In re* Elec. Privacy Info. Ctr., 571 U.S. 1023 (2013) (mem.) (petition filed on July 8, 2013 and denied on Nov. 18, 2013).

[174] Amended Complaint, First Unitarian Church of L.A. v. NSA, No. 13-cv-3287 (N.D. Cal. Sept. 10, 2013) (initial complaint was filed on July 16, 2013).

[175] Motion of the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic for the Release of Court Records, *In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02 (FISA Ct. June 12, 2013), https://repository.library.georgetown.edu/handle/10822/1055914 [https://perma.cc/6PDY-HLE2].

[176] Brief of Amici Curiae U.S. Representatives Amash, Broun, Gabbard, Griffith, Holt, Jones, Lee, Lofgren, Massie, McClintock, Norton, O'Rourke, Pearce, Salmon, Sanford, and Yoho in Support of the Motion of the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Access Clinic for the Release of Court Records, *In re Ords.*, No. Misc. 13-02, https://repository.library.georgetown.edu/handle/10822/1055916 [https://perma.cc/2SL6-KFVV]; Brief of First Amendment Coalition, American Civil Liberties Union, Center for Democracy and Technology, Electronic Frontier Foundation, and TechFreedom as Amici Curiae in Support of the Motions for Declaratory Judgment, *In re* Motion for Declaratory Judgment of Google Inc.'s First Amend. Right to Publish Aggregate Info. About FISA Orders, No. Misc. 13-03 (FISA Ct. July 8, 2013), https://repository.library.georgetown.edu/handle/10822/1055945 [https://perma.cc/4XQK-W2FA].

[177] Brief of Amici Curiae The Reporters Committee for Freedom of the Press, ABC, Inc., The Associated Press, Bloomberg, L.P., Dow Jones & Company, Inc., Gannett Co., Inc., Los Angeles Times, The McClatchy Company, National Public Radio, Inc., The New York Times Company, The New Yorker, The Newsweek/Daily Beast Company LLC, Reuters America LLC, Tribune Company, and The Washington Post in Support of the Motion for the Release of Court Records and the Motions for Declaratory Judgment, *In re* Ords. of this Ct. Interpreting Sect. 215 of the Patriot

With an eye towards their outraged customer base, corporate America engaged. On June 14, 2013, just over a week after the first article appeared, Yahoo! moved the court under FISC Rule 62(a) to request publication of an April 2008 opinion, which had been appealed to the FISCR and referenced in *In re Directives*, 551 F.3d 1004 (FISA Ct. Rev. 2008).[178] Five days later, Microsoft requested permission to disclose aggregate information regarding the FISC orders it had received.[179] Google, Facebook, and LinkedIn later entered similar motions.[180] Further filings and motions to the court to obtain opinions and orders continued into the autumn and beyond.[181]

Act, No. Misc. 13-02 (FISA Ct. July 15, 2013), https://repository.library.georgetown.edu/handle/10822/1055922 [https://perma.cc/DHY7-UTMC].

[178] Provider's Unclassified Motion Under FISC Rule 62 for Publication of this Court's Decision and Other Records, *In re* Directives Pursuant to Sec. 105B of the Foreign Intel. Surveillance Act, No. 105B(g) 07-01 (FISA Ct. June 14, 2013), https://repository.library.georgetown.edu/handle/10822/1055883 [https://perma.cc/R9DX-HJVV].

[179] Microsoft Corporation's Motion for Declaratory Judgment or Other Appropriate Relief Authorizing Disclosure of Aggregate Data Regarding Any FISA Orders It Has Received, *In re* Motion to Disclose Aggregate Data Regarding FISA Ords., No. Misc. 13-04 (FISA Ct. June 19, 2013), https://repository.library.georgetown.edu/handle/10822/1056041 [https://perma.cc/8D56-YABH].

[180] On June 18, 2013, Google moved to disclose statistics regarding receipt of FISC orders. Motion for Declaratory Judgment of Google Inc.'s First Amendment Right to Publish Aggregate Information About FISA Orders, *In re* Motion for Declaratory Judgment of a First Amend. Right to Publish Aggregate Info. About FISA Ords., No. Misc. 13-03 (FISA Ct. June 18, 2013), https://repository.library.georgetown.edu/handle/10822/1055940 [https://perma.cc/8PWR-HWT2]. On Sept. 9, 2013, Facebook moved to disclose aggregate data from FISA/FAA. Motion, *In re* Motion for Declaratory Judgment to Disclose Aggregate Data Regarding FISA Orders and Directives, No. Misc. 13-06 (FISA Ct. Sept. 9, 2013), https://repository.library.georgetown.edu/handle/10822/1056052 [https://perma.cc/T7G7-ES7H]. On Sept. 17, 2013, LinkedIn Corp. moved to report aggregated FISA data. Motion for Declaratory Judgment that LinkedIn Corporation May Report Aggregate Data Regarding FISA Orders, *In re* Motion for Declaratory Judgment that LinkedIn May Report Aggregate Data Regarding FISA Ords., No. Misc. 13-07 (FISA Ct. Sept. 17, 2013), https://repository.library.georgetown.edu/handle/10822/1056053 [https://perma.cc/5SKM-EGBV]. Judge Eagan consolidated all of the corporate cases on Sept. 18, 2013. Order, *In re* Motion for Declaratory Judgment to Report Aggregated Data Regarding FISA Ords., Nos. Misc. 13-03, 13-04, 13-05, 13-06, 13-07, GID.C.00211 (FISA Ct. Sept. 18, 2013) (Eagan, J.), https://repository.library.georgetown.edu/handle/10822/1053807 [https://perma.cc/L58G-5CRB].

[181] *See, e.g.*, Motion to Establish a Public Briefing Schedule Including the Filings of Briefs by Amici Curiae, for Leave for the Center for National Security Studies to File an Amicus Brief, and a Suggestion for Hearing En Banc, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-109 (FISA Ct. Oct. 17, 2013), https://repository.library.georgetown.edu/handle/10822/1056076 [https://perma.cc/4GF5-48XV]; Motion of the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Clinic for the Release of Court Records, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08 (FISA Ct. Nov. 7, 2013) (motion to unseal opinions addressing legal basis for bulk collection and assert First Amendment right of access), https://repository.library.georgetown.edu/handle/10822/1056054 [https://perma.cc/FDR9-HVBB]; Motion of ProPublica, Inc. for the Release of Court Records, *In re* Motion of ProPublica, Inc. for the Release of Ct. Recs., No. Misc. 13-09 (FISA Ct. Nov. 12, 2013) (invoking Rule 62 and a First Amendment right of access), https://repository.library.georgetown.edu/handle/10822/1056072

As a result of these motions, the court immediately had to address questions of standing. It was an area fraught with tension, particularly in light of the recent *Clapper* decision which had predated the unprecedented public access to the surveillance programs underway.

In September 2013, although the Government argued that the ACLU and Yale MFIAC had not been a party to the original judicial determination about bulk collection and therefore lacked standing, Judge Saylor found otherwise. Quoting *Clapper*, he noted, "To establish Article III standing, an injury must be concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling."[182] The injury caused by withholding the opinions was actual, as they were not, in fact, available to the public, the concern could be alleviated by the court, and the injury was sufficiently concrete and particularized because release would enhance the public debate and, in particular, the ACLU's activities. Withholding the opinions, on the other hand, was detrimental, because, the "ACLU's active participant in the legislative and public debates about the proper scope of Section 215 and the advisability of amending that provision is obvious from the public record."[183]

Judge Saylor determined that the other movant, Yale MFIAC, though, had neither indicated how release of information would aid its activities nor how failure to release opinions would be detrimental. The clinic had not participated in public debate about Section 215 and therefore, lacking a concrete and particularized injury, did not have standing.[184] Nearly a year later, the court granted a motion for reconsideration of the clinic's dismissal.[185] The decision recognized the recently-decided case, *Company Doe v. Public Citizen*, in which consumer advocacy organizations had asserted both a common law and First Amendment right of access to sealed documents.[186] The Fourth Circuit had held that the groups had standing

---

[https://perma.cc/T3SU-A4T5]; Motion in Opposition to Government's Imminent or Recently-Made Request to Resume Bulk Data Collection Under Patriot Act § 215, Cuccinelli v. Obama, No. Misc. 15-01 (FISA Ct. June 5, 2015), https://repository.library.georgetown.edu/handle/10822/1056098 [https://perma.cc/5CJP-746C]; Motion of the American Civil Liberties Union for the Release of Court Records, *In re* Ops. & Ords. of this Ct. Containing Novel or Significant Interpretations of Law, No. Misc. 16-01 (FISA Ct. Oct. 19, 2016) (invoking Rule 62 and a qualified First Amendment right of access of novel and significant interpretations of law from Sept. 11, 2001 through June 2, 2015), https://repository.library.georgetown.edu/handle/10822/1056108 [https://perma.cc/BJV5-PR62]; John Solomon and Southeastern Legal Foundation's Motion for Publication of Records, *In re* Motion for Publ'ns of Recs., No. Misc. 19-01 (FISA Ct. May 23, 2019) (invoking Rule 62, qualified First Amendment right of access, and common law right of access), https://repository.library.georgetown.edu/handle/10822/1056148 [https://perma.cc/68WU-FRTJ].

[182] Opinion and Order, *In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02, GID.C.00085, at 4 (FISA Ct. Sept. 13, 2013) (Saylor IV, J.) (quoting Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (internal quotations omitted)).

[183] *Id.* at 8–9.

[184] *Id.* at 9 & n.13.

[185] Opinion and Order Granting Motion for Reconsideration, *In re* Ords. of this Ct. Interpreting Sec. 215 of the Patriot Act, No. Misc. 13-02, GID.C.00221 (FISA Ct. Aug. 7, 2014) (Saylor IV, J.).

[186] Co. Doe v. Pub. Citizen, 749 F.3d 246 (4th Cir. 2014).

under Article III: "Their informational interests, though shared by a large segment of the citizenry, became sufficiently concrete to confer Art. III standing when they sought and were denied access to the information they claimed a right to inspect."[187] In the case of the FISC, the Court concluded in regard to the ACLU/MFIAC motion that principles of comity required that the motion be denied to the extent that it concerned FISC opinions at issue in separate suit brought by the ACLU in October 2011 in the Southern District of New York.[188]

On Nov. 7, 2013, the ACLU and Yale MFIAC filed another motion for declassification of opinions addressing bulk collection.[189] Two of the four opinions that the government determined were responsive to the request had already been made public in redacted form pursuant to FISCR Rule of Procedure 62(a).[190] The other two were subsequently released by the government in redacted form.[191] It was not until January 25, 2017 that the court ruled that the movants lacked standing for First Amendment right of access to the opinions.[192] FISC Presiding Judge Rosemary Collyer determined that the movants failed the experience and logic tests for a First Amendment qualified right of access.[193]

Meeting *en banc*, the FISC overturned the decision (6-5), saying that the standing requirement was satisfied.[194] The court recognized that proper analysis turns on whether the injury is concrete and actual, assuming the claim has merit. In this case, the movants lacked access to the classified opinions, satisfying the injury-in-fact requirement.[195] Judge Collyer certified the question to the FISCR on the grounds that it "would serve the interests of justice, a dispositive issue about standing was involved, and the split among the FISC Judges was very close and

---

[187] *Id.* at 264.
[188] *In re Ords.*, GID.C.00085, at 1–2.
[189] Motion of the American Civil Liberties Union, the American Civil Liberties Union of the Nation's Capital, and the Media Freedom and Information Clinic for the Release of Court Records, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08 (FISA Ct. Nov. 7, 2013), https://repository.library.georgetown.edu/handle/10822/1056054 [https://perma.cc/UF9P-FML6].
[190] Memorandum and Primary Order, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-158, GID.C.00086, 2013 U.S. Dist. LEXIS 157765 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.); Amended Memorandum Opinion and Primary Order, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things From [Redacted], No. BR 13-109, GID.C.00083 (FISA Ct. Aug. 29, 2013) (Eagan, J.).
[191] Opinion and Order, [Redacted], No. PR/TT [Redacted], GID.C.00091 (FISA Ct. [Redacted]) (Kollar-Kotelly, J.); Memorandum Opinion, [Redacted], No. PR/TT [Redacted], GID.C.00092 (FISA Ct. [Redacted]) (Bates, J.).
[192] Opinion and Order, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00127, at 2 (FISA Ct. Jan. 25, 2017) (Collyer, J.), *vacated by* GID.C.00140 (FISA Ct. Nov. 9, 2017) (en banc).
[193] *See id.* at 31–39.
[194] *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00140, 2017 WL 5983865 (FISA Ct. Nov. 9, 2017) (en banc).
[195] *See id.* at 7-8, 2017 WL 5983865, at *4.

involved a difference of opinion about the law to apply, among other considerations."[196]

On January 9, 2018, the FISCR accepted certification and publicly appointed an *amicus curiae*.[197] On March 16, 2018, the FISCR, agreeing with the *en banc* Court, held that Movants had met the requirements for standing.[198] Denial of access to the redacted materials constituted an injury-in-fact. For standing purposes, the movants "need not show that they are ultimately entitled to access the materials in question. Instead, they need only show that their claim is not immaterial nor wholly insubstantial and frivolous."[199] The court explained, "The movants have demonstrated that their claimed right of access is judicially cognizable, and we agree with the FISC majority that their claim cannot be characterized as 'completely devoid of merit,' or 'wholly insubstantial and frivolous,' even though it may ultimately be determined to be legally unsound.[200] The court reached neither the merits of the movants' claims nor jurisdictional issues.

Along with direct efforts to obtain documents from the court, which necessarily implicated questions of standing, following the publication of the foreign intelligence programs, motions began to appear requesting to intervene in cases. In 2015, for instance, Judge Michael Mosman exercised his discretion *sua sponte* to dismiss one such request, without reaching the standing question.[201]

F. *Subject Matter Jurisdiction*

Numerous cases have dealt with FISC jurisdiction over FISA-specific electronic surveillance, physical search, PRTT, business records, and review of Section 702 certifications; targeting procedures; and minimization.[202] A few cases address jurisdiction over outstanding matters once Congress removes the original authority. At the expiration of the PAA, for example, the FISA Court held that it retained jurisdiction even after the statute lapsed because it ordered that the directives remain in effect until their expiration.[203] This included jurisdiction over

---

[196] *In re* Ops. & Ords of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00141, at 1, 2018 WL 396244, at *1 (FISA Ct. Jan. 5, 2018) (Collyer, J.).
[197] *In re* Certification of Questions of L. to the Foreign Intel. Surveillance Ct. of Rev., No. 18-01, GID.CA.00006, at 2, 6, 2018 WL 2709456, at *1, *3 (FISA Ct. Rev. Jan. 9, 2018) (per curiam). The FISCR appointed the author of this Article as *amicus curiae*.
[198] *See id.* at 8-15, 2018 WL 2709456, at *4–7.
[199] *Id.* at 2, 2018 WL 2709456, at *1.
[200] *Id.* at 15, 2018 WL 2709456, at *7.
[201] *In re* Application of the FBI for an Ord. Requiring the Prod. Of Tangible Things, No. BR 15-75, GID.C.00117, 6–7 & n.6, 2015 WL 5637562, at *3 & n.6 (FISA Ct. June 29, 2015) (Mosman, J.).
[202] *See, e.g.*, *In re* Proc. Required by Section 702(i) of the FISA Amends. Act of 2008, No. Misc 08-01, GID.C.00028, 8-10, 2008 WL 9487946, at *4–5 (FISA Ct. Aug. 27, 2008) (McLaughlin, J.).
[203] Memorandum Opinion, *In re* Directives to Yahoo!, Inc. Pursuant to Sec. 105B of the Foreign Intel. Surveillance Act, No. 105B(g): 07-01, GID.C.00025, at 5–12 (FISA Ct. Apr. 25, 2008) (Walton, J.) (GID.C.000238 is the same opinion, but with different redactions); Memorandum

reviewing revised or additional procedures during the interim period.[204] Similarly, in the USA FREEDOM Act, Congress provided for a 180-day grace period before bulk collection ended.[205] The opinion, authored by Judge Mosman, began: "'Plus ça change, plus c'est la même chose,' well, at least for 180 days."[206] The determination of whether the court extends subject matter jurisdiction over a government request for surveillance or a court order evokes statutory questions about the subject matter before the court. Here, as the next Part discusses, the key question often turns on whether the technologies involved fit the statutory language or are able to cabin the amount and type of information sufficiently to ensure that the collection comports with FISA.

III. Cluster 2: New Technologies / Old Statutory Language

The second cluster of opinions centers on clarifying the type of surveillance allowable under FISA. Many of these appear to come about because of the basic question: how do new technologies fit with old statutory language? This impacts the type of information to be obtained, how it is to be collected, retained, accessed, and shared, and the ways in which technology can (or cannot) be used to limit collection or to ensure that certain information does not end up getting stored, analyzed, and shared. Three characteristics of technology drive the tension that marks this area.

First, technology changes the information available. Volume is the most obvious shift. Collecting information about one telephone call is quantitatively and qualitatively different from collecting all telephone calls that an individual, much less an entire city or country, makes. The shifting nature of information extends beyond this, as the *type* of data that can be collected also changes. Previously, geolocational data, detailed mapping of social relationships, and certain religious and medical information was unavailable. Now it is available, along with sophisticated algorithms that generate more insight into what people do, think, and believe and, critically, are *likely* to do, think, and believe, in the future. The key question that the court has to confront here is whether the type of information being proposed for collection is the *type* of information anticipated by the statute. What constitutes "electronic surveillance" in a digital age? What about dialing, routing, addressing, and signaling information (DRAS)? Or content versus non-content? These distinctions matter, because which statutory language applies, and what steps the government has to go through to get the data, changes depending on how it is characterized.

Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00242, at 2–5 (FISA Ct. June 18, 2008) (Kollar-Kotelly, J.).

[204] *See [REDACTED]*, GID.C.00242, at 5.

[205] *In re* Application of the FBI, GID.C.00117, at 1, 2015 WL 5637562, at *1.

[206] *Id.* at 1, 2015 WL 5637562, at *1 (translated: "The more things change, the more they stay the same.").

Second, how information can be obtained is rapidly changing in a way not contemplated by the statute. But the manner in which information is collected determines which statutory provision applies—and, consequently, how to analyze the collection under the First or Fourth Amendment. For instance, are searches of mobile devices physical searches, and thus within Title III, or ELSUR, and thus subject to Title I? What about intercepts? Stored communications? Business records? How should chats be considered, or communication within online gaming systems? What constitutes a "search" for Fourth Amendment purposes?

Third, FISC/FISCR jurisprudence makes apparent that technology also limits the ability of the government to meet constitutional requirements. What should the court do when confronted by the government's ability to collect data, but inability to determine crucial information about the target, such as their identity or location? What if the facility can be targeted, but the user cannot be confirmed? The same issue presents with the question of content versus non-content: how should the court handle post-cut-through-dialed-digits, or multi-communication transactions carrying entirely domestic conversations? What about the problem of complicated technologies that carry unintended consequences, or overcollection? How should the court deal with this in light of the statutory regime?

Technology is catapulting forward at a lightning rate. The average product life cycle in Silicon Valley is a matter of months. Title I has remained largely unchanged since 1978. Even the most recent major revisions were in 2015, six years ago. The government must adapt to the risks posed by these technologies, even as it uses them to try to head off national security threats. A growing body of jurisprudence addresses efforts by the court to reconcile the resulting tension between new technologies and swiftly antiquated statutory language.

A. *Electronic Surveillance and Physical Search*

The FISC, on multiple occasions, has acknowledged its jurisdiction over applications for electronic surveillance (ELSUR).[207] For Title I, probable cause applies to each of the facilities to be surveilled.[208] But interpretive problems have

---

[207] *In re* Application of the United States for an Ord. Authorizing the Physical Search of Nonresidential Premises and Pers. Prop., GID.C.00001 (FISA Ct. June 11, 1981) (Hart, J.), *reprinted in* S. REP. NO. 97-280, at 16–19 (1981). "The language of the FISA clearly limits the authority of the judges designated to sit as judges of the FISC to the issuance of orders approving 'electronic surveillance' as that term is defined in the act. *Id.* at 17. *In re* All Matters Submitted to Foreign Intel. Surveillance Court, 218 F. Supp. 2d 611, GID.C.00002 (FISA Ct. 2002) (Lamberth, J.). "Clearly this Court's jurisdiction is limited to granting orders for electronic surveillances and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the Act." *Id.* at 614, GID.C.0002, at 614.

