ARTICLE

401–FORBIDDEN: AN EMPIRICAL STUDY OF FOREIGN INTELLIGENCE SURVEILLANCE ACT NOTICES, 1990–2020

Sarah Beller[*]

ABSTRACT

The Foreign Intelligence Surveillance Act ("FISA") is one of the government's most powerful spying tools, but the public knows little about how the law is used and cannot hold the government accountable for privacy violations and overreach. FISA requires the government to give official notice to people it spied on before it uses surveillance evidence against them in court. Despite notice being a key oversight mechanism, there has never been a comprehensive investigation of FISA notices or the people who receive them. This Article fills that gap by compiling and publishing the first exhaustive collection of all 401 notices given between 1990 and 2020. Examining the notice recipients leads to two main insights.

First, advocates have hypothesized for years that the government disproportionately uses its surveillance and law enforcement powers against Muslim-Americans, and increasingly against Chinese-Americans. The notice recipients show dramatic demographic and ideological disparities that align with those theories. Although the recipients are a small subset of all FISA targets, they represent a rare empirical look at surveillance in practice, and the trends support calls for increased transparency about and scrutiny of FISA usage to ensure that the same troubling patterns are not present in the larger set of targets.

Second, this group is the entire population of instances where the government has publicly used FISA evidence in court. After the Supreme Court's 2013 opinion in Clapper v. Amnesty International USA*, they are the only people with standing to challenge FISA's constitutionality. Their cases reveal insurmountable procedural hurdles in litigating against FISA evidence, obstacles that threaten to undermine the adversary system and erase constitutional protections for criminal defendants.*

[*] Law Clerk, U.S. District Court for the Central District of California.

CONTENTS

INTRODUCTION....160
I. FISA KNOWNS AND UNKNOWNS....166
II. DATA COLLECTION AND ANALYSIS....169
A. *Overview of Methodology*....169
B. *Brief Overview of the Dataset*....171
III. NATIONAL SECURITY THREATS IN FISA CASES....175
A. *Concerns About Bias and Threat Prioritization in Surveillance Decisions*....176
B. *Trends in FISA Notice Cases*....181
1. Demographics....181
2. Alleged National Security Threats....185
3. Tenuous Terrorism Charges....188
C. *Implications of Results for FISA Reform*....192
IV. LITIGATING AGAINST FISA EVIDENCE....194
A. *Litigating FISA in Theory*....194
B. *FISA Litigation in Practice*....195
1. Courts have so narrowly construed FISA's disclosure mechanism and the Franks standard that no defendant has ever seen their FISA warrant or affidavit....195
2. The government uses its classification power to defendants' detriment....198
C. *Implications of Results of Litigation*....201
V. CONSTITUTIONAL CHALLENGES....203
A. *Squaring FISA and the Fourth Amendment*....203
1. Probable Cause....204
2. Particularity....205
3. Notice....206
4. Warrantless Surveillance under Section 702....206
B. *Adjudicating FISA's Constitutionality*....207
C. *Implications for Accountability*....210
CONCLUSION....211
APPENDIX....213
A. *Notice Collection*....213
1. Docket Searches....213
2. ACLU Compilation....214
3. The Intercept's Trial and Terror Database....214
4. Treatises....215
5. Opinion Searches....216
6. News Articles....217

7. Westlaw Key Numbers.....217
8. Potential Reasons for Missing Notices.....218
B. *Recipient Information Collection* 219
C. *Dataset Representativeness* 221

INTRODUCTION

As Professor Xi Xiaoxing and his family slept, a dozen armed Federal Bureau of Investigation ("FBI") agents broke into their house and arrested him.[1] The government charged Xi with selling trade secrets to China[2] and Temple University subsequently stripped him of his position as Chair of the Physics Department.[3] Professor Xi then received a one-sentence letter:

> The United States of America . . . provides notice to defendant Xiaoxing Xi and to the Court, that pursuant to Title 50, United States Code, Sections 1806(c) and 1825(d), the United States intends to offer into evidence, or otherwise use or disclose in any proceedings in the above-captioned matter, information obtained or derived from electronic surveillance and physical search conducted pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801–1812 and 1821–1829.[4]