[208] To order electronic surveillance, the Court must find "probable cause to believe that — (A) the target of the electronic surveillance is a foreign power or agent of a foreign power . . . . ; and (B) *each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used*, by a foreign power or agent of foreign power." 50 U.S.C.A. § 1805(a)(2) (West) (emphasis added)." The order must also specify "the identity, if known, or a description of the target of the electronic surveillance," "the nature and location of each of the facilities or places at which

been caused by new technologies and collection techniques. What constitutes a "facility"? What falls within ELSUR? What is the line between ELSUR and physical search? The stakes are high: things that do not come within the statutory definition are outside the court's purview.

Title I of FISA requires that the government establish probable cause that the foreign power (FP) or agent of a foreign power (AFP) being targeted will use the facility to be placed under surveillance.[209] The natural question then becomes, what is a facility? In 2007, the Justice Department's National Security Division proposed a change that would have eviscerated statutory protections. It argued that for electronic intercept of Internet communications, an entire cablehead or gateway should be considered a "facility" within the meaning of FISA. Because the Government could demonstrate that FP/AFPs use the Internet, the Justice Department argued the court should make a probable cause finding in regard to the facility generally and leave it to the government to determine specific targets, which communications related to them should be collected, and the like. This would have shifted analysis to the minimization procedures, making them something exercised by the executive branch—not an aspect of judicial review. To accept this reading, the court would have had to find that the backbone of the Internet was the facility under which surveillance would be directed.

Judge Vinson rejected this interpretation. Even if surveillance occurred on the backbone, the government would not be acquiring everything travelling across the circuit. Instead, only content to or from particular phone numbers or addresses would be obtained. He therefore understood those particular numbers as the facility being targeted. Zooming out and applying probable cause, the government's interpretation would create a disconnect between the court's probable cause finding, who was actually being targeted for surveillance, and what was being required. As a textual analysis, if the government was only acquiring a small fraction of the communications at a larger facility, and selecting communications by reference to other, smaller facilities (like phone numbers), then the facilities at which the acquisition of the communications is being directed are the smaller facilities. The court rejected the government's request.[210]

The volume of information that would thereby be obtained under the government's interpretation, and the implications for U.S. citizens' communications flowing into and out of the U.S., raised jurisdictional concerns. The court wrote:

---

the electronic surveillance will be directive, if known," and "the type of information sought to be acquired and the type of communication or activities subjected to the surveillance." *Id.* § 1805(c)(1)(A) – (C).

[209] *See* 50 U.S.C. § 1805(a)(2)(B).

[210] *See* Order and Memorandum Opinion, *In re* [REDACTED], No. [REDACTED], GID.C.00012, at 6–10, 12–16 (FISA Ct. Apr. 3, 2007) (Vinson, J.) (rejecting the government's identification of facilities at which surveillance was directed for purposes of the probable cause requirement now codified at § 1805(a)(2)(B) and denying application for lack of probable cause).

> [G]iven the large number of selectors involved [REDACTED] it appears likely that this surveillance would acquire some indeterminate number of communications to or from persons in the United States. See, e.g., id. at 6-8. [REDACTED] In view of this apparent likelihood, the government's implicit request that the Court exercise jurisdiction over the submitted application, the Court's prior acceptance of jurisdiction in Docket No. [REDACTED] and prior decisions of this court that have accepted jurisdiction in similar cases [REDACTED] I assume for purposes of this order and opinion that this case does involve "electronic surveillance" as defined by FISA, such that this Court has jurisdiction. However, I believe that the jurisdictional issues regarding the application of FISA to phone numbers and e-mail addresses that are used exclusively outside the United States merit further examination.[211]

In 2019, the issue again arose in the context of the statutory requirement that the facilities at which ELSUR is directed must be used (or be about to be used) by the target of the surveillance.[212] The court appointed *amici curiae* to assist, one of whom took the position that the proposed facility did not meet the statutory definition. The amicus argued for a narrow interpretation of "facilities" to ensure that FISA be applied with caution in a technological context that could not be foreseen when the statute was first enacted. Presiding Judge Rosemary Collyer concluded otherwise, stating that Congress "did not intend the term 'facilities' in § 1805(a)(2)(B) to be interpreted in that narrow fashion.[213] To support its broad reading of the term, the court looked to the dictionary from 1976, which defined facility in relevant part as "the means used to facilitate an action or process; convenience; provision: *the facilities of a library*."[214] Judge Collyer further noted that the statutory language (which referred to "the facilities or places") suggested that Congress meant it to apply widely.[215] She also noted that while the meaning of what constituted a facility for ELSUR may have been fixed at the time when the statute was enacted, new applications of the term could arise in light of new technologies.[216]

The most remarkable part of the decision is that the court went on to rule that the statutory requirement that probable cause apply to "each" facility did not mean that it had to apply to "all" facilities; instead, the court determined that the probable cause standard "requires only a fair probability."[217] The new technology

---

[211] Order and Memorandum Opinion, *In re* [REDACTED], No. [REDACTED], GID.C.00012, at 8 n.12 (FISA Ct. Apr. 3, 2007) (Vinson, J.).
[212] Opinion, *In re* [REDACTED] Non-U.S. Persons, No. 19-218, GID.C.00287, at 1–2 (FISA Ct. Mar. 5, 2020) (Collyer, J.).
[213] *Id.* at 6.
[214] *Id.* at 7 n.5 (emphasis in original) (citing THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 469 (new college ed. 1976)).
[215] *Id.* at 7–9.
[216] *Id.* at 12.
[217] *Id.* at 23.

essentially made it possible to target multiple facilities, but then failed to provide a way to delimit the number of facilities thus surveyed. Because the government stated that it could not separately target each facility "without altering the manner in which the surveillance would be conducted," instead of rejecting the use of the technology to carry out the surveillance, the court relaxed the probable cause "each" requirement.[218] The case is a great example of the problem created where technology allows for acquisition but not specificity in a manner that comports with the statutory language.

Which collection techniques fall within the definition of ELSUR matters because whether the court has jurisdiction over the type of communication in question turns, at least for purposes of Title I, on the status of those communications. In one heavily redacted opinion, it appears that the government interpreted the statutory provisions in a manner with which the court disagreed, issuing "an order authorizing electronic surveillance . . . of all communications to or from" a particular facility.[219] The court objected on the grounds that it did not have jurisdiction over the type of foreign intelligence collection it was being asked to authorize.[220] In another opinion, the court held that the type of surveillance requested did constitute "electronic surveillance" as defined in FISA, but it was not clear who constituted the type of carrier contemplated by the statute.[221]

The language of some of the opinions suggests that the government is trying to bring collection otherwise conducted outside the statute into the FISA framing—which is consistent with Jack Goldsmith's discussion of his time at OLC.[222] For instance, in one opinion whose date is redacted (likely 2005), the court set out its reasons for adding clarification for its jurisdiction and the scope of its authorization into the surveillance order language.[223] In this case, the court was focused on an FBI application. The judge wrote that the court did not have jurisdiction, "to authorize the acquisition of wire communications that fall outside the applicable" statutory language.[224] The Court also recognized that the "Executive Branch has long asserted the authority, consistent with but outside of FISA, to acquire [REDACTED] other than those described in [REDACTED].[225]

As with the definition of ELSUR and facilities, FISC opinions that have been made public demonstrate a struggle with how to incorporate mobile

---

[218] *See id.* at 23–24.
[219] Memorandum Opinion as to Electronic Surveillance Pursuant to [REDACTED], [REDACTED], No. [REDACTED], GID.C.00143, at 3 (FISA Ct. [REDACTED]) (Kollar-Kotelly, J.).
[220] *See id* at 3.
[221] *See* Memorandum Opinion, [REDACTED], No. [REDACTED], GID.C.00149, at 1, 4–7 (FISA Ct. [REDACTED]) (Hogan, J.).
[222] *See* Donohue, *supra* note 30.
[223] Order and Opinion, [REDACTED], No. [REDACTED], GID.C.00153 (FISA Ct. [REDACTED]) (Davis, J.) (pincite is to the opinion, not the order).
[224] *Id.* at 3.
[225] *Id* at 4.

technologies and roving surveillance into the statutory language.[226] Judge Thomas Hogan's opinion that the government had exceeded the scope of its statutory authorization provides one example.[227]

So, too, does the line between ELSUR and physical search fall under pressure in the context of new technologies. In one case that the court confronted, the government argued, based on the use of the term "intercept" in FISA legislative history and Title III of the Omnibus Crime Control and Safe Streets Act of 1968, that it should be understood in a particular manner.[228]

With an eye towards new technologies, it is worth mentioning that, to the extent that information is obtained directly from a mobile device itself, as opposed to communications obtained in transit (e.g., Section 702 upstream collection), then a colorable argument could be raised that what is happening is actually a physical search, which must comport with Title III. While there is no released opinion that appears to address this, it would match with the general tension in this category. If you are getting information directly from a device, then it is not an intercept. Simultaneously, it is different from the type of search (i.e., of real property) that drove the language in the 1994 Act. A similar, colorable argument could be raised for search of any stored data.

As a matter of physical search, the FISC determined in 1981 that it did not have authority for physical searches under ELSUR.[229] The distinguishing factor was whether the court could authorize the search of *real* property. The FISC determined that "the clearly expressed intent of Congress to withhold authority to issue orders approving physical searches" makes it moot to "consider whether a judge of the FISC nevertheless has some implied or inherent authority to do so."[230] It continued, "[W]here a given authority is denied it cannot be supplied by resort to principles of inherent, implied or ancillary jurisdiction."[231] This holding suggests that the government had been arguing that the Court could grant physical search warrants by nature of its status as an Article III court. After Congress amended FISA, following the Aldrich Ames investigation, to allow for physical search, the

---

[226] *See* Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00138, at 4 (FISA Ct. [REDACTED]) (Hogan, J.).
[227] *Id.* at 1.
[228] Memorandum Opinion, [REDACTED], No. [REDACTED], GID.C.00139, at 3 n.3 (FISA Ct. [REDACTED]) (Feldman, J.). Because of the redactions in the document, we don't know exactly what the surveillance was or which side of the divide it fell on; however, we do know that it was relatively recent, having been issued sometime between 2010 and 2017, when Judge Feldman, who authored the opinion, served on the court.
[229] *In re* Application of the United States for an Ord. Authorizing the Physical Search of Nonresidential Premises and Pers. Prop., GID.C.00001 (FISA Ct. June 11, 1981) (Hart, J.), *reprinted in* S. REP. NO. 97-280, at 16–19 (1981).
[230] *Id.* at 19.
[231] *Id.*

court acknowledged that its jurisdiction extended to granting warrants to search real property.[232]

B. *Pen Register and Trap and Trace Devices*

A number of the opinions that are publicly available center on pen register/trap and trace (PRTT).[233] As a matter of the incorporation of new technologies into the statutory language, the court has had to address at least three prominent issues: email and Internet metadata, content versus non-content, and post-cut-through-dialed-digits (PCTDDs).

Perhaps the most significant opinion in this realm was the decision by Judge Colleen Kollar-Kotelly sometime in or around 2004, which transferred parts of the Terrorist Surveillance Program to the FISA framing.[234] It appears to be the first opinion to expand PRTT beyond individual targets. The document notes that the government request implicates a "much broader type of collection than other pen register/trap and trace applications and therefore presents issues of first impression."[235] The court held that bulk Internet metadata collection was consistent with 50 U.S.C. Sections 1841–46 in that it met the definition of what constitutes a pen register or trap and trace, the type of information to be obtained did not include the contents of the communications, the type of data constituted dialing, routing, address, or signaling information (DRAS), and the manner in which it would be obtained was consistent with the statute.[236] It is not clear from the redacted version whether the court considered how Internet information could be construed differently because of the type of information that was revealed. Subject information in an email, for instance, frequently reveals what the message is about—indeed, that is the whole point of the subject line. So, too, does knowing which URLs or websites are visited indicate the content of the material being accessed.

---

[232] *See supra* text accompanying notes 5-15. Intelligence Authorization Act for Fiscal Year 1995, Pub L. No. 103-359, sec. 807(a)(3), § 302(a)(1)(A)(i), 108 Stat. 3423, 3444 (1994) (codified as amended at 50 U.S.C.A. § 1822(a)(1)(A)(i) (West)); *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 614, GID.C.00002, at 614 (FISA Ct. 2002) (Lamberth, J.) ("Clearly this Court's jurisdiction is limited to granting orders for electronic surveillances and physical searches for the collection of foreign intelligence information under the standards and procedures prescribed in the Act.")

[233] *See, e.g.*, Supplemental Opinion and Primary Order, [REDACTED], No. [REDACTED], GID.C.00034 (FISA Ct. Dec. 18, 2008) (Vinson, J.); Memorandum Opinion, [REDACTED], No. PR/TT [REDACTED], GID.C.00092 (FISA Ct. [REDACTED]) (Bates, J.) (circa 2010–2013).

[234] *See* Opinion and Order, [REDACTED], No. PR/TT [REDACTED], GID.C.00091, at 1, 10 n.8 (FISA Ct. [REDACTED]) (Kollar-Kotelly, J.) (circa 2004-2009).

[235] *Id.* at 2. Kollar-Kotelly, J. added, "This is the first application presented to this Court for authority to [READACTED] under pen register/trap and trace authority. The Court understands that FBI devices implementing prior pen register/trap and trace surveillance authorized by this Court have not obtained [REDACTED]." *Id.* at 10 n.8.

[236] *Id.* at 2–3.

The court, nevertheless, held that the restrictions on retention, accessing, use, and dissemination of such information satisfies the requirements of 50 U.S.C. § 1842, and that the installation and use of the PRTT devices for bulk email and Internet metadata collection is consistent with the First and Fourth Amendments—despite the acknowledgment that "The raw volume of the proposed collection is enormous," and will result in the collection of USPs inside the country "who are not the subject of any FBI investigation."[237]

The problem with other data being collected along with DRAS was presented to the court sometime between 2010 and 2013. Judge Bates noted that the court had set certain categories that the government could collect, and others which it could not—but that the government had not abided by the order. According to Judge Bates, "the government acknowledges that NSA exceeded the scope of authorized acquisition continuously during the more than [REDACTED] years of acquisition under these orders."[238] Although the government stated that "all the technologies used by NSA to implement the authorizations granted by docket number PR/TT [REDACTED] and previous docket numbers only collect, or collected, authorized metadata," there had been systemic overcollection *continuously* since the initial authorization.[239] As a result, nearly *every* PRTT record generated by the program included some data that was not authorized for collection.[240] A second ruling by Judge Bates addressed limited collection authority for several categories of metadata collection.[241]

These opinions generate insight into the difficult role that the court has of ensuring that the government is collecting and using data in the approved manner. They also illustrate the challenge of what to do with information collected outside the prescribed limits.[242] With very few exceptions, the government's position has been to request that it be allowed to keep the data.

PCTDDs (i.e., the use of numbers on a telephone keypad to navigate commercial activity) have also caused concern, not least because, by definition, they include content. When a customer calls the bank and uses the number pad to transfer money from her savings account to her checking account, she enters her social security number, her bank account number, and how much money is being transferred. This is content. In 2016, the court had to determine whether it had the

---

[237] *Id.* at 1–2, 39. There is another Kollar-Kotelly opinion on PRTT issues, together with business records, but heavily redacted and not thoroughly analyzed. *See* Opinion, [REDACTED], No. [REDACTED], GID.C.00159, at 3–4 (FISA Ct. [REDACTED]) (Kollar-Kotelly, J.) (circa 2002-2009) (applying the rule in *Smith v. Maryland*, 442 U.S. 735, 740, 743–44 (1979), indicating persons had no legitimate expectation of privacy in phone numbers dialed, and thus, did not have a "Fourth Amendment right to keep the information form being turned over to the Government.").

[238] *[REDACTED]*, GID.C00092, at 2–3.

[239] *Id.* at 20.

[240] *Id.* at 20–21

[241] Supplemental Opinion and Amendment to Primary Order, [REDACTED], No. [REDACTED], GID.C.00136 (FISA Ct. [REDACTED]) (Bates, J.).

[242] *See* discussion, Part V, *infra*.

authority to authorize the collection of all PCTDDs under a PRTT order. The FISCR found in the affirmative—once again, because the technology was not sophisticated enough to distinguish between content and non-content DRAS—subject to a prohibition on the affirmative investigative use of any content.[243] The court of review also found that "incidental collection of content information during the collection of post-cut-through digits . . . is constitutionally reasonable, even when done without a probable-cause warrant."[244]

C. *Business Records, Bulk Collection and § 702*

A number of opinions accept the proposed minimization procedures for tangible things.[245] The most important law and technology question that arose in this context appears to have been whether in Section 215 could be used for bulk collection of internet and telephone metadata.[246] However, the first time the court appears to have confronted the issue, it summarily applied *Smith v. Maryland*, and, after just a half a page of discussion, it granted the order.[247]

Further questions accompanied the querying of the data obtained. Training proved a persistent concern.[248] In 2013, the query issue again arose. Judge Claire Eagan determined that non-content queries met the requirements of the Fourth

---

[243] *In re* Certified Question of L., 858 F.3d 591, 610-11, GID.CA.00003 at 37–38 (FISA Ct. Rev. 2016) (per curiam).

[244] *Id.* at 605, GID.CA.00003, at 26. The court found that the following factors rendered the search "reasonable" for Fourth Amendment purposes: "(1) the paramount interest in investigating possible threats to national security; (2) the investigative importance of having access to the dialing information provided by the post-cut-through digits, (3) the incidental nature of the collection of content information from post-cut-through digits, (4) the relatively slight intrusion on privacy entailed by the acquisition of post-cut-through digits, (5) the prohibition against the use of any content information obtained from the pen register or trap-and-trace device, (6) the steps taken by the government to minimize the dissemination of post-cut-through digits; and (7) the fact that FISA pen register interceptions are conducted only with the approval and under the supervision of a neutral magistrate, in this case a FISC judge." *Id.* at 607–08, GID.CA.00003, at 31–32.

[245] *See, e.g.*, Memorandum Opinion, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 14-96, GID.C.00103 (FISA Ct. June 19, 2014) (Zagel, J.).

[246] Business records and bulk collection are covered by Foreign Intelligence Surveillance Act of 1978, § 501, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C.A. § 1861 (West)).

[247] Opinion, [REDACTED], No. [REDACTED], GID.C.00159, at 3–4 (FISA Ct. [REDACTED]) (Kollar-Kotelly, J.) (circa 2002–2009). Note also that for telephony metadata, the court as a consequence had to address tension between 50 U.S.C.A. § 1861 and 18 U.S.C.A. §§ 2702–2703 (§ 2702 gives apparently exhaustive set of circumstances under which service provider may provide non-content records; § 2703 describes apparently exhaustive set of means by which government may compel provider to produce them). *See* Supplemental Opinion, *In re* Prod. of Tangible Things From [REDACTED], No. BR 08-13, GID.C.00033 (FISA Ct. Dec. 12, 2008) (Walton, J.) (deciding call detail records were obtainable via § 1861).

[248] At one point, for instance, the NSA created an email distribution list with 189 analysts on it, only 53 of whom had been trained, and then shared the business records query results with them. The court went on to order a more detailed report, as it was concerned that the NSA was querying the metadata without reasonable articulable suspicion (RAS). Supplemental Opinion and Order, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things from [REDACTED], No. BR 09-15, GID.C.00048, at 3, 5–6 (FISA Ct. Nov. 5, 2009) (Walton, J.).

Amendment.[249] Two months later, in October, Judge McLaughlin agreed with Judge Eagan that collection of bulk telephone metadata met the Section 215 relevance standard and, under *Smith*, that the Fourth Amendment did not apply. Although Justice Sonia Sotomayor had suggested in *United States v. Jones* that the Supreme Court may need to revisit third party doctrine, the principle remained intact.[250]

Once the statutory language changed in 2015 to prohibit bulk collection, the court had to turn its attention to the new statutory requirements, as is typical whenever Congress alters FISA.[251] One of the most notable decisions at the time was authored by Judge Mosman, who approved continued retention of bulk telephony metadata under Section 215 after November 28, 2015 and limited access to two purposes: first, for a limited time as a comparison set to verify the completeness and accuracy of call detail records produced under the targeted (non-bulk) production orders issued after November 28, 2015; and, second, for retention to comply with litigation-related obligations.[252]

In 2015, Judge Hogan also addressed the statutory changes, providing detail about the new requirements under § 1861.[253] The court noted that the statute requires for applications to have a specific selection term to be used as the basis for production. For production on an ongoing basis of call detail records, there must also be a statement of facts showing there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term are relevant to an authorized international terrorism investigation as well as a reasonable articulable suspicion that those terms are associated with a foreign power.[254]

In sum, the main emphasis of the court's jurisprudence in the statutory realm has to do with how to fit new technologies into the statutory language and, when Congress does alter the statute, how to implement the new provisions in light of the

---

[249] Amended Memorandum Opinion and Primary Order, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-109, GID.C.00083, at 6–9 (FISA Ct. Aug. 29, 2013) (Eagan, J.). *See also* United States v. Jones, 565 U.S. 400 (2012).

[250] Memorandum and Primary Order, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-158, GID.C.00086, at 5 (FISA Ct. Oct. 11, 2013) (McLaughlin, J.).

[251] *See, e.g.*, Opinion and Ordrt, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things, Nos. BR 15-75, Misc. 15-01, GID.C.00117, at 1 (FISA Ct. June 29, 2015) (Mosman, J.) (authorizing continued collection of bulk telephone metadata under § 215 for 180 days until the USA FREEDOM Act takes effect); Memorandum Opinion, *In re* Application of the FBI for an Ord. Requiring the Prod. of Tangible Things, Nos. BR 15-77, 15-78, GID.C.00114, at 13 (FISA Ct. June 17, 2015) (Saylor IV, J.) (determining that the USA FREEDOM Act reinstated the § 215 BR provision of the PATRIOT Act that had lapsed on June 1, 2015).

[252] Opinion and Order, *In re* Application of the FB. for an Ord. Requiring the Prod. of Tangible Things from [REDACTED], No. BR 15-99, GID.C.00122, at 6–8 (FISA Ct. Nov. 24, 2015) (Mosman, J.).

[253] Memorandum Opinion, *In re* Application of the FBI for Ords. Requiring the Prod. of Call Detail Recs., No. [REDACTED], GID.C.00123, at 3–6 (FISA Ct. Dec. 31, 2015) (Hogan, J.).

[254] *See id.*; 50 U.S.C.A. § 1861(b) (West).

technologies available. To the extent that the latter represents an effort by the legislature to get up to speed on new forms of collection and communication, the basic struggle remains: how to think about the quality of the information available, how to access it, and how to take account of limitations that would otherwise protect individuals from undue government surveillance of their private lives.

IV. Cluster 3: Constitutional Rights

The Church Committee hearings, which gave birth to FISA, showed that the intelligence community had placed Americans under surveillance based on what they said and did—and with whom. Decisions were made on the basis of political views, and in some cases, religious beliefs. Targets ranged from the Women's Liberation Movement to "every Black Student Union and similar group regardless of their past or present involvement in disorders," federal judges, Members of Congress, and political candidates.[255] Intelligence collection reflected partisan politics. In drafting FISA, the Senate thus expressed particular concern "that the surveillance authorized . . . not result in the retention or dissemination of information which would adversely affect the exercise of [F]irst [A]mendment rights."[256]

Ten separate requirements incorporated into FISA, accordingly, center on the First Amendment, with the result that *every* form of surveillance that can target a U.S. person is explicitly limited. No U.S. person targeted for ELSUR or physical search can "be considered an agent of a foreign power solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution of the United States."[257] Similarly, the Attorney General can apply for an order or extension of PRTT "provided that [] investigation of a United States person is not conducted solely upon the basis of activities protected by the [F]irst [A]mendment to the Constitution."[258] The applicant must certify to the Court that the investigation is not premised on First Amendment activities.[259] Similar requirements mark applications for business records.[260] For Sections 703 and 704, similar to Title I, the judicial determination as to whether a U.S. person is or is not a foreign power or an agent thereof cannot be premised solely on First Amendment activities.[261]

---

[255] *FBI Oversight: Hearing Before the Subcomm. on Civ. & Constitutional Rts. of the H.R. Comm. on the Judiciary*, 94th Cong., pt. 3, at 426–27 (1976).
[256] *Foreign Intelligence Surveillance Act of 1978*, S. REP. NO. 95-701, at 42 (1978).
[257] 50 U.S.C.A. § 1805(a)(2); *see id.* § 1824(a)(2)(A).
[258] *Id.* § 1842(a)(1).
[259] *Id.* § 1843(a).
[260] *Id.* § 1861(a)(1) (stating that the FBI may make an application for an order requiring the production of tangible things "for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment.") The statute also states: "An investigation conducted under this section shall…not be conducted of a United States person solely upon the basis of activities protected by the first amendment." *Id.* § 1861(a)(2).
[261] *Id.* §§ 1881b(c)(2), 1881c(c)(2).

With such an emphasis on the First Amendment, one might expect, correspondingly, a significant number of opinions to address it. But, thus far, only two public opinions handle First Amendment issues in any depth. Indeed, there are triple the number of cases addressing the First Amendment right of access, which derives not from the associational rights, but from the right to petition.

What has garnered considerably more attention than either of these areas are concerns related to the Fourth Amendment. FISA requires that acquisition of foreign intelligence collection under Section 702 be consistent with the Fourth Amendment.[262] Queries of Section 702 data must also comport with it.[263] Government certification must attest that the targeting and minimization procedures, and guidelines adopted by the Attorney General and the Director of National Intelligence to ensure compliance, are similarly consistent.[264] The court, in turn, must ascertain whether the targeting, minimization, and querying procedures are consistent with the Fourth Amendment.[265] The statute requires the court, in the event that the clause is not satisfied, to direct the government to correct any deficiency within 30 days and to "cease, or not begin, the implementation of the authorization for which such certification was submitted."[266]

Quite apart from the statutory requirements, surveillance must comport with the First and Fourth Amendments, as well as the other aspects of the Bill of Rights, such as Fifth Amendment due process rights. Reflecting their changing role from merely granting orders for narrowly-targeted ELSUR to handling complex surveillance programs impacting millions of people, the FISC and FISCR have increasingly been forced to address the relationship of foreign intelligence collection to individual rights.

A. *First Amendment Associational Rights*

Congress continues to express concern about how FISA impacts free speech and association and freedom of religion and the press. Senators Patrick Leahy (D-VT) and Mike Lee (R-UT), arguing for their amendment to the FISA bill (which easily passed the Senate in spring 2020), emphasized the importance of seeking greater input from *amici* in all sensitive cases, "such as those involving significant First Amendment issues—thereby adding a layer of protection for those who will likely never know they have been targeted for secret surveillance."[267]

---

[262] *Id.* § 1881a(b)(6).
[263] *Id.* § 1881a(f)(1).
[264] *Id.* § 1881a(h)(2)(A)(iv).
[265] *Id.* § 1881a(j)(3)(A).
[266] 50 U.S.C.A. § 1881a(j)(3)(B).
[267] Patrick J. Leahy & Mike Lee, *FISA Needs Reform. Our Amendment Would Do That—and Protect Constitutional Rights*, WASH. POST (May 10, 2020), https://www.washingtonpost.com/opinions/2020/05/10/fisa-needs-reform-our-amendment-would-do-that-protect-constitutional-rights/ [https://perma.cc/TT5Z-2WUD].

There is a disconnect, however, between Congress's emphasis and concerns, and the intelligence community guidelines and practices that govern foreign intelligence. To some extent this reflects the broader structure: open source intelligence collection is almost entirely premised on First Amendment-type activities.[268] Neither the Department of Defense manual governing similar collection nor the Attorney General Domestic Investigations Operations Guide provide a heightened predication standard for allegations potentially implicating the First Amendment.[269] Minimization procedures approved by the court, such as the FBI's Section 702 procedures, fail to contemplate the full range of First Amendment activity in their exposition of sensitive information—which, in any event, can still be retained, analyzed, and disseminated.[270]

As a judicial matter, the statute's emphasis on "solely" has come into play, rendering the requirement far less effective than it might otherwise be in protecting individual rights. In 2013, Judge Bates determined that the FISC could issue an order for business records even where "*[n]one* of the conduct or speech" attributed to the subject of the investigation fell "*outside* the ambit of the [F]irst [A]mendment."[271] He looked to "related conduct" by others which was not constitutionally protected.[272] The court considered a statement made by the target, noting that it "seems to fall well short of the sort of incitement to imminent violence or 'true threat' that would take it outside the protection of the [F]irst [A]mendment. The government's own assessment of [REDACTED] points to the conclusion that it is protected speech."[273] Judge Bates reflected, "Under the circumstances, the [c]ourt is doubtful that the facts regarding [REDACTED] own words and conduct alone establish reasonable grounds to believe that the investigation is not being conducted solely on the basis of the first amendment."[274]

---

[268] *See, e.g.*, CIA, CENTRAL INTELLIGENCE AGENCY ACTIVITIES: PROCEDURES APPROVED BY THE ATTORNEY GENERAL PURSUANT TO EXECUTIVE ORDER 12333, at 14 (Jan. 17, 2017) (basic collection includes publicly available information), https://repository.library.georgetown.edu/handle/10822/1053881 [https://perma.cc/9JKC-NN5Q].

[269] DEP'T OF DEF., DOD MANUAL 5240.01: PROCEDURES GOVERNING THE CONDUCT OF DOD INTELLIGENCE ACTIVITIES (Aug. 8, 2016), https://repository.library.georgetown.edu/handle/10822/1053876 [https://perma.cc/H5DF-CEUK]; FBI, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE (2016), https://repository.library.georgetown.edu/handle/10822/1053180 [https://perma.cc/K25P-VTYU]. Note, however, that the Domestic Investigations and Operations Guide makes a number of references to the First Amendment in Parts 1 and 2.

[270] § 702 Minimization Procedures (2019)—William P. Barr, Exhibit D: 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, *[REDACTED]*, No. [REDACTED] (FISA Ct. Sept. 17, 2019), https://repository.library.georgetown.edu/handle/10822/1060321.

[271] Opinion, *In re* Application of the FBI for an Ord. Requiring Prod. of Tangible Things from [REDACTED], No. BR 13-25, GID.C.00080, at 4 (FISA Ct. Feb. 19, 2013) (Bates, J.) (emphasis added).

[272] *Id.* at 5.

[273] *Id.*

[274] *Id.*

Nevertheless, the court read 50 U.S.C. § 1861 as permitting consideration of related conduct "in determining whether the [F]irst [A]mendment requirement is satisfied."[275] In other words, the court looked to the conduct of others, together with entirely protected First Amendment activity, to find that the proposed collection comported with the statutory requirements. Judge Bates explained:

> The text of Section 1861 does not restrict the Court to considering only the activities of the subject of the investigation in determining whether the investigation is "not conducted solely on the basis of activities protected by the first amendment." Rather, the pertinent statutory text focuses on the character (protected by the first amendment or not) of the "activities" that are the "basis" of the investigation.[276]

The activities of a non-U.S. person could be used in conjunction with protected First Amendment protected activities to target a U.S. person.

The court has also considered the First Amendment in the context of using PRTT to obtain Internet metadata.[277] The application included the requisite certification that the investigation of the target, a U.S. person, did not solely rely upon First Amendment-protected activities. The investigation had been conducted under Executive Order 12333.[278] Judge Colleen Kollar-Kotelly suggested that the "unusual breadth" of the proposed collection, "and its relation to the pertinent FBI investigations" called for further attention to the First Amendment concerns.[279]

Usually, PRTT collection would be directed at a particular facility being used by an individual of investigative interest. In the case before the court, though, the government was directing collection at metadata. It is not clear how such a shift fit the statutory language. Judge Kollar-Kotelly leapt to the legislative purpose, instead of the actual requirements, suggesting that it was "best effectuated at the querying stage, since it will be at a point that an analyst queries the archived data that information concerning particular individuals will first be compiled and reviewed."[280] It was a remarkable move, since the impact on the target's First Amendment activity occurs at the point of collection—not query.

Nevertheless, the Court ordered that the NSA modify its proposed criterion for querying the archived data to bring it into line with the First Amendment

---

[275] *Id.*
[276] *Id.* According to the application, the government was investigating the target not just based on "his own personal words and conduct (which, as noted, suggest sympathy toward, if not support of, international terrorism), but also on the basis of the admitted or suspected [REDACTED]." *Id.*
[277] Opinion and Order, [REDACTED], No. PR/TT [REDACTED], GID.C.00091 (FISA Ct. [REDACTED]) (Kollar-Kotelly, J.).
[278] *Id.* at 55.
[279] *Id.* at 56.
[280] *Id.* at 57.

requirement.[281] The court applied the standard articulated by the Supreme Court in *Brandenburg v. Ohio*, writing:

> [A]n e-mail account used by a U.S. person could not be a seed account if the *only* information thought to support the belief that the account is associated with [REDACTED] is that, in sermons or in postings on a web site, the U.S. person espoused jihadist rhetoric that fell short of "advocacy . . . directed to inciting or producing imminent lawless action and . . . likely to incite or produce such action."[282]

The court also directed the government to address "the general First Amendment implications of collecting and retaining this large volume of information that is derived, in part, from the communications of U.S. persons."[283] The government, in turn, acknowledged that surveillance acquiring "the contents of communications might in some cases implicate First Amendment interests, in particular the freedom of association," but then went on minimize any constitutional intrusion brought about by the collection of non-content addressing information.[284]

Bafflingly, the court looked to the Fourth Amendment to determine whether there were any First Amendment implications, concluding that because metadata did not implicate the former, the impact on the latter was only incidental.[285] What made this remarkable is that the entire point of collecting the metadata was to establish associational details—part of the core protections extended by the First Amendment. Nevertheless, the court determined that a good faith exception existed, particularly in light of the compelling national security interest at stake.[286]

The court remained uneasy, however, about the breadth of information being collected, noting that such collection carried "with it a heightened risk that collected information could be subject to various forms of misuse, potentially involving abridgement of First Amendment rights of innocent persons."[287] So the judge put into place special restrictions on the access, retention, and dissemination of such information.[288] She distinguished what the government was asking to do from a 1978 case from the District Court in New Jersey, which had held that a mail

---

[281] *Id*. at 57–58 ("[REDACTED] will qualify as a seed [REDACTED] only if NSA concludes, based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable articulable suspicion that a particular known [REDACTED] is associated with [REDACTED] *provided, however, that an* [REDACTED] *believed to be used by a U.S. person shall not be regarded as associated with* [REDACTED] *solely on the basis of activities that are protected by the First Amendment.*")
[282] *Id.* at 58 (quoting Brandenberg v. Ohio, 395 U.S. 444, 447 (1969) (per curiam)).
[283] *Id*. at 66.
[284] *Id.*
[285] *Id.* at 66–68.
[286] *Id*.
[287] *Id.* at 68.
[288] *Id.* at 68–69.

cover on a dissident political organization violated the First Amendment.[289] In contrast, in the case before the FISC, the PRTT did not specifically target a political group, and it had been authorized by statute on the grounds of being relevant to an investigation to protect against international terrorism.[290]

The court further pointed to *United States v. Falvey*, a 1982 case from the Eastern District of New York, which had upheld FISA provisions as constitutional on their face.[291] In that case, the court noted that Congress put restrictions on the government to prevent political abuse (e.g., the judge makes the probable cause finding in regard to whether the target is a foreign power or an agent of a foreign power). "Hence, to obtain a FISA surveillance order, the Government must provide the FISA judge with something more than the target's sympathy for the goals of a particular group, in this case, the IRA."[292]

To meet any remaining concerns, the court required that a "First Amendment proviso" be included as part of the "reasonable suspicion" standard querying archived meta data; adopted a date after which data could not be retained (four and a half years); and enhanced the role of the NSA Office of General Counsel.[293]

While only two opinions are available that address First Amendment associational rights, it appears that on at least one other occasion, the FISC wrestled with similar questions. A Justice Department Office of Inspector General (IG) report into the use of Section 215 orders for business records, issued in March 2008, took note.[294] When a Section 215 request was twice presented to the FISC, the IG notes, "[o]n both occasions, the FISA Court indicated it would not sign the order because of First Amendment concerns."[295] Later in the document, the IG explained,

---

[289] *Id.* at 69 n.49 (citing Paton v. La Prade, 469 F. Supp. 773, 780–82 (D.N.J. Nov. 29, 1978)).
[290] *Id*.
[291] *Id.* (citing United States v. Falvey, 540 F. Supp. 1306, 1314–15 (E.D.N.Y. Jun. 15, 1982)).
[292] *Falvey*, 540 F. Supp. at 1314.
[293] *[REDACTED]*, GID.C.00091, at 69 n.50; *see also* Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00004, at 23-24 (FISA Ct. [REDACTED]) (Baker, J.) ("Where a particular surveillance is especially likely to acquire communications that pertain to activities protected by the First Amendment, minimization procedures should be tailored to address the heightened concern that information could be used in a way that chills such activity"); *id.*, at 24 ("The committee is concerned that the surveillance authorized . . . not result in the retention or dissemination of information which would adversely affect the exercise of first amendment rights.") (quoting S. REP. NO. 95-701, at 42 (1978)); *id.* ("For a wiretap of 'a foreign spy acting as a newspaper reporter, . . . the committee expects that the minimization procedures . . . would be more strict to assure that information unrelated to his spy activities was not misused.'") (quoting H.R. REP. NO. 95-1283, pt. 1, at 61 (1978)); *id.* ("The technique in question results in an overbroad acquisition of communications that are [REDACTED], and therefore to the purpose of the particular surveillance, but that do relate to activities of non-target U.S. persons protected by the First Amendment.")
[294] OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., A REVIEW OF THE FBI'S USE OF SECTION 215 ORDERS FOR BUSINESS RECORDS IN 2006 (Mar. 2008, as released in redacted form in Feb. 2016), https://repository.library.georgetown.edu/handle/10822/1058990 [https://perma.cc/TF8Q-FZRR].
[295] *Id.* at 33–34; *See also id.* at 65 ("the FISA Court had twice declined to approve a Section 215 application based on First Amendment concerns.").

"The FISA Court declined to approve the first application. OIPR and NSLB e-mails state that the FISA Court decided that 'the facts were too "thin" and that this request implicated the target's First Amendment rights.'"[296] The problem was that when FISC refused the FBI permission to undertake the surveillance, the FBI had simply gone on to use National Security Letters to get the same information—despite the same First Amendment prohibitions in the parallel statutes.[297]

B. *First Amendment Right to Petition*

Despite the desuetude of the right to petition, the Framers considered it one of the most critical constitutional protections.[298] It surpassed the associative rights (speech, press, and assembly) in importance.[299] It allowed individuals to seek redress for wrongs and "could force the government's attention on the claims of the governed when no other mechanism could."[300] Subjects could go directly to the Crown to challenge lesser tribunals and authorities.[301]

The right to petition is distinct from the other expressive rights in that it protects (a) active political engagement; (b) directed at a particular body of persons; (c) demanding an action in response; and (d) not diluted through representation, giving citizens a better opportunity to be heard.[302] It ensures that changes in society are reflected in government.[303] It prevents the government from being the guardian of the collective public will.[304] It gives citizens the ability to act on their concerns.

The right of access to agencies and courts has long been recognized by the Supreme Court as "part of the right of petition protected by the First Amendment."[305] Citizens cannot petition and seek redress, if they cannot access the law. The case is even stronger in relation to government malfeasance, where remedies for unlawful

---

[296] *Id.* at 68.

[297] *See, e.g.*, 18 U.S.C. § 2709(b)(1) (requiring that the FBI certify that the investigation of a U.S. person "is not conducted solely upon the basis of activities protected by the first amendment to the Constitution of the United States.")

[298] 1 JOHN PHILLIP REID, CONSTITUTIONAL HISTORY OF THE AMERICAN REVOLUTION: THE AUTHORITY OF RIGHTS 4 (1986).

[299] *See* Julie M. Spanbauer, *The First Amendment Right to Petition Government for a Redress of Grievances: Cut from a Different Cloth*, 21 HASTINGS CONST. L.Q. 15, 17, 34–39 (1993); Norman B. Smith, *"Shall Make No Law Abridging . . .": An Analysis of the Neglected, But Nearly Absolute, Right of Petition*, 54 U. CIN. L. REV. 1153, 1165–67 (1986).

[300] Gregory A. Mark, *The Vestigial Constitution, The History and Significance of the Right to Petition*, 66 FORDHAM L. REV. 2153, 2157 (1998).