After almost five months of trying to obtain this foreign intelligence evidence, the government gave Professor Xi's lawyers its supposed smoking gun: a diagram of a pocket heater, a restricted device used to create semiconductors.[5] It immediately became apparent to Professor Xi that the diagram was of a different, unrestricted device. After leading scientists—including a co-inventor of the pocket heater—informed the Department of Justice ("DOJ") that their case was baseless,[6] the government quietly dismissed the charges by telling the court that "additional information came

---

[1] Matt Apuzzo, *U.S. Drops Charges That Professor Shared Technology with China*, N.Y. TIMES (Sept. 11, 2015), https://www.nytimes.com/2015/09/12/us/politics/us-drops-charges-that-professor-shared-technology-with-china.html [https://perma.cc/3BBP-VJ88].
[2] Indictment, United States v. Xi, No. 2:15-cr-00204 (E.D. Pa. May 14, 2015), ECF No. 1.
[3] Apuzzo, *supra* note 1.
[4] Notice of Intent to Use Foreign Intelligence Surveillance Act Information, United States v. Xi, No. 2:15-cr-00204 (E.D. Pa. June 9, 2015), ECF No. 16.
[5] Apuzzo, *supra* note 1.
[6] *Id.*

to [their] attention."[7]

A decade earlier, Sami Al-Hussayen was completing his Computer Science PhD at the University of Idaho and volunteering as webmaster for a Muslim non-profit that hosted religious websites.[8] The government arrested him in his dormitory and charged him with material support of terrorism based on others' blog posts on those websites, in addition to visa fraud for not disclosing his volunteer webmaster role.[9] Mr. Al-Hussayen received an almost-identical one-sentence letter notifying him that he had been spied on under the Foreign Intelligence Surveillance Act ("FISA").[10]

The FBI told Mr. Al-Hussayen that it had intercepted tens of thousands of his calls and emails,[11] but the government refused to declassify the recordings apart from the few it planned to use.[12] Because the recordings were classified, the government did not allow Mr. Al-Hussayen to listen to his own calls, and prohibited his cleared attorneys from discussing them with him to determine which could help his case. Worse, almost all the calls were in Arabic, which his attorneys did not speak, and the defense could not find local translators with security clearances.[13] After ten months of asserting the grave national security risk of declassifying the calls, the government declassified everything the weekend before trial.[14] Despite these litigation hurdles for the defense, the jury found that "[t]here was a lack of hard evidence" for any of the government's allegations.[15] Ultimately, the jury acquitted Mr. Al-Hussayen of all terrorism charges and hung on all lesser charges.

---

[7] Government's Unopposed Motion to Dismiss, United States v. Xi, No. 2:15-cr-00204 (E.D. Pa. Sept. 11, 2015), ECF No. 29.

[8] Indictment at 6–7, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Feb. 13, 2003), ECF No. 1.

[9] Superseding Indictment, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Jan. 9, 2004), ECF No. 378.

[10] Notice of Intent to Use Foreign Intelligence Surveillance Act Information, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Mar. 11, 2003), ECF No. 33.

[11] Memorandum in Support of Motion to Suppress at 3, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho June 27, 2003), ECF No. 90.

[12] Memorandum in Support of Motion to Declare CIPA Unconstitutional as Applied at 1–2, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Feb. 17, 2004), ECF No. 446.

[13] *Id.* at 3–4.

[14] Motion in Limine (FISA derived evidence) at 2, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Apr. 16, 2004), ECF No. 578.

[15] Associated Press, *No Conviction for Student in Terror Case*, N.Y. TIMES (June 11, 2004), www.nytimes.com/2004/06/11/us/no-conviction-for-student-in-terror-case.html [https://perma.cc/4FKS-EPYP].

Ordinary American citizens and residents collaborate on work projects and volunteer for community groups every day. But each year a few dozen people, frequently Muslims and those of Chinese descent, are arrested and sent a notice like the ones Professor Xi and Mr. Al-Hussayen received. This barebones letter thrusts people into the Kafkaesque world of FISA litigation, where they must challenge allegations based on secret evidence they are not allowed to see.[16]

FISA was originally designed to curb government abuses of power. Congress passed FISA[17] in 1978 in response to public concern about warrantless wiretapping and other intelligence scandals.[18] FISA aimed to control extralegal surveillance by requiring advance court authorization; in return, the government could search for foreign intelligence information using a lower standard than that required for a regular criminal investigation. Public transparency was intended to increase efficiency and professionalism and preserve constitutional rights. But FISA's goals of improving government accountability have failed. Instead, based on even the limited information available to the public discussed in Part I, it is increasingly clear that the intense secrecy surrounding the statute has enabled mass surveillance with little public insight into how the law's powerful tools are used.

Surveillance under FISA differs dramatically from ordinary searches and wiretapping. Generally, to search someone's home or access stored communications, the government must prove to a judge that there is probable cause to believe the subject is involved in criminal activity and that the specific thing to be searched will yield evidence.[19] To intercept communications in real time, the Wiretap Act of 1968 requires the

---

[16] *See infra* Part IV.

[17] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 102, 92 Stat. 1786 (1978).

[18] The Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, known as the Church Committee, investigated intelligence abuses from 1975 to 1976. The information released (or leaked) caused significant public outrage. *See generally* William Safire, *Inside Church's Bunker*, N.Y. TIMES (Mar. 4, 1976), timesmachine.nytimes.com/timesmachine/1976/03/04/75577234.html [https://perma.cc/PG2L-VWQW] (mentioning a CIA-run "illegal domestic intelligence operation" and the wiretapping of Dr. Martin Luther King, Jr. as among the report's contents).

[19] *See* U.S. CONST. amend. IV.

government to explain why less invasive methods are insufficient.[20] In contrast, under FISA, the government does not have to prove probable cause of criminal activity; it simply provides cause that the subject is an "agent of a foreign power" and certifies that a "significant purpose" of the search is to obtain "foreign intelligence information,"[21] all nebulous terms. "Foreign powers" can include any non-domestic political group, such as Greenpeace or Oxfam.[22] Judges on the secret FISA Court ("FISC") have limited ability to question applications and must grant a surveillance order if the requirements are met.[23] If the subject of an ordinary search warrant or wiretap order is prosecuted, they may see and challenge the warrant or wiretap application and evidence. But under FISA, defendants must challenge surveillance without being allowed to see the application, order, or evidence against them.[24]

These minimal requirements were reduced even further after 9/11. FISA originally required "[t]he purpose" of surveillance to be to obtain foreign intelligence information, meaning that foreign intelligence had to be the government's *primary* purpose.[25] The Patriot Act gave the government even more discretion by changing that language to "a significant purpose."[26] That shift allows the government to use FISA when its primary purpose is ordinary law enforcement, so long as *a* purpose relates to foreign intelligence.

The standards for surveillance are even lower if the target is not American. In 2008, Congress added a new provision, known as Section 702, that allows the government to obtain yearlong orders to surveil non-Americans abroad, capturing all their communications with almost no restrictions.[27] Section 702 does not require the government to specify the people targeted or demonstrate any probable cause; all that is required is a government certification that the targets are "reasonably believed" to be

---

[20] Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2518(3)(c) (1986).
[21] 50 U.S.C. §§ 1804(a)(3), 1823(a)(3); 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B).
[22] *See, e.g.*, *id.* § 1801(a)(5).
[23] *See id.* § 1805(a).
[24] *Id.* §§ 1806(f), 1825(g), 1845(f).
[25] *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) ("[T]he executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons.").
[26] USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 291 (2001) (amending 50 U.S.C. §§ 1804(a)(7)(B), 1823(a)(7)(B)).
[27] 50 U.S.C. § 1881a.

outside the United States and are not Americans or permanent residents.[28]

Given this lower bar for surveillance, Congress created a notice requirement to increase accountability: FISA requires the government to inform people when it intends to use "any information obtained or derived from an electronic surveillance of that aggrieved person" against them in a court proceeding.[29] As Professor Xi's notice illustrates, these notices are perfunctory and give almost no personalized information. There is no indication of when or why the surveillance was authorized, or whether the recipient was the target or swept up in an unrelated investigation.