[301] *Id.* at 2163.

[302] *Id*. at 2157.

[303] *See* Thomas v. Collins, 323 U.S. 516, 545–46 (1945) (Jackson, J., concurring).

[304] *See id.* at 545.

[305] Cal. Motor Transp. Co. v. Trucking Unlimited, 404 U.S. 508, 513 (1972). *Accord* Chambers v. Balt. & Ohio R.R., 207 U.S. 142, 148 (1907); Bradley v. Pittsburgh Bd. of Educ., 913 F.2d 1064, 1076 (3d Cir. 1990); NAACP v. Button, 371 U.S. 415, 429–30 (1963); *see also* Carol Rice Andrews, *A Right of Access to Court Under the Petition Clause of the First Amendment: Defining the Right*, 60 OHIO ST. L.J. 557, 595–625 (1999) (finding historical, textual, and policy support for reading the First Amendment to include a right of access to the courts).

conduct create a "constitutional antidote" to sovereign immunity.[306] "These expressly guaranteed freedoms share a common core purpose of assuring freedom of communication on matters relating to the functioning of government."[307]

The First Amendment thus:

> embodies more than a commitment to free expression . . . ; it has a *structural* role to play in securing and fostering our republican system of self-government. . . . Implicit in this structural role is not only "the principle that debate on public issues should be uninhibited, robust, and wide-open," but also the antecedent assumption that valuable public debate—as well as other civic behavior—must be informed.[308]

It protects the "conditions of meaningful communication" by prohibiting the government "from limiting the stock of information from which members of the public may draw."[309] For court records, the test is "whether the place and process have historically been open to the press and general public," and "whether public access plays a significant positive role in the functioning of the particular process in question."[310] The courts include witness testimony, voir dire, preliminary hearings, bail pleas, sentencing hearings, and criminal and civil trials.[311]

In light of the history and scope of the right to petition, it is not surprising that following the release of the Snowden documents, numerous motions filed before the FISC demanded a First Amendment right of access to the court's opinions and, in some cases, orders. As a result, about half a dozen FISC/FISCR opinions in the public domain raise the issue. Just two cases reached the First Amendment question on the merits.

The first, from December 2007, related to an ACLU motion for the release of court orders and government pleadings that related to the Terrorist Surveillance Program.[312] The court determined that while it had jurisdiction over the motion, no

---

[306] James E. Pfander, *Sovereign Immunity and the Right to Petition: Toward a First Amendment Right to Pursue Judicial Claims Against the Government*, 91 NW. U. L. REV. 899, 899 (1997).
[307] Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 575 (1980); *accord* Globe Newspaper Co. v. Superior Ct., 457 U.S. 596, 604 (1982) (quoting *Richmond Newspapers*, 448 U.S. at 575); Mills v. Alabama, 384 U.S. 214, 218 (1966); Thornhill v. Alabama, 310 U.S. 88, 95–96 (1940).
[308] *Richmond Newspapers*, 448 U.S. at 587 (Brennan, J., concurring) (quoting N.Y. Times Co. v. Sullivan, 376 U.S. 254, 270 (1964)).
[309] *Id.* at 588; *id.* at 576 (majority); *see also* Kleindienst v. Mandel, 408 U.S. 753, 762–63 (1972).
[310] Press-Enter. Co. v. Superior Ct. (Press-Enterprise II), 478 U.S. 1, 8 (1986); *see also id.* at 8–10 (discussing the experience and logic test).
[311] *See, e.g.*, *id.* at 10–15; Press-Enter. Co. v. Superior Ct. (Press-Enterprise I), 464 U.S. 501, 505–510 (1984*); Globe Newspaper*, 457 U.S. at 603–06.
[312] Specifically, based on statements by government officials, the ACLU sought "the unsealing of (i) orders issued by this Court on January 10th, 2007 []; (ii) any subsequent orders that extended, modified, or vacated the January 10th orders; and (iii) any legal briefs submitted by the government in connection with the January 10th orders or in connection with subsequent orders that extended,

First Amendment right of access attached.[313] At that point, there was no tradition of openness or public access to government briefing materials. The "experience" test could not be satisfied.[314] Similarly, the "logic" test failed because, focusing on national security concerns, the "detrimental consequences of a broad public access to FISC proceedings or records would greatly outweigh any such benefits."[315] Even partial releases of declassified information with redactions "may confuse or obscure, rather than illuminate, the decisions in question."[316]

The second case, from February 2020, addressed the aforementioned ACLU/MFIAC motion, in regard to which the FISCR had previously determined that the movants had standing.[317] The court determined that it had subject matter jurisdiction over the motion, but, largely along the lines adopted by Judge Bates in the 2007 case, that the First Amendment did not confer a qualified right of public access to the material sought. Nor, Judge Collyer determined, was "there reason for the [c]ourt to exercise any discretion" or inherent authority "it may have to grant the relief requested."[318]

In applying the experience-and-logic test to the FISC opinions, the court found itself in a rather different position than it had been in 2007.[319] Hundreds of orders and nearly 80 FISC opinions were, at that point, in the public domain. Nevertheless, the court determined that it still did not have a history of openness to its opinions and that much of what was available was because of the executive branch, and not the court.[320]

Setting aside for the moment the fact that the executive branch *cannot* bind an Article III court in this manner, the court's assumption was not correct. Based on my own analysis, of the 88 FISC opinions currently in the public domain, at least 35% have been released by the FISC, while approximately 40% have been released in the course of FOIA suits in regular Article III courts. Only some 25% of the opinions in the public domain had been released in redacted form by the Office of the Director of National Intelligence, which, in some cases, has been the result of being ordered to do so by the FISC.

---

modified, or vacated the January 10th orders." *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 485 n.2, GID.C.00021, at 1 n.2 (FISA Ct. 2007) (Bates, J.).

[313] *Id.* at 486, GID.C.00021, at 2.

[314] *Id.* at 491–93, GID.C.00021, at 13–15.

[315] *Id.* at 494, GID.C.00021, at 17.

[316] *Id.* at 495, GID.C.00021, at 19.

[317] Opinion, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00267, at 2–4 (FISA Ct. Feb. 11, 2020) (Collyer, J.).

[318] *See id.* at 4.

[319] *Id.* at 19 (contrasting the quantity opinions and orders which have been made public since 2007 to those made public prior).

[320] *See id.* at 23.

In the 2020 decision, the court went on to find the logic test similarly unsatisfied.[321] It reasoned that release of the requested material could (a) create a chilling effect that could damage national security interests if the government failed to search or surveil legitimate targets in order to retain control over sensitive information; (b) create an incentive for the government to avoid judicial review, and (c) threaten the free flow of information to the FISC needed for an *ex parte* proceeding to result in sound decision making and effective oversight.[322]

The FISCR, on review, declined to consider the merits, dismissing the Petition for lack of jurisdiction over constitutional claims.[323] The court noted three limitations on it: first, that the issue constitute a case or controversy within the meaning of Article III (given effect by various judicial doctrines, such as standing, ripeness, mootness, and no advisory opinions); second, that the action arise under the Constitution, a law, or a treaty of the U.S. or fall within one of the other enumerated categories of Article III(2); and third, that the action is described by any jurisdictional statute as the kind of action that Congress intended to be subject to a court's adjudicatory authority.[324] For the court, the third category was problematic: movants had not brought a dispute within one of the statutorily enumerated areas over which the court had appellate jurisdiction.[325] The court explained, "If a dispute is not of the kind that Congress has determined should be adjudicated, we 'have no business deciding it, or expounding the law."[326] Further, for the court, the movants themselves were not authorized by Congress through statute to seek review.[327]

The FISCR has jurisdiction to review denials of applications, production or nondisclosure orders (Section 215), directives issued to electronic service providers (Section 702), and orders approving certifications and targeting, minimization, and querying procedures for Section 702 acquisition.[328] FISA also authorizes consideration of questions of law certified by the FISC.[329] But FISA is very specific about which parties can come before the court: the government may file a petition of review and any person receiving a production or nondisclosure order, or an electronic communication service providers receiving a directive, could come

---

[321] *Id.* at 26–27.
[322] *Id.* (quoting *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 496, GID.C.00021, at 20 (FISA Ct. 2007)).
[323] *In re* Ops. & Ords. by the FISC Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, 957 F.3d 1344, 1347, GID.CA.00013, at 3 (FISA Ct. Rev. 2020) (per curiam).
[324] *Id.* at 1349, GID.CA.00013, at 6–7.
[325] *Id.* at 1350-51, GID.CA.00013, at 9–12.
[326] *Id.* at 1350, GID.CA.00013, at 8 (quoting DaimlerChrysler Corp. v. Cuno, 547 U.S. 332, 341 (2006)).
[327] *Id.* at 1351, GID.CA.00013, at 11–12.
[328] *Id.* at 1350-51, GID.CA.00013, at 10–11.
[329] *Id.* at 1351, GID.CA.00013, at 11. FISC "shall certify for review . . . any question of law that may affect resolution of the matter in controversy that the court determines warrants such review because of a need for uniformity or because consideration . . . would serve the interests of justice. 50 U.S.C.A. § 1803(j) (West).

before it.[330] No provision had been statutorily made for parties such as the ACLU or MFIAC to come before the FISCR. Congress, moreover, had elsewhere given district courts the authority to raise Constitutional concerns.[331]

What is surprising about the FISCR's decision is the assumption that Congress could, by majority vote, either establish or override a *constitutional* right to petition. As Judge Bates and Judge Collyer had previously acknowledged, the movants were trying to exercise a constitutionally protected right to access judicial documents.[332] Congress does not have the right to take away such a claim.

Though Congress nowhere provided explicitly for the FISC or FISCR to consider Fourth Amendment rights in relation to Titles I, III, or IV, such constitutional questions nevertheless are well within the courts' domain. No one would object on the grounds that Congress had not specifically empowered the court to consider such claims, as the legislature lacks the power to divest courts of their ability to handle constitutional matters by mere majority vote. Specialization does not affect Article III courts' position as guardians of the Constitution. Should someone challenge a ruling in the bankruptcy court as a violation of due process, for instance, it matters naught whether Congress has provided in the statute establishing bankruptcy courts that they can hear Fifth Amendment arguments.

The FISCR decision also ignored the fact that under the doctrine of inherent powers, other courts *cannot* provide relief. Only the FISC and FISCR control their records. That is how the federal system works. It would be impossible, for instance, to go to Southern District of New York to petition for the judicial records of the Northern District of California. To obtain relief under either common law or the First Amendment right of access, you have to go to the court that had control over the original determination. The FISCR declined to rely on any ancillary authority that it had over the petition.[333] The decision also sidestepped the common law right of access claim, which the litigants had not raised, but which the amicus had addressed in detail.[334]

---

[330] *In re Ops. & Ords.*, 526 F. Supp. 2d at 1351, GID.CA.00013, at 11–12.

[331] *See* 28 U.S.C.A. § 1331 ("The district courts shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.")

[332] *See In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, GID.C.00021 (FISA Ct. 2007) (Bates, J.); Opinion, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00267 (FISA Ct. Feb. 11, 2020) (Collyer, J.).

[333] *In re Ops. & Ords.*, 957 F.3d 1344, 1356-57, GID.CA.00013, at 22–23.

[334] Brief of Amicus Curiae, *In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act*, No. Misc. 13-08 (FISA Ct. June 13, 2018), at 3, 8, 21, 22, 30, https://repository.library.georgetown.edu/bitstream/handle/10822/1056066/Misc%252013-08%2520Brief%2520of%2520Amicus%2520Curiae%2520180613.pdf?sequence=1&isAllowed=y ; Reply Brief of Amicus Curiae, *In re Opinions & Orders of this Court Addressing Bulk Collection of Data Under the Foreign Intelligence Surveillance Act*, No. Misc. 13-08 (FISA Ct. Aug. 1, 2018), at 11, 17, 34–45, https://repository.library.georgetown.edu/bitstream/handle/10822/1056071/Misc%252013-

Where the decision reflected stronger reasoning was in its observation that an "application made under this chapter" in 50 U.S.C. § 1803(b) generally refers to government applications for surveillance—not applications from individuals outside the FISA structure.[335] But if the court was right to suggest that FISCR lacked jurisdiction over this particular appeal, then it simply could not hear the case. This would leave the lower decision intact.

That is not what happened. Instead, the FISC followed the decision by dismissing three separate motions for access to judicial decisions for lack of jurisdiction.[336] The Court held that "the FISC is not empowered by Congress to consider constitutional claims generally, First Amendment claims specifically, or freestanding motions filed by persons who are not authorized by FISA to invoke this Court's jurisdiction."[337] The court continued that because the "reasons why the FISCR found it unwarranted to exercise ancillary jurisdiction over the ACLU motion apply to" the pending motion, "the FISC is foreclosed from doing so here."[338] But if the FISCR did not have jurisdiction over the motion in the first place based on the argument in regard to the appeal, it is not clear how their opinion could control the FISC in this regard.

C. *Common Law Right of Access*

At the founding of the United States, the First Amendment right to petition incorporated the common law right of access into its auspices. The Supreme Court applies a historical test to determine common law rights incorporated in the Constitution. It has consistently held, for instance, that the common law encapsulated in the Seventh Amendment refers to "the common law of England."[339] In similar fashion, the writ of habeas corpus "became an integral part of our common-law heritage by the time the Colonies achieved independence."[340] "[A]t the absolute minimum, the Suspension Clause protects the writ as it existed in 1789."[341] The Court looked to the writ's "historical core" to prevent the executive from wrenching habeas from the Court's jurisdiction.[342] Like habeas, the right of

---

08%2520Reply%2520Brief%2520of%2520Amicus%2520Curiae%2520180802.pdf?sequence=1&isAllowed=y. The amicus briefs share the same author (Professor Donahue) as this article.

[335] *In re Ops. & Ords.*, 957 F.3d at 1352.

[336] *See* Opinion and Order, *In re* Motion for Publ'n of Recs., No. Misc. 19-01, GID.C.00286 (FISA Ct. Sept. 15, 2020) (Boasberg, J.); Opinion and Order, *In re* Ops. & Ords. of this Ct. Containing Novel or Significant Interpretations of L., No. Misc. 16-01, GID.C.00285 (FISA Ct. Sept. 15, 2020) (Boasberg, J.); Opinion and Order, *In re* Motion of ProPublica, Inc. for the Release of Ct. Recs., No. Misc. 13-09, GID.C.00284 (FISA Ct. Sept. 15, 2020) (Boasberg, J.).

[337] *In re Motion of ProPublica*, GID.C.00284, at 3.

[338] *Id.*

[339] United States v. Wonson, 28 F. Cas. 745, 750 (C.C.D. Mass. 1812) (Story, J.); *see also* Balt. & Carolina Line, Inc. v. Redman, 295 U.S. 654, 657 (1935); Slocum v. N.Y. Life Ins. Co., 228 U.S. 364, 377 (1913).

[340] Rasul v. Bush, 542 U.S. 466, 473–74 (2004) (citation and quotation omitted).

[341] INS v. St. Cyr, 533 U.S. 289, 301 (2001) (quotation omitted).

[342] *Rasul*, 542 U.S. at 474.

access to judicial opinions arose centuries ago, becoming "an integral part of our common-law heritage."[343]

English common law recognizes and relies upon a public right of access to judicial opinions. Since the time of Edward II, who ruled England 1307–1327, English judicial records have been public.[344] In 1372, Parliament expanded the common law right of access to include court records and evidence, even where it might be used as evidence against the Crown.[345] Sir Edward Coke cited the right to the petition as undergirding the rule that records and reports be available to any English subject to uncover legal precedent:

> [W]hensoever a man is enforced to yield a reason of his opinion or judgment, that then he set down all authorities, precedents, reasons, arguments and inferences whatsoever that may be probably applied to the case in question.[] These records, for that they contain great and hidden treasure, are faithfully and safely kept (as they well deserve) in the King's Treasury. And yet not so kept but that any subject may for his necessary use and benefit have access thereunto, which was the ancient law of England, and so is declared by an act of Parliament in 46 Edw. 3.[346]

Even the deplorable Star Chamber "heard cases in public."[347] As a consequence, together with the presence of lawyers, the court's decisions and their reasoning would be known.[348]

Common law depended upon the promulgation of judicial decisions, initially for "common erudition" and thereafter for authoritative case law.[349] *Genera customes* "guided and directed" the "proceedings and determinations in the king's ordinary courts of justice."[350] They depended "upon immemorial usage . . . for their support."[351] Judges served as "the depositary of the laws," their decisions providing "the principal and most authoritative evidence" of the law.[352] Blackstone noted the importance of public access:

---

[343] *See* Preiser v. Rodriguez, 411 U.S. 475, 485 (1973).
[344] 1 WILLIAM BLACKSTONE, COMMENTARIES *71–72.
[345] *Compare* 46 Edw. 3 (1372) (Eng.), *reprinted in* 2 THE STATUTES AT LARGE 196–97 (Danby Pickering ed., 1762), *with* 14 Edw. 3, stat. 1, c. 14 (1340) (Eng.).
[346] 2 EDWARD COKE ET AL., THE REPORTS OF SIR EDWARD COKE IN THIRTEEN PARTS vi (London, Joseph Butterworth and Son new ed. 1826).
[347] 5 WILLIAM S. HOLDSWORTH, A HISTORY OF ENGLISH LAW 156 (3d ed. 1922–1938).
[348] *Id. See also* WILLIAM HUDSON, A TREATISE OF THE COURT OF THE STAR CHAMBER 48 (Francis Hargrave ed., 1986) (1792).
[349] *See* JOHN BAKER, OXFORD HISTORY OF THE LAWS OF ENGLAND: VOLUME VI: 1483–1558, at 488–89 (2003).
[350] 1 BLACKSTONE, *supra* note 344, at *68.
[351] *Id.*
[352] *Id.* at *69.

> The judgment itself, and all the proceedings previous thereto, are carefully registered and preserved, under the name of *records*, *in publick repositories set apart for that particular purpose; and to them frequent recourse is had*, when any critical question arises, in the determination of which former precedents may give light or assistance.[353]

Judicial decisions were "not only preserved as authentic records in the treasuries of the several courts," but they were "handed out to public view in the numerous volumes of *reports*."[354] According to Blackstone, the reports included "histories of the several cases, with a short summary of the proceedings, which are preserved at large in the record; the arguments on both sides; and the reasons the court gave for their judgment."[355] As Greenleaf later summarized, "[I]n regard to the inspection of public documents, it has been admitted, from a very early period, that the inspection and exemplification of the records of the king's courts is the common right of the subject."[356]

In recognition of this heritage, U.S. courts have long recognized a common law public right of access to judicial opinions. In 1834, the Supreme Court unanimously held that a court reporter could not hold a copyright to judicial records, as they were part of the public domain.[357] No more so could a bookseller hold an exclusive copyright to the written opinions of state judges: "The whole work done by the judges constitutes the authentic exposition and interpretation of the law, which, binding every citizen, is free for publication to all, whether it is a declaration of unwritten law, or an interpretation of a constitution or a statute."[358] As recognized by lower courts, "The right to examine certain records and papers . . . . exists as to the books containing the docket or minute entries of the judgments and decrees of the court."[359]

State courts followed suit. All persons, even if they were not citizens, had a right to inspect court records.[360] As early as 1894, the District of Columbia

---

[353] *Id.* (emphasis added)
[354] *Id.* at *71.
[355] *Id.* English law drew a line between formal matters of record and other judicial muniments. *See, e.g.*, Hewitt v. Pigott (1831) 131 Eng. Rep. 155, 155; Browne v. Cumming (1829) 109 Eng. Rep. 377, 377–78; Turner v. Eyles (1803) 127 Eng. Rep. 248, 248. The fact a document was not part of the formal record, though, still did not insulate it from public view. *See* Fox v. Jones (1828) 108 Eng. Rep. 897, 898; Taylor v. Sheppard (1835) 160 Eng. Rep. 110, 110–11.
[356] 1 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE § 471, at 623 (John Henry Wigmore ed., Boston, Little, Brown, & Co. 16th rev., enlarged, and annotated ed. 1899).
[357] Wheaton v. Peters, 33 U.S. (8 Pet.) 591, 668 (1834).
[358] Banks v. Manchester, 128 U.S. 244, 253 (1888). A recent Supreme Court case, Georgia v. Public.Resource.Org, Inc., 140 S. Ct. 1498 (2020), also held that annotations contained in Georgia's official annotated code fell within the government edicts doctrine and were ineligible for copyright protection.
[359] *In re* McLean, 16 F. Cas. 237, 239 (C.C.S.D. Ohio 1879) (No. 8877).
[360] *See, e.g.*, Nash v. Lathrop, 6 N.E. 559, 560-61, 563 (Mass. 1886); Nowack v. Fuller, 219 N.W. 749, 750, 752 (Mich. 1928).

recognized public access. The court denounced a motion for court records to be "preserved *in secrecy*," distinguishing between judicial records and "other mere official records."[361] "The rules of the Patent Office have no application to the proceedings of this court . . . . They may be very necessary and proper for conducting the affairs of that office . . . but it does not follow that similar rules should be adopted and enforced as applicable in an appellate court of record."[362]

Permeating these decisions was the understanding that the court's legitimacy depended upon open and public access both to its proceedings and to its decisions.[363] These principles have continued to be embraced from the mid-20th century, up through the present day.[364]

In the latter half of the 20th century, different methods of reproduction brought new questions to the fore. The courts reiterated the common law right to inspect judicial records. Third parties sought non-documentary evidence introduced at trial.[365] The courts doubled down, stating, "[t]he existence of the common law right to inspect and copy judicial records is beyond dispute."[366] Where denied, it tended to be in the service of competing rights, such as fair trial or freedom of the press.[367] Judges also looked to the role that the documents played in the adjudicative process and their relationship to substantive rights.[368] What was not questioned was whether the public had a right to actual decisions. To the contrary, since 1834, the courts have explicitly recognized that judicial opinions belong to the People.[369]

The First Amendment encapsulates and expands the common law right of access to judicial opinions; however, the common law right itself still exists. And FISC has had to confront it.