While the notice provision is central to FISA's accountability goals, there are very few instances of notice actually being provided. Unlike the several hundred thousand people estimated to be spied on under various FISA provisions each year,[30] people who receive notices are the rare few who can prove that they were surveilled. This is critical after the Supreme Court's 2013 opinion in *Clapper v. Amnesty International USA*.[31] In *Clapper*, human rights organizations and defense attorneys challenged FISA's constitutionality based on their "reasonabl[e] belie[f]" that the government was surveilling their communications with clients, colleagues, and other contacts.[32] The Court rejected the challenge after finding that the harm of such surveillance was not "certainly impending" or "fairly traceable" to FISA.[33] As a result, only people who are *certain* that they were surveilled have standing to challenge the statute's constitutionality. A core basis of the Court's decision was the belief that the government was giving criminal defendants notice of FISA surveillance, and therefore that potential litigants existed who could sufficiently prove standing.[34] After this decision, FISA notice recipients are arguably the only people "*Clapper*-qualified" to challenge the law.[35]

---

[28] *Id*.

[29] *Id*. §§ 1806(c) (electronic surveillance), 1825(d) (physical searches), 1845(c) (pen register/trap-and-trace surveillance), 1880e(a)(1), 1880e(b) (international surveillance).

[30] *See infra* Part I for estimates from public disclosures.

[31] 568 U.S. 398 (2013).

[32] Complaint at 2, Amnesty Int'l USA v. McConnell, No. 1:08-cv-06259 (S.D.N.Y. July 10, 2008), ECF No. 1.

[33] *Clapper*, 568 U.S. at 414.

[34] *Id*. at 421.

[35] Order Denying Motion to Suppress Evidence Obtained or Derived Under FISA Amendments Act or for Discovery at 3, United States v. Muhtorov, No. 1:12-cr-00033 (D. Colo. Nov. 19, 2015), ECF No. 885.

Despite the importance of these notice provisions for oversight, "discussion of how FISA-derived evidence makes its way into a criminal prosecution is rendered largely an afterthought,"[36] and there has never been a comprehensive investigation of FISA notices. This Article fills that gap by compiling and publishing the first exhaustive set of FISA notices given between 1990 and 2020. Examining the recipients of these notices leads to two main insights.

First, advocates have hypothesized for years that the government disproportionately uses its surveillance and law enforcement powers against Muslim-Americans, and increasingly against Chinese-Americans. The notice recipients show dramatic demographic and ideological disparities that align with advocates' theories. Although the recipients are a small subset of all FISA targets, they are a rare empirical look at surveillance in practice, and these trends support calls for increased transparency about and scrutiny of FISA usage to ensure that the same troubling patterns are not present in the larger set of targets.

Second, this group is the entire population of instances where the government publicly uses FISA evidence in court. Their cases reveal insurmountable procedural hurdles in litigating against FISA evidence, obstacles that threaten to undermine the adversary system and erase constitutional protections for criminal defendants.

* * *

This Article proceeds in five Parts. Part I canvasses the small amount of public information about FISA usage, which shows that hundreds of thousands and potentially millions of Americans are spied on every year. Given the breadth of this government intrusion and the lack of publicly available information, Part I also explains why this notice dataset is a critical window into foreign intelligence surveillance and prosecution. Part II gives an overview of my data collection methodology and provides a descriptive portrait of the notice recipients and their cases.

Part III explains the first contribution of this Article, namely that notice recipients show dramatic demographic and ideological disparities that warrants greater transparency about FISA usage. Part III outlines academics' hypotheses that FISA disproportionately targets Muslims,

---

[36] WADIE E. SAID, CRIMES OF TERROR: THE LEGAL AND POLITICAL IMPLICATIONS OF FEDERAL TERRORISM PROSECUTIONS 78 (2015).

Chinese-Americans, and immigrants for surveillance while excluding internationally linked white supremacists. I then discuss findings about the demographics of people who receive notices and the outcomes of their cases. I find that a significant proportion were not charged with any terrorism- or national security-related offenses, despite the government claiming links to terrorist groups. In addition, the terrorism-related charges seemed weaker than those in other federal cases, as FISA defendants were acquitted and had charges dismissed at appreciably higher rates than usual. I then consider implications of these findings for FISA reform efforts.

Parts IV and V discuss the second contribution of this Article: these FISA cases reveal insurmountable procedural hurdles that erode constitutional protections for criminal defendants. Part IV examines the difficulties of litigating against FISA evidence, which include secret and unchallengeable warrants and limited access to classified evidence. I find that people rarely file motions relating to FISA evidence—and when they do, they are almost uniformly denied. These obstacles distort the functioning of the adversary system and raise substantial fairness concerns, since non-FISA defendants charged with similar crimes have significantly greater ability to challenge the evidence against them.

Part V discusses constitutional concerns with FISA, particularly as amended by the FISA Amendments Act and Patriot Act, and analyzes the dearth of public court decisions considering the statute's constitutionality. I find that very few notice recipients make constitutional challenges, mainly those represented by a small cadre of experienced defense attorneys. The lack of litigated challenges combined with minimal judicial inquiry raises concerns about missing oversight of this wide-reaching law.

I. FISA KNOWNS AND UNKNOWNS

Every year, the government publishes glossy "transparency reports" about how the intelligence community uses FISA.[37] These reports suggest an intelligence community that is a model of restraint: the government files one to two thousand FISA applications a year, targeting about the same

[37] *See, e.g.*, OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, STATISTICAL TRANSPARENCY REPORT REGARDING USE OF NATIONAL SECURITY AUTHORITIES: CALENDAR YEAR 2019 (2020), www.dni.gov/files/CLPT/documents/2020_ASTR_for_CY2019_FINAL.pdf [https://perma.cc/G9LF-XPY6] [hereinafter DIR. OF NAT'L INTELLIGENCE, 2019 TRANSPARENCY REPORT].

number of people.[38] These numbers may seem insignificant. But FISA's power is obscured by these statistics, because having one "target" means that everyone who communicates with that person is surveilled—think of how many people you contact every month by phone, text, email, and other messaging applications. There is no public information on the total number of people, or the number of Americans, on whom the government has spied.

Technology companies present a clearer window into the true scale of surveillance. While the number of FISA orders each company receives is low, the number of user accounts accessed by the government has risen dramatically: Facebook reports a 20x increase (2013–2019);[39] Google a more than 50x increase (2009–2019);[40] and Apple an over 100x increase (2013–2019)[41] in the number of accounts they are ordered to turn over to the government each year.[42]

---

[38] *Foreign Intelligence Surveillance Act Court Orders 1979-2017*, ELEC. PRIVACY INFO. CTR., ftp.epic.org/privacy/surveillance/fisa/stats/ [https://perma.cc/EK4V-B9NE] (compiling a list of figures from annual reports); DIR. OF NAT'L INTELLIGENCE, 2019 TRANSPARENCY REPORT, *supra* note 37, at 10, 26.

[39] *Transparency Report: Government Requests: United States*, FACEBOOK, transparency.facebook.com/government-data-requests/country/US [https://perma.cc/ZQQ5-D2WV].

[40] *Transparency Report: United States National Security Requests for User Information*, GOOGLE, transparencyreport.google.com/user-data/us-national-security [https://perma.cc/54ZA-S7LH].

[41] *Transparency Report: United States of America*, APPLE, www.apple.com/legal/transparency/us.html [https://perma.cc/ZQQ5-D2WV?type=image]. Apple's earlier reporting aggregates FISA orders and National Security letters, disaggregating beginning in 2018.

[42] Microsoft is a low outlier on content orders. *U.S. National Security Orders Report*, MICROSOFT, www.microsoft.com/en-us/corporate-responsibility/us-national-security-orders-report [https://perma.cc/S9W3-5SEJ].