In 2007, Judge Bates responded with his take on the First Amendment right of access: it is inapplicable to documents traditionally cloaked from public view. "In

---

[361] *Ex parte* Drawbaugh, 2 App. D.C. 404, 404, 407 (D.C. Cir. 1894).
[362] *Id.* at 405.
[363] *See, e.g.*, *Ex parte* Gay, 20 La. Ann. 176, 177 (La. 1868) (requiring the trial of a case to be tried in open court); Scott v. Stutheit, 121 P. 151, 154 (Colo. App. 1912) ("The law is well settled . . . that . . . a judgment or decree, to be valid, must be rendered in open court during term time . . . .This is the general rule in this country, and has been adopted by the appellate courts in most, if not all, of the states of the Union.")
[364] *See* 45 AM. JUR. *Records and Recording Laws* § 16, Westlaw (database updated Feb. 2021); 53 C.J.S. *Records* § 74, Westlaw (database updated Feb. 2021); M.C. Dransfield, Annotation, *Restricting Access to Judicial Records*, 175 A.L.R. 1260, Westlaw (originally published in 1948, database updated weekly).
[365] *See, e.g.*, Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 591 (1978); United States v. Myers (*In re* Nat'l Broad. Co.), 635 F.2d 945, 947-49 (2d Cir. 1980); Belo Broad. Corp. v. Clark, 654 F.2d 423, 425 (5th Cir. 1981).
[366] *In re Nat'l Broad. Co.*, 635 F.2d at 949.
[367] *See, e.g.*, *Belo Broad. Corp.*, 654 F.2d at 431.
[368] *See, e.g.*, *In re* United States for an Ord. Pursuant to 18 U.S.C. Section 2703(D), 707 F.3d 283, 290–91 (4th Cir. 2013); *In re* Providence J. Co., 293 F.3d 1, 9 (1st Cir. 2002); United States v. El-Sayegh, 131 F.3d 158, 163 (D.C. Cir. 1997).
[369] *See* Wheaton v. Peters, 33 U.S. (8 Pet.) 591, 668 (1834).

the FISA context, there is an unquestioned tradition of secrecy, based on the vitally important need for national security."[370] FISC/FISCR records are kept under a statutory scheme intended to protect them from public disclosure. For Bates, there was "no role for this Court independently to review, and potentially override, Executive Branch classification decisions," and thus the controlling statute preempts any right of common law access that might otherwise exist.[371]

In the ACLU/MFIAC case decided by FISC and FISCR in 2020, the movants did not raise a common law claim and neither court addressed whether it might apply.[372] Nevertheless, Judge James E. Boasberg in dismissing a suit on the strength of the FISCR First Amendment ruling suggested that "FISA does not grant the FISC jurisdiction over claims asserting a common-law right of access either."[373] The common law right, though, does not require any statutory permission for its enactment. Indeed, it is a judicially-created right of access that dates back centuries.

D. *Fourth Amendment*

Numerous opinions issued by the foreign intelligence courts find applications or certifications consistent with the Fourth Amendment.[374] The key questions that the court has wrestled with in this area have been the significant purpose test, the warrant requirement, what constitutes a search, the reasonableness requirement, and the contours of probable cause. Underscoring the importance of FISC/FISCR opinions being made public is how the courts have approached the constitutional questions, in the process carving out an exception to the warrant requirement in the context of national security. These changes, and replacement of the primary purpose with the significant purpose test, have had a profound impact on U.S. persons' constitutional rights.

The key case on the shift from the primary purpose to the significant purpose test famously came with the FISCR decision *In re Sealed Case*, which dealt with a Title I order.[375] The FISC had determined that proposed standard minimization procedures (SMPs) were not reasonably designed because their purpose and technique were not "consistent with the need of the United States to

---

[370] *In re* Motion for Release of Ct. Recs., 526 F. Supp. 2d 484, 490–91, GID.C.00021, at 11 (FISA Ct. 2007) (Bates, J.).
[371] *Id.* at 491, GID.C.00021, at 11–12.
[372] Opinion, *In re* Ops. & Ords. of this Ct. Addressing Bulk Collection of Data Under the Foreign Intel. Surveillance Act, No. Misc. 13-08, GID.C.00267, at 11 n.8 (FISA Ct. Feb. 11, 2020) (Collyer, J.).
[373] Opinion and Order, *In re* Motion for Publ'n of Recs., No. Misc. 19-01, GID.C.00286, at 3 (FISA Ct. Sept. 15, 2020) (Boasberg, J.).
[374] *See, e.g.*, Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00031, at 6–7 (FISA Ct. 2008) (McLaughlin, J.); Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00079, at 20 (FISA Ct. 2012) (Bates, J.).
[375] *In re* Sealed Case, 310 F.3d 717, GID.CA.00001 (FISA Ct. Rev. 2002) (per curiam).

obtain, produce, or disseminate foreign intelligence information."[376] The court had blocked intelligence and sharing procedures which the government claimed could be used primarily for a law enforcement purpose.[377] It also had set extensive conditions for information sharing and coordination under the SMPs, for the first time setting down in a judicial opinion what the court believed the practice hitherto had been in regard to maintaining the wall between foreign intelligence and criminal investigations.[378]

In 2002, the FISCR overturned the lower court's decision, bringing down the wall that had previously existed within the Department of Justice and FBI between foreign intelligence collection and criminal investigations.[379] The court held that FISA did not require the government to demonstrate that its primary purpose in conducting electronic surveillance was foreign intelligence. The USA PATRIOT Act's addition of the word "significant" imposed a requirement that the government have a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes.[380] "So long as the government entertains a realistic option of dealing with the [foreign] agent other than through criminal prosecution, it satisfies" the statutory requirements for acquisition.[381]

According to the court, SMPs are designed to protect, as far as reasonable, against the acquisition, retention, and dissemination of nonpublic information that

---

[376] *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 625, GID.C.00002, at 625 (FISA Ct. 2002) (Lamberth, J.), *rev'd by In re Sealed Case*, 310 F.3d 717, GID.CA.00001.

[377] *Id.* at 623, GID.C.00002, at 623.

[378] The requirements included the following: "a. reasonable indications of significant federal crimes in FISA cases are to be reported to the Criminal Division of the Department of Justice; b. The Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, *but may not direct or control* the FISA investigation toward law enforcement objectives; c. the Criminal Division may consult further with the appropriate U.S. Attorney's Office about such FISA cases; d. on a monthly basis senior officials of the FBI provide briefings to senior officials of the Justice Department, including OIPR and the Criminal Division, about intelligence cases, including those in which FISA is or may be used; e. all FBI 90–day interim reports and annual reports of counterintelligence investigations, including FISA cases, are being provided to the Criminal Division, and must now contain a section explicitly identifying any possible federal criminal violations; f. all requests *for initiation or renewal of FISA authority* must now contain a section devoted explicitly to identifying any possible federal criminal *violations*; g. the FBI is to provide monthly briefings directly to the Criminal Division concerning all counterintelligence investigations in which there is a reasonable indication of a significant federal crime; h. prior to each briefing the Criminal Division is to identify (from FBI reports) those intelligence investigations about which it requires additional information and the FBI is to provide the information requested; and i. since September 11, 2001, the requirement that OIPR be present at all meetings and discussions between the FBI and Criminal Division involving certain FISA cases has been suspended; instead, OIPR reviews a daily briefing book to inform itself and this Court about those discussions." *Id.* at 619, GID.C.00002, at 619.

[379] *See In re Sealed Case*, 310 F.3d at 746, GID.CA.00001, at 746.

[380] *Id.* at 734–35, GID.CA..00001, at 734–35.

[381] *Id.* at 735, GID.CA.00001, at 735.

is not foreign intelligence information.[382] Evidence of criminal activity, however, can be retained and disseminated. SMPs do not limit prosecutorial advice to FBI intelligence officials regarding the initiation, operation, continuation, or expansion of FISA surveillance.[383]

Even as it adopted this broad view, the FISCR recognized some limitations: the FISA process could not be used to investigate ordinary crimes wholly unrelated to foreign intelligence.[384] Where "the FISC has reason to doubt that the government has any real non-prosecutorial purpose in seeking foreign intelligence information it can demand further inquiry into the certifying officer's purpose—or perhaps even the Attorney General's or Deputy Attorney General's reasons for approval."[385]

In 2008, a second major Fourth Amendment decision emerged as the FISC recognized a foreign intelligence exception to the warrant requirement.[386] The government had moved to compel Yahoo!, Inc. to comply with a directive issued pursuant to the Protect America Act of 2007 (PAA).[387] The company had refused to comply on the grounds that the directives violated the statutory language and the Fourth Amendment, as well as separation of powers.[388] It was a matter of first impression for the court. Although the PAA had sunset, the directives temporarily remained in effect.[389]

Ruling on the constitutional question, the court noted that for the exception to apply, it must be within the 2002 FISCR determination: i.e., a significant purpose must be the acquisition of foreign intelligence, and "a sufficiently authoritative official must find probable cause to believe that the target of the search or electronic surveillance is a foreign power or its agent."[390] In *United States v. Bin Laden*,[391] the reasonableness of surveillance targeted at a U.S. person abroad had taken into

---

[382] *Id.* at 740-41, GID.CA.00001, at 740–41.

[383] *Id.* at 731, GID.CA.00001, at 731. The court determined that the reasonableness of this approach depends on facts and circumstances of each case. Less minimization at the acquisition stage may be justified if the language is coded, there is a widespread conspiracy, or the intercepts are in a foreign language when no contemporaneous translator is available. *Id.* at 740-41, GID.CA.00001, at 740–41.

[384] *Id.* at 735–36, GID.CA.00001, at 735–36.

[385] *Id.* at 736, GID.CA.00001, at 736.

[386] Memorandum Opinion, *In re* Directives to Yahoo!, Inc. Pursuant to Section 105B of the Foreign Intel. Surveillance Act, No. 105B(g): 07-01, GID.C.00025, at 59 (FISA Ct. Apr. 25, 2008) (Walton, J.).

[387] *Id.* at 1 (citing Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552).

[388] *Id*. at 3.

[389] *See id.* at 2–4.

[390] *Id.* at 59. The court first observed that for U.S. persons inside the United States, surveillance under FISA is reasonable for Fourth Amendment purposes based the fact that there is some degree of prior judicial scrutiny, probable cause to believe that the target is an agent of a foreign power (or a foreign power itself) and likely to use the facility being targeted, at least some constitutionally-required determinations are made by the senior Executive Branch officials. In addition, the orders could extend to 90 days, particularly when there is Court oversight or minimization procedures, and such minimization procedures are in place and being applied. *Id.* at 77.

[391] United States v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

account the existence of minimization procedures, the duration of monitoring, the nature of the threat being investigated, and the extent to which the targeted facilities were used in support of the activity being investigated.[392] For the FISC, the factors going to the reasonableness determination for the targeting of U.S. persons overseas were slightly different. They included the minimization procedures, the duration of the surveillance, authorization by a senior government official, and identification of the facilities to be targeted.[393] As a threshold matter, such surveillance must also meet the criteria of the foreign intelligence exception to the Fourth Amendment's warrant requirement.

Upon review, in *In re Directives*, the FISCR determined that the exception was akin to a "special needs" exception for domestic foreign intelligence collection targeted at foreign powers or agents of foreign powers outside the U.S.[394] The warrant exception is undertaken for national security purposes (of which the government's interest is particularly intense) and involves acquisition from overseas foreign agents or regarding foreign intelligence.[395] To determine the reasonableness of a particular government action, a court must consider the totality of the circumstances: i.e., the nature of the intrusion and how it is implemented. The more important the government's interest, the greater the intrusion that may be constitutionally tolerated. In the case of national security, "the relevant governmental interest . . . is of the highest order of magnitude." [396] The court continued, "Collectively, these procedures require a showing of particularity, a meaningful probable cause determination, and a showing of necessity."[397] The duration (90 days) had already been found reasonable, and the risks of error and abuse are within "acceptable limits and effective minimization procedures are in place."[398]

The month after *In re Directives* issued, the FISC took a similar tack to find that Section 702 certification and targeting and minimization procedures also fell within the foreign intelligence exception to the Fourth Amendment warrant requirement.[399] The court looked to the pre-targeting determination, the post-targeting analysis, and documentation and oversight to determine that the procedures met the demands of reasonableness in light of the significance of the national security interest and the mitigation of unintentional incidental collection by the retention procedures in place.[400]

---

[392] *In re Directives*, GID.C.00025, at 80.
[393] *Id.* at 86.
[394] *In re* Directives to Yahoo! Inc. Pursuant to Section 105B of Foreign Intel. Surveillance Act, 551 F.3d 1004, 1011, GID.CA.00002, at 14–15 (FISA Ct. Rev. 2008) (Selya, J.).
[395] *Id.*, GID.CA.00002, at 15. The Court also reiterates that "a significant purpose" standard is the correct standard to apply. *See id.*, GID.CA.00002, at 15–16.
[396] *Id.* at 1012, GID.CA.00002, at 19.
[397] *Id.* at 1016, GID.CA.00002, at 27–28.
[398] *Id.*, GID.CA.00002, at 28.
[399] *See* Memorandum Opinion, *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01, GID.C.00030, at 35 (FISA Ct. Sept. 4, 2008) (McLaughlin, J.).
[400] *See id.* at 37–41.

The FISC has also confronted reasonableness in the context of PRTT and search of the captured data. In the 2016 case *In re Certified Question of Law*, the FISC had issued an order approving a PRTT application, including the proviso that the government "not make any affirmative investigative use of post-cut-through digits acquired through pen register authorization that do not constitute call dialing, routing, addressing or signaling information, unless separately authorized by this Court."[401] The order served on the provider required that it furnish "all information, facilities, or technical assistance necessary to accomplish the installation and operation of the . . . device(s)."[402] That authorization was consistent with prior practice of the court: as noted by the FISCR, since at least 2006, PRTT orders had authorized the acquisition of PCTDDs, "while generally prohibiting the use of those digits that do not constitute dialing information."[403] Throughout that time period, the government had argued that despite a statutory prohibition that contents not be obtained through PRTT devices, as a statutory matter, the government was only required to "use technology reasonably available to it . . . so as not to include the contents of any wire or electronic communications."[404] In light of the difference in practice between the FISC and ordinary Article III courts, the FISC judge considered it appropriate to certify the question to the FISCR.

The FISCR determined that the search of PCTDDs is reasonable even without a warrant.[405] A key consideration for the court was that technology that would enable the government to distinguish between content/non-content DRAS was not available. To distinguish the matter before the FISC from the ordinary criminal law context, the court looked to:

> (1) the paramount interest in investigating possible threats to national security;
> (2) the investigative importance of having access to the dialing information provided by the post-cut-through digits,
> (3) the incidental nature of the collection of content information from post-cut-through digits,
> (4) the relatively slight intrusion on privacy entailed by the acquisition of post-cut-through digits,
> (5) the prohibition against the use of any content information obtained from the pen register or trap-and-trace device,
> (6) the steps taken by the government to minimize the dissemination of post-cut-through digits; and

---

[401] *In re* Certified Question of L., 858 F.3d 591, 593, GID.CA.00003, at 4 (FISA Ct. Rev. 2016) (per curiam).
[402] *Id.*, GID.CA.00003, at 4.
[403] *Id.* at 594, GID.CA.00003, at 5.
[404] *Id.* at 595, GID.CA.00003, at 6 (quoting 18 U.S.C.A. § 3121(c) (West)).
[405] *Id.* at 605, 610, GID.CA.00003, at 26, 37.

> (7) the fact that FISA pen register interceptions are conducted only with the approval and under the supervision of a neutral magistrate, in this case a FISC judge.[406]

In 2018, the FISC turned to the scope of the search of communications collected under Section 702 and held, contrary to the *amici* who had been appointed in the case, that the query of the communications did not constitute a separate Fourth Amendment search event subject to its own reasonableness analysis.[407] Nevertheless, under a totality of the circumstances test, the court arrived at the same conclusion as the amici, which was that the FBI query procedures being proposed were unreasonable under the Fourth Amendment.[408] For the court, the privacy interests were substantial, as "the FBI has conducted tens of thousands of unjustified queries of Section 702 data."[409] Judge Boasberg noted that "the reported querying practices present a serious risk of unwarranted intrusion into the private communications of a large number of U.S. persons."[410] The court explained:

> The goal of the Fourth Amendment is to protect individuals from arbitrary governmental intrusions on their privacy. . . . The FBI's use of unjustified queries squarely implicates that purpose: the FBI searched for, and presumably examined when found, private communications of particular U.S. persons on arbitrary grounds . . . . The government is not at liberty to do whatever it wishes with those U.S.-person communications, notwithstanding that they are "incidental collections occurring as a result of" authorized acquisitions.[411]

---

[406] *Id.* at 607-08, GID.CA.00003, at 31–32.

[407] [REDACTED], 402 F. Supp. 3d 45, 86, GID.C.00258, at 86–87 (FISA Ct. 2018) (Boasberg, J.). The FISA Amendments Reauthorization Act of 2017, had required that the querying procedures comport with the Fourth Amendment. Pub. L. No. 115-118, sec. 101(a), § 702(f)(1), 132 Stat. 3, 4 (2018) (codified at 50 U.S.C.A. § 1881a(f)(1) (West)). Section 702(f)(2), moreover, requires the FBI to obtain a FISC order in certain circumstances prior to examining any content obtained by query of the data. Sec. 101(a), § 702(f)(2), 132 Stat. at 4–5. Amici pointed to these alterations as requiring the court to re-visit its early approach, suggesting that "Congress has acknowledged the reality that FBI agents querying databases containing raw 702 information for a variety of purposes are, in effect, undertaking new 'searches,' some of which now require a court order." *[REDACTED]*, 402 F. Supp. 3d at 85, GID.C.00258, at 85 (quoting Brief of Amici Curiae at 56–57, *[REDACTED]*, 402 F. Supp. 3d 45 (No. [REDACTED]) (brief not publicly available)). Amici had further noted that evolution of caselaw: in 2014, the Supreme Court in *Riley v. California* required law enforcement to obtain a warrant to search mobile phones obtained incident to arrest. *Id.*, GID.C00258, at 86 (citing *Riley v. California*, 573 U.S. 373, 401 (2014)). Various lower court cases affirmed that even where objects might come into the possession of law enforcement, subsequent inspection constitutes a separate event for Fourth Amendment purposes. *Id.* at 85, GID.C.00258, at 85. The court rejected these arguments, noting that the statutory changes instituted by Congress were just that: statutory (not expansions of constitutional rights) and that in a number of the cases presented, the objects in question had been provided to the law enforcement by third parties—whereas the government already held the content of communications under § 702. *Id.* at 86, GID.C.00258, at 86-88.

[408] *Id.* at 86, GID.C.00258, at 88.

[409] *Id.* at 87, GID.C.00258, at 88.