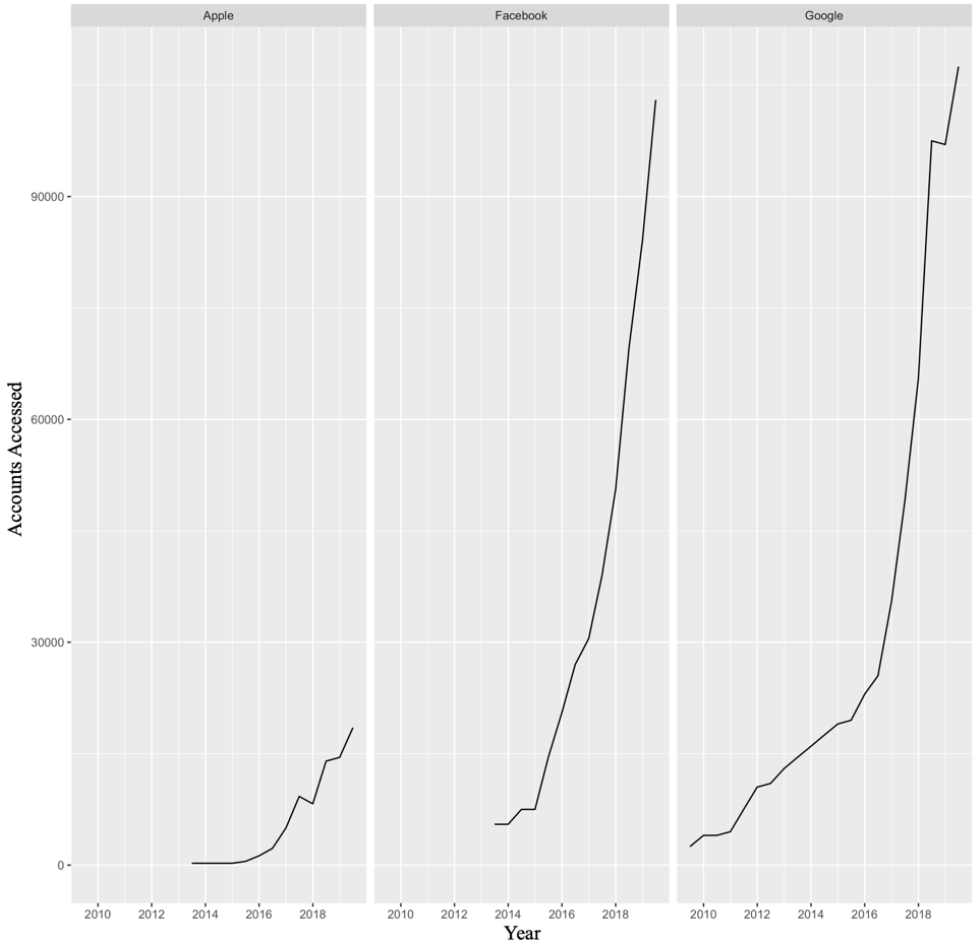

Figure 1: Upper bound of accounts accessed through FISA orders and directives

In addition to these private-sector reports, the government publishes some information about people targeted in bulk warrantless searches under Section 702.[43] That number has also risen considerably and passed 200,000 targets in 2019.[44] While Section 702 targets are supposed to be non-Americans abroad, the records collected frequently include "incidental" collection of Americans' communications, which are then stored in government databases. The National Security Agency ("NSA") searches these databases for information about Americans up to 30,000 times a year.[45]

---

[43] *See infra* Part V.A.4 for a discussion of constitutional concerns with Section 702's warrantless and broad searches.

[44] DIR. OF NAT'L INTELLIGENCE, 2019 TRANSPARENCY REPORT, *supra* note 37, at 14.

[45] *Id.* at 16.

As a result of these partial disclosures, all we know is that the government "targets" several hundred thousand people and organizations every year for surveillance, but with such a broad net that it sweeps up the private communications of many times that number, including potentially millions of Americans.

What the government refuses to disclose is how many people it actually surveils each year under FISA, and how many of those are American citizens or residents. When Congress pushed for an estimate of how often Americans are "incidentally" surveilled by Section 702's warrantless searches, the government admitted that it had no idea and argued that it was "infeasible" for the NSA to calculate how many Americans' communications are intercepted.[46] And the FBI refuses to report how often it searches for Americans in the bulk database, though doing so is a routine part of its investigations performed without a warrant or any suspicion of wrongdoing.[47]

While we know that many people are monitored and searched under FISA each year, very few receive notice: I found only 401 people who had received a notice over the past three decades. These 401 are a tiny fraction of the hundreds of thousands of people surveilled each year.

II. DATA COLLECTION AND ANALYSIS

A. Overview of Methodology

I relied primarily on docket searches through Bloomberg and LexisNexis, both of which index the U.S. Courts' Public Access to Court Electronic Records ("PACER") system and various state court docket databases. I searched for keywords aimed at finding FISA notices, including statutory provisions and wording common to many notices. I then performed a series of checks to ensure that the dataset was exhaustive,

---

[46] *Open Hearing on FISA Legislation: Hearing Before the S. Comm. on Intelligence*, 115th Cong. (2017) (statement of Daniel Coats, Dir. of Nat'l Intelligence); Letter from Ron Wyden, Sen., to Daniel Coats, Sen., Nominee for Dir. of Nat'l Intelligence (Mar. 8, 2017), assets.documentcloud.org/documents/3518073/Wyden-Coats.pdf [https://perma.cc/VQF6-QPTU].

[47] Neema Singh Guliani, *Congress Just Passed a Terrible Surveillance Law. Now What?*, ACLU (Jan. 18, 2018), https://www.aclu.org/blog/national-security/privacy-and-surveillance/congress-just-passed-terrible-surveillance-law-now [https://perma.cc/B8DH-XFYJ].

including keyword searches of court opinions, citations in major national security treatises, news articles, links to Westlaw Key Numbers, citations to published FISA cases from every circuit, and cross-references against an *Intercept* database and a manually gathered American Civil Liberties Union ("ACLU") collection of notable cases from 2009 onwards. I found decreasing numbers of previously undiscovered cases in each subsequent source I searched, and I found no additional cases in the final two sources. These results give me high confidence that the notice dataset is as exhaustive and complete as possible. Appendix A contains a detailed description of my data collection process and explores some factors that may have caused notices to be missing, primarily spotty digitization of court records through the 1990s.