[410] *Id.*, GID.C.00258, at 89.

[411] *Id.*, GID.C.00258, at 89 (citations and quotations omitted).

In re Directives had relied on the assurance that the government does not maintain a database of incidentally-collected information. Here, however, not only was there a database, but the FBI was regularly querying it.

In 2011, the FISC similarly determined that intrusion caused by the NSA's targeting and minimization procedures, as related to its acquisition of Internet multi-communication transactions (MCTs) authorized by Section 702, was not reasonable under Fourth Amendment.[412] The NSA was acquiring a large number (i.e., tens of thousands) of Fourth Amendment-protected MCTs that had no direct connection to any targeted facility, and thus did not serve national security needs underlying FISA. The government's proposed handling of MCTs tended to maximize retention of such information and hence to enhance risk that it would be used and disseminated.[413]

The NSA amended its procedures, which the court subsequently approved as consistent with the Fourth Amendment.[414] The new version addressed different types of MCTs, based on whether the active user was the target, and, if not, the nationality and location (to the extent known) of the active user. It provided for the more problematic categories of MCTs to be sequestered and instituted a shorter retention period put into place, whereby an MCT of any type could not be retained more than 2 years after expiration of certification under which it was acquired, unless applicable retention criteria met.[415] The provisions categorically prohibited NSA analysis from using known U.S. person identifiers to query the results of upstream Internet collection.[416] The protections, such as they were, proved short-lived.[417]

---

[412] [REDACTED], No. [REDACTED], GID.C.00073, at 78–79, 80, 2011 WL 10945618, at *28 (FISA Ct. Oct. 3, 2011) (Bates, J.).

[413] [Judge] Bates explained, "Both in terms of its size and its nature, the intrusion resulting from NSA's acquisition of MCTs is substantial. The Court now understands that each year, NSA's upstream collection likely results in the acquisition of roughly two to ten thousand discrete wholly domestic communications that are neither to, from, nor about a targeted selector, as well as tens of thousands of other communications that are to or from a United States person or a person in the United States but that are neither to, from, nor about a targeted selector." *Id.* at 72, 2011 WL 10945618, at *26. By using to/from/about upstream (*see infra* discussion Part V), the NSA could collect an entire MCT for which active user was a non-target and that mostly pertained to non-targets, merely because a single, discrete communication within the MCT was to, from, or contained a reference to a tasked selector—even if non-target active user was United States person in the United States and MCT contained a large number of domestic communications that did not pertain to a foreign intelligence target. The Court concluded, "NSA could do substantially more to minimize the retention of information concerning United States persons that is unrelated to the foreign intelligence purpose of its upstream collection." *Id.* at 61. 2011 WL 10945618, at *22.

[414] [REDACTED], No. [REDACTED], GID.C.00076, at 1, 22, 2011 WL 10947772, at *1, *7 (FISA Ct. Nov. 30, 2011) (Bates, J.).

[415] *Id.* at 7–11, 2011 WL 10947772, at *3–*5.

[416] *Id.* at 9, 2011 WL 10947772, at *4.

[417] *See*, Part V(C), *infra*.

E. *Fifth Amendment (Due Process)*

The final area of constitutional adjudication has to do with Fifth Amendment due process. Only one case, from 2014, appears to address it. There, the court denied a motion for disclosure of prior FISC decisions on the grounds that "neither FISA nor the . . . [FISC] Rules of Procedure . . . require, or provide for discretionary, disclosure of the Requested Opinions in the circumstances of this case," and determined that the due process clause "does not compel the requested disclosure."[418] Instead, it requires the court to review an application, order, and other materials relating to ELSUR *in camera* or *ex parte* if the Attorney General's affidavit indicates that disclosure would harm national security. Disclosure may only occur where it is necessary to make an accurate determination of the legality of the surveillance.[419]

V. Cluster 4: Process and Compliance

The fourth and final cluster of FISC/FISCR opinions centers on the tension between public and private accountability. They reveal that the government continually pushes the boundaries set by the court and Congress, at times crossing them entirely. The courts, caught in the middle, have to work to ensure compliance, further underscoring how much their roles have altered since 1978. While some of the transgressions have been minor, others have had a tremendous impact on citizens' rights, making it even more important that the courts' determinations be made public. In a democratic state, it is critical that the people know how the government is using powers it has been afforded. It is all the more important when the government inadvertently, or at times deliberately, flouts judicial orders—and then (as discussed in Part IV, *supra*) attempts to prevent findings revealing malfeasance from reaching light of day.

As a practical matter, the FISC has had to account for irregularities in regard to special minimization procedures, as well as SMPs and targeting and querying procedures. It has confronted inaccurate, materially omitted, erroneous, and false statements by the government. And it has found itself in a data dilemma: what to do with information (which the government asks to retain and continue to use) obtained outside statutory authority or requirements put into place by the courts. Efforts by the government to request that the court approve such behavior borders on pushing the FISC to issue an Advisory Opinion – well outside the bounds of Article III.

While earlier in its history, the FISC appears to have been more deferential to the government, it has become less patient in light of the government's repeated failure to comply with judicial direction and submission of inaccurate and false statements to the court.

---

[418] Opinion on Motion for Disclosure of Prior Decisions, *[REDACTED]*, No. [REDACTED], GID.C.00112, at 3 (FISA Ct. 2014) (Collyer, J.).
[419] *Id.* at 8–9.

A. *SMPs/Minimization*

FISA requires that the court ensures that the intrusiveness of electronic intercepts and physical search is consistent with the need to collect foreign intelligence information from foreign powers and their agents.[420] The first time judicial concerns appears to have arisen in regard to SMPs appears to have been in *In re All Matters*.[421] The court rejected the government's proposed 2002 minimization procedures because it would have empowered criminal prosecutors to "advise FBI intelligence officials concerning the initiation, operation, continuation, or expansion of FISA searches or surveillance," allowing the government to use FISA primarily for a law enforcement purpose.[422] In *In re Sealed Case,* as the prior section noted, the FISCR overturned the lower court.

Similar process questions arose in 2004, when the FISC determined that the government could not mark the identities of non-target U.S. persons during the retention process for the purpose of facilitating subsequent retrieval of those persons' communications.[423] The SMPs did not allow for using alternative or additional means of recording identities of those not party to a communications. The government practice therefore violated the procedures.[424]

Again in 2007, the government tried to convince the FISC that alternative, extra-statutory minimization procedures met the requirements. In this case, the NSA was unilaterally initiating surveillance of foreign telephone numbers or e-mail addresses without express judicial approval—even after the fact.[425] The court rejected the practice. According to Judge Roger Vinson, it failed to follow either the letter or the spirit of the statute.[426]

Perhaps nowhere has the pressure on the court from the government to expand what is allowed under the minimization procedures been more evident than in the Section 702 context, which ten opinions address. A clear tension between the statutory prohibition on intentionally targeting and incidental collection of U.S. persons' communications exists. The matter appears to have first come to the fore in a 2008 opinion authored by Judge McLaughlin. At that point, the court went with

---

[420] *In re* All Matters Submitted to the Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 616, GID.C.00002, at 616 (FISA Ct. [REDACTED] 2002) (Lamberth, J.), *rev'd by In re* Sealed Case, 310 F.3d 717, GID.CA.00001 (FISA Ct. Rev. [REDACTED] 2002) (per curiam).
[421] *In re All Matters*, 218 F. Supp. 2d 611, GID.C.00002, at 611.
[422] *Id.* at 623, GID.C.00002, at 623 (quotations omitted).
[423] Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00004, at 20 (FISA Ct. [REDACTED] 2004) (Baker, J.).
[424] *Id.*
[425] Order and Memorandum Opinion, *In re* [REDACTED], No. [REDACTED], GID.C.00012, at 17–20 (FISA Ct. Apr. 3, 2007) (Vinson, J.).
[426] *See id.* at 17–20.

the government representation, finding the minimization procedures sufficient.[427] The statute's prohibition on intentionally targeting a U.S. person or someone within the U.S. still permitted the retention of mistaken, but reasonable beliefs that the target was a non-U.S. person outside the U.S. [428]

In 2010, Judge Bates again confronted a similar question.[429] But his most consequential decision came in October 2011, when he ruled that the NSA's minimization procedures, in relation to its upstream collection of internet MCTs, were not reasonably designed to minimize retention of non-publicly-available information concerning nonconsenting U.S. persons, given that the NSA did not limit access to specially-trained analysts or require those analysts to mark relevant portions of MCTs.[430] In that opinion, as discussed in Part IV, *supra*, Judge Bates ruled that the intrusion caused by NSA's targeting and minimization procedures, as related to its acquisition of Internet MCTs authorized by Section 702, was not reasonable under the Fourth Amendment.

The reason the practice failed constitutional muster was because the NSA had been acquiring a large number—tens of thousans—of Fourth Amendment-protected MCTs that had no direct connection to any targeted facility and thus did not serve national security purpose. Its proposed handling of MCTs, moreover, tended "to maximize the retention of such information and hence to enhance risk that it would be used and disseminated."[431]

In the following month, November 2011, the court approved amended minimization procedures and Section 702 collection resumed.[432] The additional measures related to:

> (1) the post-acquisition segregation of those types of transactions that are most likely to contain non-target information concerning United States persons or persons in the United States; (2) special handling and marking requirements for transactions that have been removed from or that are not subject to segregation; and (3) a two-year default retention period for all upstream acquisitions.[433]

---

[427] Memorandum Opinion, *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01, GID.C.00030, at 24–25 (FISA Ct. Sept. 4, 2008) (McLaughlin, J.).
[428] *Id.* at 25–27 (FISA Ct. Sept. 4, 2008) (McLaughlin, J.).
[429] *See* Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00060 (FISA Ct. [REDACTED] 2010) (Bates, J.). Note that Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00061 (FISA Ct. [REDACTD] 2010) (Bates, J.), contains similar language and analysis as *[REDACTED]*, GID.C.00060.
[430] [REDACTED], No. [REDACTED], GID.C.00073, at 59–63, 2011 WL 10945618, *20–22 (FISA Ct. Oct. 3, 2011) (Bates, J.).
[431] *Id.* at 78–79, 2011 WL 10945618, at *28.
[432] *See* [REDACTED], No. [REDACTED], GID.C.00076, at 21–22, 2011 WL 10947772, at *7 (FISA Ct. Nov. 30, 2011) (Bates, J.).
[433] *Id.* at 7, 2011 WL 10947772, at *3.

Numerous opinions approve ELSUR/Physical surveillance SMPs as well as those adopted in the Section 702 context.[434] These, and other rulings, demonstrate a steady pattern of special amendments and exceptions that expand access to information obtained via FISA. In 2012, for example, the government obtained permission for the FBI to provide the National Counterterrorism Center (NCTC) with raw data relating to international terrorism (as opposed to derivative information) and to permit NCTC to review, retain, and disseminate such information.[435] The same year, the NSA amended their minimization procedures to allow for the sharing of unminimized communications obtained from Internet Service Providers.[436] The following year, the FISC accepted further amendments to the § 702 procedures.[437] The court approved new FBI SMPs to allow for the storage of unminimized FISA-acquired information in "ad hoc" FBI databases that do not comply with Section III of the minimization procedures.[438] The purpose was to enable FBI personnel to review and analyze the information, which apparently could not be completed within the compliant systems.[439]

The steady expansion continued. In 2014, the government amended SMPs for ELSUR and physical search to allow for the dissemination to the National Center for Missing and Exploited Children (NCMEC) for law enforcement purposes, and to exempt information from removal that might be required for litigation-related reasons.[440] The FISC also approved amendments to allow the FBI to retain information longer than the normal retention period if considered necessary for administrative, civil, or criminal litigation, as long as the Bureau informed the court.[441] And in 2017, the court approved extending the retention periods for upstream collection from two years to five years.[442] Part of the rationale

---

[434] *See, e.g.*, Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00039 (FISA Ct. Apr. 7, 2009) (McLaughlin, J.); Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00256 (FISA Ct. Sept. 20, 2012) (Bates, J.); Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00089 (FISA Ct. Dec. 13, 2013) (Walton, J.); Memorandum Opinion and Order Compelling Compliance with Directives, [REDACTED], No. [REDACTED], GID.C.00111 (FISA Ct. [REDACTED] 2014) (Collyer, J.).

[435] Memorandum Opinion and Order, *In re* Elec. Surveillance, Physical Search, & Other Acquisitions Targeting Int'l Terrorist Grps., Their Agents, & Related Targets, No. [REDACTED], GID.C.00077 (FISA Ct. May 18, 2012) (McLaughlin, J.).

[436] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00079, at 1, 5–6, 20 (FISA Ct. 2012) (Bates, J.) (holding the amendments consistent with the Fourth Amendment).

[437] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00089, at 27–28 (FISA Ct. Dec. 13, 2013) (Walton, J.) (holding that that the Nov. 15, 2013 amended minimization procedures are consistent with the requirements of 50 U.S.C. § 1881a(e) and the Fourth Amendment).

[438] *See id.* at 22–27.

[439] *Id.* at 25.

[440] Opinion and Order, *In re* Standard Minimization Procs. for FBI Elec. Surveillance & Physical Search Conducted Under the Foreign Intel. Surveillance Act, Nos. Multiple including [REDACTED], GID.C.00105, at 1 (FISA Ct. Aug. 11, 2014) (Collyer, J.).

[441] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00106, at 21–26, 41–42 (FISA Ct. Aug. 26, 2014) (Hogan, J.).

[442] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00282, at 46, 49 (FISA Ct. Dec. 6, 2019) (Boasberg, J.)

at the time was that the scope of upstream acquisition had narrowed from TFA to only communications to or from a selector associated with the target; however, this condition is subject to change at the discretion of the Executive with just thirty days' notice to Congress (and no notice in exigent circumstances).

The pattern that emerges is one familiar to scholars who focus on the history of surveillance: the steady expansion of the type of information obtained, the purposes to which it is put, and the government agencies with whom it is shared.

B. *Targeting*[443]

While numerous FISC opinions have found Section 702 targeting procedures consistent with the statutory and constitutional requirements, there has been a significant amount of concern generated by the government's effort to expand targeting to communications not just to or from a target, but also *about* a target or a selector associated with a target.[444]

The first engagement with to/from/about (TFA) collection in the Section 702 context appears in a 2008 opinion, in which Judge McLaughlin determined that the procedures were reasonably designed to ensure that the users of tasked selectors are reasonably believed to be abroad, and to prevent the intentional acquisition of about communications to which the sender and all intended recipients were known to be inside the U.S.[445] The agencies could reach out to foreign governments for technical and linguistic assistance.[446]

In 2009, the court had to address an overcollection issue in which the government argued that the procedures, not implementation, mattered. The Section 702 submissions indicated that the government would be collecting telephone and internet communications. For the former, the targeting would only be to/from; for the latter, it would be TFA, to ensure the collection of communications that would contain a reference to the name of the tasked account.[447] While substantial

---

[443] For one of the better publicly-available summaries of targeting procedures, see Memorandum Opinion and Order Compelling Compliance with Directives, [REDACTED], No. [REDACTED], GID.C.00111, at 6–10 (FISA Ct. 2014) (Collyer, J.).

[444] *See, e.g.*, Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00060 (FISA Ct. 2010) (Bates, J.); Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00062 (FISA Ct. 2010) (McLaughlin, J.); [REDACTED], 402 F. Supp. 3d 45, 55–64, GID.C.00258, at 10–45 (FISA Ct. 2018) (Boasberg, J.).

[445] Memorandum Opinion, *In re* DNI/AG Certification [REDACTED], No. 702(i)-08-01, GID.C.00030, at 19 (FISA Ct. Sept. 4, 2008) (McLaughlin, J.). In 2007 Judge Vinson considered a similar question in regard to Title I ELSURV. Order, *In re* [REDACTED], No. [REDACTED], GID.C.00016, at 12-13 (FISA Ct. May 31, 2007) (Vinson, J.) (approving collection not just to or from but also about a selector).

[446] *Id.* at 28–29.

[447] The court determined that the CIA and NSA minimization procedures comported with FISA and the Fourth Amendment. Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00039 (FISA Ct. Apr. 7, 2009) (McLaughlin, J.). Those procedures permit U.S. person queries and require a written explanation of the basis for their assessment (at the time of targeting)

implementation problems could speak to whether targeting procedures were reasonably designed, statutory compliance was merely a matter of procedure.[448] Judge McLaughlin rejected the government's approach and took the actual instance of overcollection on board.[449]

The following year, Judge Bates held that the enhanced and remedial measures for NSA's failure to effectively purge databases of Section 1881a information required under minimization procedures, and NSA's backlog in conducting post-targeting review of selectors for which NSA had indications such selectors might have been used within the U.S., were adequate to address concerns.[450] The court determined that the relatively few post-tasking review problems compared to the total number of tasking decisions, coupled with the limited duration of any improper taskings in those cases, and the assurance that the process has been improved, did not undermine basis for approval of targeting and minimization procedures.[451]

Although the court in April 2011 approved the Section 702 submissions, the following month, on May 2, the government filed a supplemental letter disclosing that NSA's upstream collection included the acquisition of entire transactions, which "may contain data that is wholly unrelated to the tasked selector, including the full content of discrete communications that are not to, from, or about the facility tasked for collection."[452] The NSA had significantly exceeded approved scope of collection.

In October 2011, Judge Bates wrote, "the Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions

---

"that the target possesses, is expected to receive, and/or is likely to communicate foreign intelligence information concerning [the] foreign power or foreign territory" about which foreign intelligence information is being sought. *Id.*

[448] *See* Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00039, at 23 (FISA Ct. Apr. 7, 2009) (McLaughlin, J.) ("The Court is unpersuaded by the government's contention that compliance with Section 1881a(d)(l) is purely a matter of intent. Substantial implementation problems can, notwithstanding the government's intent, speak to whether the applicable targeting procedures are 'reasonably designed' to acquire only the communications of non-U.S. persons outside the United States.")

[449] *Id.* at 23–24. The court found that the "enhanced measures recently implemented by NSA to detect and filter out such non-targeted communications [REDACTED] *before* such communications enter repositories that are accessible to analysts . . . provide a basis for finding, despite overcollections, that the NSA Targeting Procedures are reasonably designed." *Id.* The government indicated that it identified [REDACTED] overcollection incidents (regarding Internet communications), and the NSA was able to identify the causes for [REDACTED] incidents. *Id.* at 18. Further, the NSA purges all files erroneously acquired. *Id.* at 19. The government claims that it adopted substantial remedial and preventing measures to alleviate overcollection (such measures are redacted). *Id.* at 21.

[450] *See* Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00060, at 9–10 (FISA Ct. 2010) (Bates, J.).

[451] *Id.* at 10–11.

[452] [REDACTED], No. [REDACTED], GID.C.00073, at 5; 2011 WL 10945618, at *2 (FISA Ct. Oct. 3, 2011) (Bates, J.).

mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[453] It turned out that the NSA had been acquiring Internet transactions *since before the Court approved the first Section 702 certification in 2008*.[454] This information spurred Judge Bates to observe that FISA makes it a crime "(1) to 'engage[] in electronic surveillance under color of law except as authorized' by statute or (2) to 'disclose[] or use[] information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized' by statute.[455]

Although the Court had authorized acquisition of certain categories of "about" communications, moreover, dating from Judge McLaughlin's 2009 opinion, *the NSA had been collecting all of them*: "The Court now understands that all 'about' communications are acquired by means of NSA's acquisition of Internet transactions through its upstream collection.[456]

In addition, as aforementioned in the Fourth Amendment analysis, the NSA was not just collecting discreet communications, but also "internet transactions"—including some that include a single, discrete communication (single communication transaction or SCT) as well as MCTs. Judge Bates wrote, "[F]or the first time, the government has now advised the Court that the volume and nature of the information it has been collecting is fundamentally different from what the Court has been led to believe."[457] As a result, the NSA was knowingly collecting tens of thousands of entirely domestic communications—precisely the types of communications prohibited by statute.

The government reached for a familiar trope, arguing that the technology was insufficient to know at moment of collection whether the transaction is a SCT or MCT, or to identify parties to any particular communication within the transaction.[458] The court had previously understood—from the government—that it *could* use technical measures to prevent acquisition of entirely domestic communications. The expansion basically meant that the NSA had, "as a practical matter, circumvented the spirit" of the law.[459]

The issues did not end in 2011. Five years later, the government again informed the court of significant noncompliance with NSA and FBI querying

---

[453] [REDACTED], GID.C.00073 at 16 n.14; 2011 WL 10945618, at *5 n.14. The other misrepresentations marked the Section 215 program as well as PRTT, discussed *infra*.
[454] [REDACTED], GID.C.00073 at 17; 2011 WL 10945618, at *6.
[455] [REDACTED], GID.C.00073 at 17 n.15; 2011 WL 10945618, at *6 n.15 (quoting 50 U.S.C.A. § 1809(a) (West)).
[456] [REDACTED], GID.C.00073 at 17 n.16; 2011 WL 10945618, at *6 n.16. See also Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00039 (FISA Ct. Apr. 7, 2009) (McLaughlin, J.).
[457] [REDACTED], GID.C.00073 at 28; 2011 WL 10945618, at *9.
[458] [REDACTED], GID.C.00073 at 43; 2011 WL 10945618, at *14.
[459] [REDACTED], GID.C.00073 at 48; 2011 WL 10945618, at *16.

procedures.[460] A subsequent hearing proved insufficient to address the court's concerns and to assess the procedures submitted with the certifications.[461] Although the executive branch made further submissions in January 2017, discussing what it was doing to try to even understand the scope and the causes of the compliance issues, and to propose potential solutions, the court still did not find that the government had adequately ascertained the scope of the issues.[462]

Unable to address the problem with TFA and under pressure from the court, the government agreed to sequester and then to destroy raw upstream Internet data previously collected and to substantially narrow to breadth of information collected upstream. "Most significantly," the court explained, "the government will eliminate 'abouts' collection altogether, which will have the effect of eliminating acquisition of the more problematic types of MCTs."[463] The government would make quarterly report s to the court over the next year as it undertook the process. Under the amended procedures, the NSA could still acquire MCTs, but only when it could ensure that the target was an active user (i.e., a party to the entire MCT).[464]

The opinion was issued April 26, 2017, and released the same day. Two days later, the NSA announced that it was choosing to eliminate the upstream data—*without* explaining that the NSA had been collecting information outside of either statutory or constitutional constraints for seven years.[465]

The public about-face and release of the court opinion underscored the already heightened public concern about TFA. Accordingly, the FISA Amendments Reauthorization Act of 2017 limited the acquisition of "communications that contain a reference to, but are not to or from, a target of an acquisition authorized" under Section 702.[466] The statute provided for the government to resume abouts collection with 30 days' notice to Congress, with an exception for exigent circumstances.[467] In the interim, the government must "fully and currently inform" the Judiciary and Intelligence Committees of the House and Senate of "significant noncompliance . . . concerning any acquisition of abouts communications."[468] In light of the narrowing of abouts collection, the querying provisions broadened.

---

[460] See further discussion, Part IV(D), *infra*.
[461] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00130, at 4 (FISA Ct. Apr. 26, 2017) (Collyer, J.).
[462] *Id.* at 5. The government requested an extension until May 26, 2017, which the court approved only through April 28, 2017. *Id.*
[463] *Id.* at 23.
[464] *Id.* at 24–26.
[465] *See* Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. TIMES (Apr. 28, 2017), https://www.nytimes.com/2017/04/28/us/politics/nsa-surveillance-terrorism-privacy.html [https://perma.cc/U6MQ-KK9V].
[466] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115–118, §§ 103(a)(3)(5), 702(b)(5), 132 Stat. 3, 10 (2018) (codified at 50 U.S.C.A. § 1881a(b)(5) (West)).
[467] *Id.* § 103(b)(2)-(4).
[468] *Id.* §§ 103(b)(5)(B), § 702(m)(4), 132 Stat. at 12–13.

C. *Querying*

Both the § 215 bulk collection program and § 702 upstream collection have been beset by concerns about the querying procedures and the government's violation of judicial orders.

According to the FISC, in March 2009, the NSA telephony bulk collection under § 215 was "premised on a flawed depiction of how the NSA uses [the acquired] metadata."[469] The misperception by FISC started from day one, in May 2006, "buttressed by repeated inaccurate statements made in the government's submissions, and despite a government-devised and Court-mandated oversight regime."[470] Contrary to the government's repeated assurances, the NSA had been routinely running queries of the metadata using terms that did not meet the required standard of reasonable, articulable, suspicion (RAS). The Court concluded that requirement had been "so frequently and systemically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."[471]

In regard to § 702, as aforementioned, in October 2016, the government informed the court that it had been violating the restrictions established by Bates in 2011 that forbade using U.S. person identifiers to query upstream data. As the court explained in 2017: "The October 26, 2016 Notice informed the Court that NSA analysts had been conducting such queries in violation of that prohibition, with much greater frequency than had previously been disclosed to the Court."[472] Preliminary reports by the NSA inspector general suggested that the problem was widespread.[473] The government had not been forthright: as Judge Collyer explained, "The full scope of non-compliant querying practices had not been

---

[469] *In re* Prod. of Tangible Things from [REDACTED], GID.C.00036, at 10–11, 2009 WL 9150913, at *5 (FISA Ct. Mar. 2, 2009) (Walton, J.).
[470] *Id.* at 11; 2009 WL 9150913, at *5.
[471] Prod. of Tangible Things from [REDACTED], GID.C.00036 at 11; 2009 WL 9150913, at *5.
[472] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00130, at 19 (FISA Ct. Apr. 26, 2017) (Collyer, J.).
[473] *Id.*; *see also* Exhibit A: 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 at 2, [REDACTED] (FISA Ct. Mar. 30, 2017) (No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1053027 [https://perma.cc/P7G9-28S2]; Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(b)(4)b, at 4, [REDACTED] (FISA Ct. Mar 30, 2017) (No. No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1053259 [https://perma.cc/D5LM-G5U7] (amended minimization procedures to state that Internet transactions acquired after Mar. 17, 2017 that were not to/from target "are unauthorized acquisitions and therefore will be destroyed upon recognition.")

previously disclosed to the Court."[474] The court considered it an institutional "lack of candor," and noted it was "a very serious Fourth Amendment issue."[475]

Even as the government was forced to jettison TFA collection, it pressed the court to allow it to begin querying upstream data using known U.S. person identifiers, subject to a requirement that the facts establishing the use of any such identifier as a selection term was reasonably likely to return foreign intelligence information.[476] The court agreed with the amended procedures, stating that it was satisfied that the same restrictions applied as existed in regard querying other forms of 702-acquired data (which Bates had said was acceptable in his October. 3, 2011 memorandum opinion).[477]

The 2017 FISA Amendments Reauthorization Act, in addition to limiting TFA, also provided new measures to address querying procedures, requiring that they be "consistent with the requirements of the fourth amendment . . . for information collected."[478] Under the statute, a "query" means "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized" under § 702 certification.[479]

In prior years, minimization procedures for § 702 included rules for querying raw data.[480] But following introduction of the new statute, the AG and DNI adopted separate querying procedures for each agency.[481] Under all of them, a U.S. person (USP) query term is defined as "a term that is reasonably likely to identify one or more specific" USPs which "may be either a single item of information or information that, when combined with other information, is reasonably likely to identify one or more specific" USPs.[482] Depending on context,

---

[474] *[REDACTED]*, GID.C.00130, at 4.
[475] *Id.* at 19 (quotations omitted).
[476] *See id.* at 28–29.
[477] *Id.*.
[478] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, §§ 101(a)(1), 702(f)(1)(A), 132 Stat. 3, 4 (2018) (codified at 50 U.S.C.A. § 1881a(f)(1)(A) (West)).
[479] 50 U.S.C.A. § 1881a(f)(3)(B).
[480] *See, e.g.*, Exhibit D, Minimization Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § III.D., at 11-12, [REDACTED] (FISA Ct. Sept. 26, 2016) (No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1056245 [https://perma.cc/6PCK-43SL].
[481] For reference, see the separate querying procedures starting in 2018 for the FBI, NSA, CIA, and NCTC. *See Statutory and Regulatory Authorities*, DIGITAL GEO., https://repository.library.georgetown.edu/handle/10822/1052817 [https://perma.cc/95F7-L3XM] (last visited Apr. 3, 2021).
[482] *See* Exhibit I: Querying Procedures Used by the Federal Bureau of Investigation in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § III.A., at 1, [REDACTED] (FISA Ct. Sept. 18, 2018) (No. [REDACTED]), *available at*

names or unique titles, government-associated personal or corporate identification numbers, street addresses, or telephone numbers, could all constitute USP query terms.[483] The FISC determines whether such procedures satisfy the statutory requirements.[484]

Under certain circumstances, the government must obtain a FISC order prior to accessing § 702-acquired information.[485] This applies only to the FBI (and not to the CIA, NSA, or NCTC) for queries made using a USP query term that was not designed to find or to extract foreign intelligence information.[486] The court order to access contents is further limited to queries made "in connection with a predicated criminal investigation opened by the [FBI] that does not relate to the national security of the United States."[487] Thus, the FBI cannot query § 702 data for domestic law enforcement purposes, and review the metadata of any returns, but it cannot examine the substance without FISC approval. The FBI does not have to go to the court if it determines there is a reasonable belief that the contents could help to mitigate/eliminate a threat to life or serious bodily harm.[488]

The 2017 Reauthorization Act also introduced a new requirement that the querying procedures "include a technical procedure whereby a record is kept of each [USP] query term used for a query."[489] Despite the plain language of the statute, in 2018 and 2019, the FISC was *again* forced to address the government's effort to resist restrictions on querying the data.

In the first review of the new procedures, the court found that the FBI's proposed measures did not comply with record-retention provisions.[490] The FBI argued that because it kept *all* the terms used to query the database, it did not need to specify which ones were USP-specific.[491] Judge Boasberg made it clear that to meet the statutory requirement, a log must be kept. The FBI querying and minimization procedures were further inconsistent with both the statutory minimization requirements and Fourth Amendment in that they failed to "require

---

https://repository.library.georgetown.edu/handle/10822/1058714 [https://perma.cc/G3EM-B6L2]. All four agencies' querying procedures have the same language.

[483] "Query" is defined as "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through acquisitions authorized under Section 702. 50 U.S.C.A. § 1881a(f)(3) (West).

[484] *See id.* § 1881a(f)(1)(C), (j)(3)(A)-(B).

[485] *See id.* § 1881a(f)(2).

[486] *See id.* § 1881a(f)(2)(A), (f)(2)(F).

[487] *Id.* § 1881a(f)(2)(A).

[488] *Id.* § 1881a(f)(2)(E).

[489] FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, §§. 101(a)(1)(B), 702(f)(1)(B), 132 Stat. 3, 4 (2018) (codified at 50 U.S.C.A. § 1881a(f)(1)(B)).

[490] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00258, at 62 (FISA Ct. Oct. 18, 2018) (Boasberg, J.).

[491] *Id.* at 49–52.

adequate documentation of the justifications for queries that use United States-person query information."[492]

The FBI had had several non-compliance issues since April 2017 in which FBI queries were not reasonably likely to return foreign intelligence information or evidence of a crime.[493] The court also noted some new non-compliance issues.[494]

Dissatisfied with the FISC's ruling, the government appealed to the FISCR, which agreed with FISC's determination. The proposed query procedures failed to comply with the plain statutory language.[495] Because the result required amendment of the procedures, the court did not reach whether the proposed query and minimization procedures complied with FISA and the Fourth Amendment.[496]

The case therefore came back to the FISC with amended procedures that acknowledged the FBI's statutory responsibility to keep a record of all U.S. person query terms.[497] Further amendments required that "[p]rior to reviewing the unminimized contents of section 702-acquired information retrieved using a United States person query term," FBI personnel must "provide a written statement of facts showing that the query was reasonably likely to retrieve foreign intelligence information or evidence of a crime."[498] The court held that this met statutory and 4th Amendment requirements and agreed to an implementation strategy, requiring a written report by September 26, 2019 and every 45 days thereafter until the FBI fully complied.[499]

As a result of the legislation and the court's opinions, each agency's querying procedures now require the agency to "generate and maintain an electronic record of each United States person query term used for a query of unminimized information acquired pursuant to section 702."[500] The records are retained for at least five years. The CIA, NCTC, and FBI require that users record the query term(s) used, the date of the query, and who ran the inquiry.[501] The NSA

---

[492] *Id.* at 133–34.
[493] *Id.* at 68–72.
[494] *Id.* at 127–32 (including NSA's backlog in processing purge orders and insider threat monitoring).
[495] *In Re* DNI/AG 702(h) Certifications 2018 [REDACTED], GID.CA.00008, 941 F.3d 547, 549–50, 555, (FISA Ct. Rev. 2019) (per curiam).
[496] *Id.* at 549–50, 555–56, GID.CA.00008, at 3–4, 42–43.
[497] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00259, at 7–8 (FISA Ct. Sept. 4, 2019) (Boasberg, J.) ("The FBI must generate and maintain an electronic record of each United States person query term used for a query of unminimized content or noncontent information acquired pursuant to section 702.") The court held that this provision did meet the requirements of Section 702(f)(1)(B). *Id.*
[498] *Id.* at 9 (quotations omitted).
[499] *Id.* at 16–18.
[500] *See id.* at 7. The procedures also indicate that if an electronic record cannot be generated, the FBI must generate and keep a written record. *Id.*
[501] *See, e.g.*, Exhibit J: Querying 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, § IV.B., at 3–4, [REDACTED] (FISA Ct. Sept.

retains the query term(s) used or approved; date of query/approval of query terms; identity of the user who conducted query or sought approval; and, for content queries, the approving official in NSA OGC office, as well as the duration of the approval.[502]

D. *Erroneous Statements and Material Omissions*

About a dozen opinions in the public domain raise concern about inaccurate, materially omitted, erroneous, or false statements to the court. Although the Russia investigation attracted a significant amount of attention in recent years, the problem did not begin there. Indeed, it started before the September 11 attacks.

In March 2000, the government informed the FISC that it had been disseminating FISA information to criminal squads in the FBI and U.S. Attorney's Office without the required authorizations of the Court in four or five separate cases.[503] This was followed in September 2000, with the government confessing to errors in 75 separate FISA applications related to major terrorist attacks, including:

> a) an erroneous statement in the FBI Director's FISA certification that the target of the FISA was not under criminal investigation; b) erroneous statements in the FISA affidavits of FBI agents concerning the separation of the overlapping intelligence and criminal investigations, and the unauthorized sharing of FISA information with FBI criminal investigators and assistant U.S. attorneys; and, c) omissions of material facts from FBI FISA affidavits relating to a prior relationship between the FBI and a FISA target, and the interview of a FISA target by an assistant U.S. attorney.[504]

The government reported similar misstatements in another series of applications, transgressing the wall between intelligence collection and criminal investigations: all of the agents involved participated in the same squad, with screening done not by the Office of Intelligence Policy Review, but by a supervisor

---

17, 2019) (No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1060328 [https://perma.cc/X4YN-7PUH].

[502] Exhibit H: Querying Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § IV.B., at 4, [REDACTED] (FISA Ct. Sept. 17, 2019) (No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1060326 [https://perma.cc/TUE8-4T7B].

[503] *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 620, GID.C.00002, at 620 (FISA Ct. 2002) (Lamberth, J.), *rev'd by In re* Sealed Case, 310 F.3d 717, GID.CA.00001 (FISA Ct. Rev. 2002) (per curiam).

[504] *Id.* at 620.

simultaneously overseeing both investigations.[505] The court, however, did not take a strong stance on these violations.[506]

The modern era has fared little better in terms of government submissions. Even the practice of reporting noncompliance has failed to comport with the requirements. In 2009, for example, the court noted that the government had been picking and choosing what it decided to reveal to the court, omitting, for instance, failures to de-task accounts even after the NSA discovered that the targets had entered the United States.[507] The court had to order the government to report *every* compliance incident that relates to the operation of the targeting or minimization procedures.[508]

In another case, the government misdescribed the actual scope of what it was collecting under Title I.[509] It was far from the first time. The court wryly noted:

> The government has exhibited a chronic tendency to mis-describe the actual scope of NSA acquisitions in its submissions to this Court. These inaccuracies have previously contributed to unauthorized electronic surveillance and other forms of statutory and constitutional deficiency. It is evident that the government needs every incentive to provide accurate and complete information to the Court about NSA operations, whenever such information is material to the case.[510]

Once again, the court ordered the government to submit a report of its effort in identifying and purging information obtained from the acquisition.[511]

The executive branch has made inaccurate representations to the court about the post-tasking review process.[512] There are numerous other examples.[513] These are in addition to the queries of § 215 metadata being run absent RAS, the bulk collection of Internet metadata outside the scope of the FISC's orders, and Judge

---

[505] *Id.* at 621.
[506] *Id.* at 620.
[507] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00050, at 12–14 (FISA Ct. 2009) (Hogan, J.). Note that is opinion is very similar to Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00051 (FISA Ct. 2009) (Hogan, J.), but with slightly different language and redactions.
[508] *[REDACTED]*, GID.C.00050, at 14.
[509] *See* Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00254, at 9–11 (FISA Ct. [REDACTED]) (Hogan, J.) (NSA's acquisition of [REDACTED] constituted unauthorized electronic surveillance because it failed to comply with 50 U.S.C.A. § 1804(a)(2), (a)(3)(B) (West)).
[510] *Id.* at 13–14 (citations have been redacted).
[511] *Id.* at 14.
[512] *See* Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00062, at 20–21 (FISA Ct. 2010) (McLaughlin, J.).
[513] *See, e.g.*, Memorandum Opinion, [REDACTED], No. PR/TT [REDACTED], GID.C.00092, at 2–3 (FISA Ct.) (Bates, J.).

Bates's now famous October 2011 opinion noting that the government had made substantial misrepresentations regarding the scope of § 702.[514]

Getting caught does not necessarily alleviate the problem. In 2012, for instance, the court reiterated its concern about NSA misrepresentations regarding upstream collection.[515] The issue did not abate: the court was surprised to learn by notice in July 2015 that the NSA had not been deleting overcollected Section 702 records placed on the Master Purge List in accordance with a May 2011 Opinion and Order.[516] The court was also dismayed that it took the government four years of continued retention before proposing a resolution to the court.[517] The government further informed the court about two NSA databases that were not compliant with minimization procedures.[518] This was all prior to the October 26, 2016 hearing in which Collyer lamented the NSA's query of § 702 data using USP identifiers despite the prohibition in the minimization procedures, noting the government's "lack of candor" and the serious constitutional questions thereby raised.[519]

The most prominent example of government malfeasance arises in the context of the Russian investigations. The FBI opened Crossfire Hurricane on July 31, 2016 to determine whether individuals associated with the Trump campaign were either wittingly or unwittingly coordinating with the Russian government's efforts to interfere in the 2016 presidential election.[520] The investigation came on the heels of a foreign government informing the administration that George Papadopoulos (a campaign adviser) had indicated that Russia had reached out to the Trump team to offer to release information that would be damaging to the democratic candidate.[521]

On December 9, 2019, Justice Department Inspector General Michael Horowitz completed a twenty-month inquiry into Crossfire Hurricane and the investigation of four members of the presidential campaign: Papadopoulos, Carter

---

[514] [REDACTED], No. [REDACTED], GID.C.00073, at 15–18, 2011 WL 10945618, at *5–6 (FISA Ct. Oct. 3, 2011) (Bates, J.).

[515] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00256, at 26–33 (FISA Ct. Sept. 20, 2012) (Bates, J.). Note that this is a more complete version of [REDACTED], No. [REDACTED], GID.C.00078, 2012 WL 9189263 (FISA Ct. Sept. 25, 2012) (Bates, J.). The reported version only included the discussion of the scope of the NSA upstream collection.

[516] Memorandum Opinion and Order, [Redacted], No. [Redacted], GID.C.00121, at 57–58 (FISA Ct. Nov. 6, 2015) (Hogan, J.).

[517] *Id.* at 58.

[518] *Id.* at 65–68.

[519] Memorandum Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00130, at 19 (FISA Ct. Apr. 26, 2017) (Collyer, J.).

[520] OFF. OF THE INSPECTOR GEN., DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION i (revised Dec. 20, 2019) [hereinafter CROSSFIRE HURRICANE REPORT], https://repository.library.georgetown.edu/handle/10822/1058716.

[521] *Id.* at ii.

Page, Paul Manafort, and Michael Flynn.[522] Having poured over more than one million documents held by the DOJ and FBI and undertaken more than 170 interviews with more than 100 witnesses, Horowitz found significant discrepancies between law, policy, and practice.[523]

In regard to the FISC applications for Title I surveillance of Carter Page, the IG found that the first application in October 2016, and the three renewal orders thereafter, which resulted in about eleven months of surveillance, was premised in part on a dossier provided by Christopher Steele.[524] Steele, a former intelligence officer, had formed a consulting firm that specialized in corporate intelligence and investigative services. In 2016, Steele was hired by a Washington, D.C. investigative firm to do political opposition research into the Russian role in the election. The reports that he produced for them became known as the Steele dossier. From July through October 2016, Steele passed several of these reports on to the FBI, which failed to press him on either his funding source, or his role in a Yahoo! News article focused on ties between Trump advisor and Kremlin.[525]

In his report, Horowitz launched a scathing critique of the investigation. The applications to the FISC for surveillance of Page left out information that cut against FBI or was inconsistent with what they were telling the court that went directly to probable cause. The FISC Rules of Procedure required that the Page applications contain all material facts. [526] Although they did not define "material," FBI policy considered that a fact was "material" where it was *relevant* to the court's probable cause determination.[527] The Woods procedures also required that all factual statements in FISA application be "scrupulously accurate."[528] It turned out that the application relied on four assertions from the Steele dossier, none of which was corroborated by other information—and none of which was made clear to the FISC.[529] In addition, the application contained seven further inaccuracies and

---

[522] *See id.* at i, 8.
[523] *See id.* at i, ii–xviii.
[524] *Id.* at vi. The first application was filed Oct. 21, 2016, while three renewal applications were filed on Jan. 12, Apr. 7, and June 29, 2017. A different FISC judge approved the requested orders, and all four orders issued resulted in about eleven months of FISA coverage targeting Carter Page, from October 21, 2016 to September 22, 2017. *Id.*
[525] *Id.* at v–vi.
[526] *Id.* at vi. FISC R. PROC. 13(a) (Correction of Misstatement or Omission; Disclosure of Non-Compliance. (a) Correction of Material Facts. If the government discovers that a submission to the Court contained a misstatement or omission of material fact, the government, in writing, must immediately inform the Judge to whom the submission was made of: (1) the misstatement or omission; (2) any necessary correction; (3) the facts and circumstances relevant to the misstatement or omission; (4) any modifications the government has made or proposes to make in how it will implement any authority or approval granted by the Court; and (5) how the government proposes to dispose of or treat any information obtained as a result of the misstatement or omission.)
[527] CROSSFIRE HURRICANE REPORT, *supra* note 520, at vi–vii.
[528] *Id.* at vii.
[529] *Id.* vii–viii. The four assertions included: "Compromising information regarding Hillary Clinton had been compiled for many years, was controlled by the Kremlin, and had been fed by the Kremlin to the Trump campaign for an extended period of time; During a July 2016 trip to Moscow, Page met secretly with Igor Sechin, Chairman of Russian energy conglomerate Rosneft and close

omissions, none of which were brought up at any of the renewals, at which point ten addition omissions of fact, misstatements, and significant errors occurred.[530]

Horowitz expressed concern, "That so many basic and fundamental errors were made by three separate, hand-picked teams on one of the most sensitive FBI investigations that was briefed to the highest levels within the FBI, and that FBI officials expected would eventually be subjected to close scrutiny, raised significant questions regarding the FBI chain of command's management and supervision of the FISA process."[531]

As if those discoveries were not enough, Horowitz found that an FBI lawyer, Kevin Clinesmith, had falsified an email from the CIA to state that Page was not a source for the agency, resulting in assuaging concerns that the declarant had about whether there was such a source relationship. As a result, nothing in the application indicated that there might be a relationship between Page and the CIA—information that went directly to the probable cause determination of whether Page was an agent of a foreign power.[532] Horowitz went on to report that the agents had not shared pertinent information with key DOJ and FBI officials, with the result that DOJ leadership "did not have accurate and complete information at the time they approved the applications."[533] Horowitz was so concerned about the findings that he initiated a second audit focused on FBI compliance with the Woods procedures in FISA applications targeting USPs in counterintelligence and counterterrorism investigations.[534]

The report shook congressional confidence in FISA, with the failure to include exculpatory evidence hearkened as a Fifth Amendment due process concern. Political leaders took aim at the court. Sen. Lindsey Graham announced,

---

associate of Putin, to discuss future cooperation and the lifting of Ukraine-related sanctions against Russia; and with Igor Divyekin, a highly-placed Russian official, to discuss sharing with the Trump campaign derogatory information about Clinton; Page was an intermediary between Russia and the Trump campaign's then manager (Manafort) in a 'well-developed conspiracy' of cooperation, which led to Russia's disclosure of hacked DNC emails to WikiLeaks in exchange for the Trump campaign's agreement to sideline Russian intervention in Ukraine as a campaign issue; and, Russia released the DNC emails to WikiLeaks in an attempt to swing voters to Trump, an objective conceived and promoted by Page and others." *Id.* (citations omitted).

[530] *Id.* at viii–ix, xi–xii.

[531] *Id.* at xiv.

[532] *Id.* at ix. ("Omitted Page's prior relationship with another U.S. government agency, despite being reminded by the other agency in June 2017, prior to the filing of the final renewal application, about Page's past status with that other agency; instead of including this information in the final renewal application, the OGC Attorney altered an email from the other agency so that the email stated that Page was "not a source" for the other agency, which the FBI affiant relied upon in signing the final renewal application"); *see also* Matt Zapotosky, *Ex-FBI Lawyer Avoids Prison After Admitting He Doctored Email in Investigation of Trump's 2016 Campaign*, WASH. POST (Jan. 21, 2021), https://www.washingtonpost.com/national-security/kevin-clinesmith-fbi-john-durham/2021/01/28/b06e061c-618e-11eb-afbe-9a11a127d146_story.html [https://perma.cc/GFS2-XLNC].

[533] CROSSFIRE HURRICANE REPORT, *supra* note 520, at 367–68.

[534] *Id.* at xiv.

"I'm a pretty hawkish guy, but if the court doesn't take corrective action and do something about being manipulated and lied to, you will lose my support. . . . I would hate to lose the ability of [FISC] to operate at a time, probably when we need it the most. But after your report, I have serious concerns about whether the FISA court can continue unless there is fundamental reform."[535]

The FISC took the offensive: on December 5, 2019, Collyer issued a classified order directing the government to identify all matters before the FISC on which Clinesmith had worked.[536] Less than a fortnight later, the court issued an unclassified order rebuking the FBI over their actions and noting that the agency had failed to fulfill the "heightened duty of candor" that accompanies *in camera, ex parte* applications.[537] Collyer wrote, "The frequency with which representations made by FBI personnel turned out to be unsupported or contradicted by information in their possession, and with which they withheld information detrimental to their case, calls into question whether information contained in other FBI applications is reliable."[538] She ordered the government to inform the court what it had done to address the errors and to ensure that similar inaccuracy and omissions did not happen again.[539] She also previously raised the question about any other matters involving Clinesmith and whether any bar association or disciplinary referrals had been made.[540]

The FBI responded with an unclassified submission to the court laying out its approach going forward.[541] Judge Boasberg, who had become Presiding Judge of the FISC at the turn of the new year, appointed former DOJ National Security Division Assistant Attorney General David Kris as *amicus curiae* to assist court in evaluating government's response.[542] Kris found the proposed measures insufficient and recommended several ways to expand and mprove assurances.[543] Soon after, the FISC declassified the order about the DOJ's handling of the Page application.[544]

---

[535] S. Comm. on the Judiciary, *Inspector General Report on Origins of FBI's Russia* Inquiry, C-SPAN, at 47:04 (Dec. 11, 2019), *available at* https://www.c-span.org/video/?466593-1/justice-department-ig-horowitz-defends-report-highlights-fisa-problems [https://perma.cc/BC3Q-JMCG].
[536] Order, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00261, at 2 (FISA Ct. Dec. 5, 2019) (Collyer, J.).
[537] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, 411 F. Supp. 3d 333, 336-337, GID.C.00260, at 2–3 (FISA Ct. Dec. 17, 2019) (Collyer, J.).
[538] *Id.* at 337, GID.C.00260, at 3.
[539] *Id.*, GID.C.00260, at 3–4.
[540] *In re Accuracy Concerns*, GID.C.00261, at 2.
[541] Response to the Court's Order Dated December 17, 2019, *In re* Accuracy Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02 (FISA Ct. Jan. 10, 2020), https://repository.library.georgetown.edu/handle/10822/1057438 [https://perma.cc/7BYJ-S4ZV].
[542] Order Appointing an Amicus Curiae, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00263 (FISA Ct. Jan. 10, 2020) (Boasberg, J.).
[543] *See* Letter Brief of Amicus Curiae David Kris, *In re* Accuracy Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02 (FISA Ct. Jan. 15, 2020), https://repository.library.georgetown.edu/handle/10822/1057439.
[544] Order Regarding Handling and Disposition of Information, In re Carter W. Page, Nos. 16-1182, 17-52, 17-375, 17-679, GID.C.00265 (FISA Ct. Jan. 7, 2020) (Boasberg, J.).

In early March 2020, the FISC issued one of its strongest opinions to date, responding to government malfeasance. Judge Boasberg noted, "There is . . . little doubt that the government breached its duty of candor to the Court with respect to [the Carter Page] applications."[545] The frequency and seriousness of the misstatements to the Court called into question the reliability of other FBI information contained in applications.[546] Separate classified proceedings were underway dealing with how to sequester information acquired pursuant to the four FISA authorizations concerning Page.[547] Boasberg highlighted problems with reliance on the Steele dossier, and he analyzed and proposed remedial actions relating to the FISA application procedures, improvements in training and other institutional changes, and greater oversight.[548]

The FISC ordered that the government provide details on the new changes, training, audit, and compliance mechanisms.[549] It banned any DOJ or FBI personnel "under disciplinary or criminal review relating to their work on FISA applications [to] participate in drafting, verifying, reviewing, or submitting such applications to the court."[550] Beginning March 9, 2020, the court required that all Title I/III, PRTT, Section 1881b or Section 1881c applications include a statement verifying that the application fairly reflected "all information that might reasonably call into question the accuracy of the information or the reasonableness of any FBI assessment in the

---

[545] Corrected Opinion and Order, *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00272, at 1 (FISA Ct. Mar. 5, 2020) (Boasberg, J.).
[546] *Id.*
[547] *Id.* at 3–4.
[548] *See id.* at 5–13, 17–19 (e.g., including all contradictory information in FISA applications, with the aim of providing information that may undermine probable cause; revising the Woods form to emphasize an obligation to re-verify factual assertions and specify what steps must be taken during legal review before submitting to FBI director; potential for DOJ attorneys to visit FBI field offices to meet with case agents and review investigative files; and, requiring the FBI case agent attest to FISA application).
[549] *See id.* at 17–19. The Court ordered the government to provide: 1) a copy of the CHS (confidential human sources) checklist and status on its implementation; 2) a description of the current responsibilities FBI OGC lawyers have throughout the FISA process; 3) planned and implemented technological improvements to the process of preparing FISA applications; 4) a report on suggested ways of improving DOJ proactiveness in ensuring the completeness in FISA applications; 5) description of steps taken to have FBI field agents to serve as declarants in FISA applications; 6) a description of DOJ's Office of Intelligence Oversight Section's process and methodology for conducting completeness reviews, and the results of such reviews presented every six months starting Sept. 1, 2020; 7) a summary description of the FBI case-study training and FISA-process training courses, and confirmation, by July 3, 2020, that FBI personnel involved in the FISA process have been trained and certified; 8) a description of any audit, review, or compliance mechanisms planned or implemented bearing on the efficacy of the aforementioned remedial measures; 9) no DOJ or FBI personnel under disciplinary or criminal review relating to their work on FISA applications shall participate in drafting, verifying, reviewing, or submitting such applications to the Court; and 10) each application submitted to the Court shall have representations or attestations indicating that all information that reasonably calls into question the accuracy of the information, the FBI assessment, and the requested findings. *Id.*
[550] *Id.* at 18.

application, or otherwise raise doubts about the requested findings."[551] From the FBI in particular, the Court required an additional statement attesting that the Justice Department's Office of Intelligence had "been apprised of all information that might reasonably call into question the accuracy of the information or the reasonableness of any FBI assessment in the application, or otherwise raise doubts about the requested findings."[552]

Soon after the FISC issued its order, another memorandum from Horowitz came out, having examined 29 separate FISC applications targeting USPs between 2014–19.[553] Remarkably, *every single one* of the applications had errors.[554] The Woods procedures were not being followed in all of the cases; indeed, in at least four cases, there were no files at all backing up the application.[555] In those cases where there were files, some facts were not supported or corroborated by the documentation, or there were inconsistent claims being made to the FISC. On average, each application had approximately 20 issues, with up to 65 issues in just one of the applications examined.[556]

Within a week of the publication of the IG report, the FISC issued an order to the government directing it to provide the court with the names of the targets and docket numbers for the 29 applications reviewed by the OIG and specify which targets/docket numbers correspond to the 4 applications where there was no Woods file.[557] The government had to assess to what extent the 29 applications involved material misstatements or omissions, and whether any such material misstatements and omissions rend authorizations granted by the court for that target invalid.[558] By June 15, 2020, the government was to make sworn submission reporting on conduct and results of the assessment—including where determined not to render applications invalid.[559] The order further required from June 15, 2020 onward that every two months the government provide a progress report on the Woods files for all dockets on or after January 2015.[560]

E. *Overcollection and the Data Dilemma*

---

[551] *Id.* at 19.
[552] *Id.*
[553] Management Advisory Memorandum from Michael E. Horowitz, Inspector Gen., to Christopher Wray, Dir., FBI, regarding the Audit of the Federal Bureau of Investigation's Execution of its Woods Procedures for Application Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons at 2 (Mar. 30, 2020), https://repository.library.georgetown.edu/handle/10822/1058475 [https://perma.cc/V9N9-2DHH].
[554] *Id.* at 3, 7–8.
[555] *Id.* at 7.
[556] *Id.*
[557] *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00274, at 3, 2020 WL1975053, at *2 (FISA Ct. Apr. 3, 2020) (Boasberg, J.).
[558] *Id.*, 2020 WL 1975053, at *2.
[559] *Id.*, 2020 WL 1975053, at *2.
[560] *Id.* at 3–4, 2020 WL 1975053, at *2.

Overcollection is, as has already been noted, a consistent problem in the government's implementation of FISA. It appears to affect nearly every area of collection.

In 2010, for instance, unauthorized surveillance under Title I lasted between fifteen months and three years, resulting in what appears to be thousands of improperly intercepted communications.[561] The communications obtained were "presumably . . . unrelated to [redacted] or any other subject of foreign intelligence interest."[562] In that case, Judge Scullin ordered the government to report on whether all of the information obtained had been destroyed (with limited exceptions) and how SMPs would apply to proposed retention.[563] The following year, assumedly because it hadn't been destroyed, the same judge ordered that it be eliminated and prohibited any further use or disclosure of the information.[564]

In another case, the government collected too much information as part of its bulk collection of Internet metadata under the PRTT provisions. The government did not come clean until August 11, 2009—five years after it had been adopted; nevertheless, the problem persisted.[565]

In 2008, the government reported overcollection in the context of Section 702.[566] While the NSA had apparently implemented measures to filter out non-targeted communications prior to the communications entering repositories accessible to analysts,[567] in 2010 it emerged that the NSA had failed to purge databases of § 1881a information required under minimization procedures and had a backlog on post-targeting review of selectors.[568] Information that should have been deleted possibly ended up in reports disseminated by NSA.[569]

In 2011, the government proposed in regard to a Title I application that it be allowed to retain the fruits of unlawful surveillance.[570] The court was surprised

---

[561] *See*, Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00059, at 1–2 (FISA Ct. Dec. 10, 2010) (Scullin, Jr., J.).
[562] *Id.* at 5.
[563] *Id.* at 8.
[564] Opinion and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00067, at 9 (FISA Ct. May 13, 2011) (Scullin Jr., J.).
[565] [REDACTED], No. [REDACTED], GID.C.00073, at 16-17 n.14, 2011 WL 10945618, at *5 n.14 (FISA Ct. [REDACTED]) (Bates, J.). Note that the Westlaw citation has the relevant information omitted.
[566] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00039, at 17, 28-29 (FISA Ct. Apr. 7, 2009) (McLaughlin, J.).
[567] *Id.* at 23–-24.
[568] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00060, 9–12 (FISA Ct. 2010) (Bates, J.).
[569] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00062, at 3 (FISA Ct. 2010) (McLaughlin, J.).
[570] Memorandum Opinion and Order, [REDACTED], Nos. [REDACTED], GID.C.00067 (FISA Ct. May 13, 2011) (Scullin, Jr., J.).

to learn four years later that the NSA *still* had not been deleting overcollected § 702 records placed on the master purge list in accordance with a May 2011 Opinion and Order.[571]

These and other cases point to what could be termed the data dilemma, which really has two constituent parts: first, what to do with communications intercepted outside the statutory and judicial restrictions; second, how to ensure that the government does with the information what it has been told to do. The courts' roles in both regards is very different than what it was originally designed to do. In large part this stems from the programmatic nature of collection under FISA—an instrument designed for more narrowly-targeted surveillance.

The data dilemma also gives rise to an associated concern, which is that the requests being put to it by the government come perilously close to the line in terms of asking for Advisory Opinions—an authority denied to Article III entities under the case-or-controversy requirement.

VI. FISC/FISCR Jurisprudence Going Forward

Over the past two decades, the roles assumed by the FISC and FISCR have evolved well beyond what Congress originally envisioned. Instead of just determining whether orders should be issued for electronic surveillance, they have had to grapple with their authority as Article III courts with specialized subject matter jurisdiction and to ascertain the extent to which they can rely on their non-statutory, inherent powers. The tension between new and emerging technologies and old statutory language has put the court into the position of having to delve deeply into telecommunications, mobile computing, and network sciences. Tension among ever more sweeping surveillance programs, national security concerns, and individual rights has forced the court to address difficult constitutional questions.

Persistent misbehavior on the part of the government presents an increasingly difficult challenge. Part of the problem derives from the ever more complex nature of the statutory and regulatory regime, as well as the technologies involved. Legal and technical expertise have historically been kept separate. More rigorous training and altering institutional arrangements, such as embedding NSD attorneys in NSA operations, may go some way toward meeting this challenge. But the underlying issue in some ways is much broader and relates to the decades of specialization that mark expertise in these different areas. Conflict between the need for discussion and protecting sensitive national security information further complicates the picture.

---

[571] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00121, at 58 (FISA Ct. Nov. 6, 2015) (Hogan, J.) (citing to Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00059, (FISA Ct. Dec. 10, 2010) (Scullin, Jr., J.); Opinion and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00067, at 9 (FISA Ct. May 13, 2011) (Scullin Jr., J.)).

Compounding the situation is the limited insight that the courts have into the inner workings of the Executive Branch—a concern at times augmented by the government's persistent disregard of statutory and judicial limits. While FISA provides for criminal penalties, the court and the Justice Department have been reluctant to invoke them. To the contrary, in a number of cases of overcollection, the government has actively sought permission simply to keep the data obtained outside statutory or judicial authorization.

Going forward, one alternative may be for Congress to create an independent entity, with deep technical expertise, which will allow for careful oversight of how the agencies conduct their operations. Such an organization could be either attached to the court or to the agencies in question, with an independent head of operations appointed by Congress—much like a number of the offices of Inspectors General. Such entities would have the additional advantage of providing a focal point for reporting, which has in many ways gotten out of control. Absent an institutional fix, it falls to the FISC/FISCR, and to government attorneys acting in good faith, for the system to work. Looked at in this light, the FISC's recent actions following Horowitz I and II were both necessary and important.

As we look toward the future, there are a few trends of note in terms of what we should expect to see. First, the demand for FISC opinions will likely, if anything, increase. What is being adjudicated is law, and the public does and will demand the right for access to it. Simultaneously, it is likely that these opinions will continue to demonstrate the four tensions identified in this Article. In addition, there may be movement in two key areas: first, notably absent from the opinions that have been made public is information related to §§ 703-704. Undoubtedly, this area, like the others, will fall subject to the concerns highlighted above. Second, we have seen only two opinions, out of nearly 90, which deal with the associational rights of the First Amendment. As non-specialized, geographically focused Article III courts begin to wrestle more with these issues in the context of new and emerging technologies, in light of FISA's emphasis of First Amendment protected activities, it is likely that we will see more discussion of these vital constitutional rights.