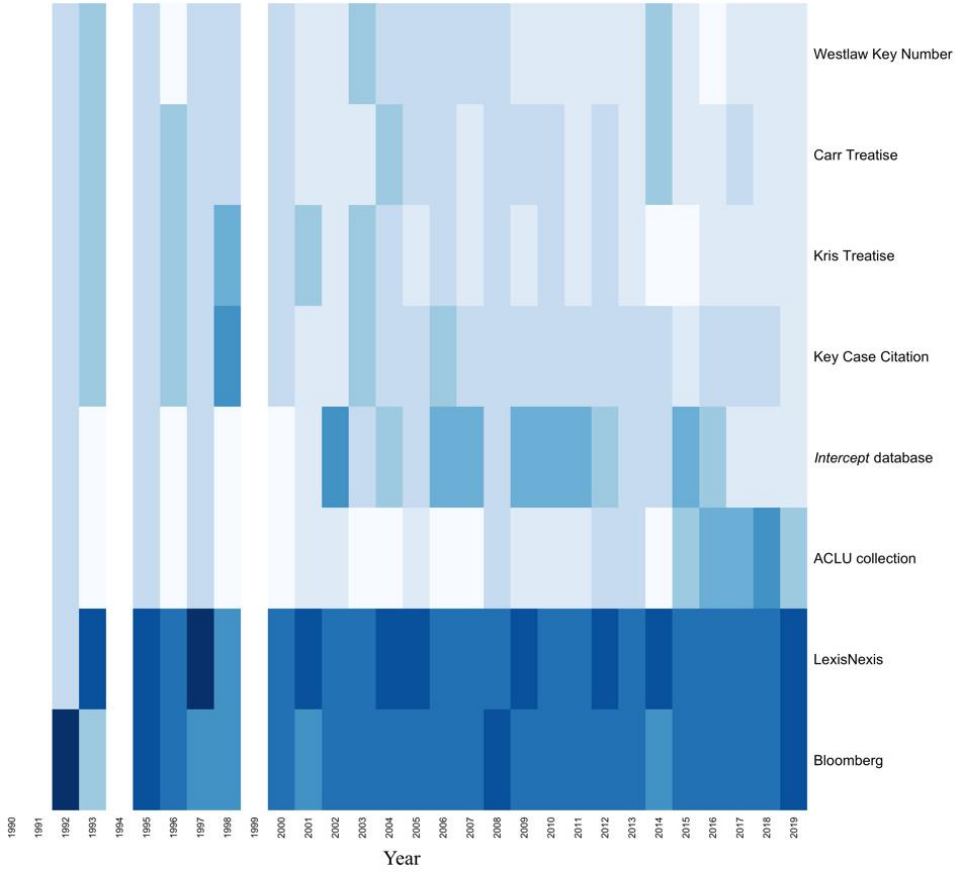

Figure 2: Case coverage by source

Once I had collected the set of notices, I gathered information about each of the people who received notice to build out a useful picture of the pool. This included biographical data, charges and related groups, and litigation strategy and case outcomes. I cross-referenced the list with the

DOJ National Security Division's International Terrorism and Terrorism-Related Convictions Chart, a list of allegedly international terrorism-related convictions since 9/11.[48] I then cleaned and standardized the data to enable comparisons across jurisdictions and time periods, which often differed in how charges were described or foreign groups spelled. I calculated several composite datapoints for each recipient based on other information, including whether the recipient was a "U.S. person" under FISA. I describe the information gathered and transformations applied in more detail in Appendix B. The original and transformed datasets are available online for public use at https://purl.stanford.edu/gw191zv5762.

B. Brief Overview of the Dataset

In total, I found 401 notices in 222 cases. I was able to obtain 278 of these; the remaining notices are either sealed or not docketed despite the government or judge confirming that notice was given.[49] As expected, almost all notices (97%) were given in federal criminal cases. One notice was given in a state criminal case,[50] because the surveillance uncovered a family murder for which there were no available federal charges. Two notices were given in courts-martial.[51] Finally, five notices were given in civil cases, which was unexpected. Those cases were two civil rights lawsuits relating to unlawful detention;[52] a challenge to being labeled a

---

[48] NAT'L SEC. DIV., DEP'T OF JUST., PUBLIC/UNSEALED INTERNATIONAL TERRORISM AND TERRORISM-RELATED CONVICTIONS FROM 9/11/01 TO 12/31/18 (updated Dec. 17, 2019), https://cdn.muckrock.com/foia_files/2020/07/27/NSD_Chart_of_Convictions_9-11-01_to_12-31-18_Updated_12-17-19.pdf [https://perma.cc/CA64-F4UH]. There are numerous concerns with the skewed coverage of the list, but it remains an important look into internal DOJ categorization. *See, e.g.*, Shirin Sinnar, *More Misleading Claims on Immigrants and Terrorism*, JUST SEC. (Mar. 4, 2017), www.justsecurity.org/38341/misleading-claims-immigrants-terrorism/ [https://perma.cc/T24B-BS28].

[49] *See, e.g.*, Memorandum in Opposition to Sabirhan Hasanoff's Motion to Correct, Vacate, or Set Aside His Conviction at 11 n.7, United States v. El-Hanafi, No. 1:10-cr-00162 (S.D.N.Y. Feb. 11, 2015), ECF No. 208 ("During discovery, the Government provided Hasanoff's counsel with notice for purposes of 50 U.S.C. §§ 1806(c) and 1825(d)."); FISA Notification, United States v. Chen, No. 05-cr-00659 (D.N.J. Sept. 13, 2005), ECF No. 21 ("This same notice previously was given to defendants orally on or about July 21, 2004.").

[50] People v. El-Astal, No. 07-005092-01-FC (3d Jud. Cir. of Mich., Crim. Div. Feb. 2, 2007).

[51] United States v. Millay, No. 3:13-mc-00005 (D. Alaska Jan. 17, 2013); United States v. Hasan, No. 6:12-cv-00195 (W.D. Tex. July 27, 2012).

[52] Al-Kidd v. Ashcroft, No. 1:05-cv-00093 (D. Idaho Mar. 15, 2005); Mayfield v. United States, No. 6:04-cv-01427 (D. Or. Oct. 4, 2004).

Specially Designated Global Terrorist;[53] a challenge to denial of naturalization;[54] and a wrongful death claim where the government gave notice to the surveillance subject's estate.[55]

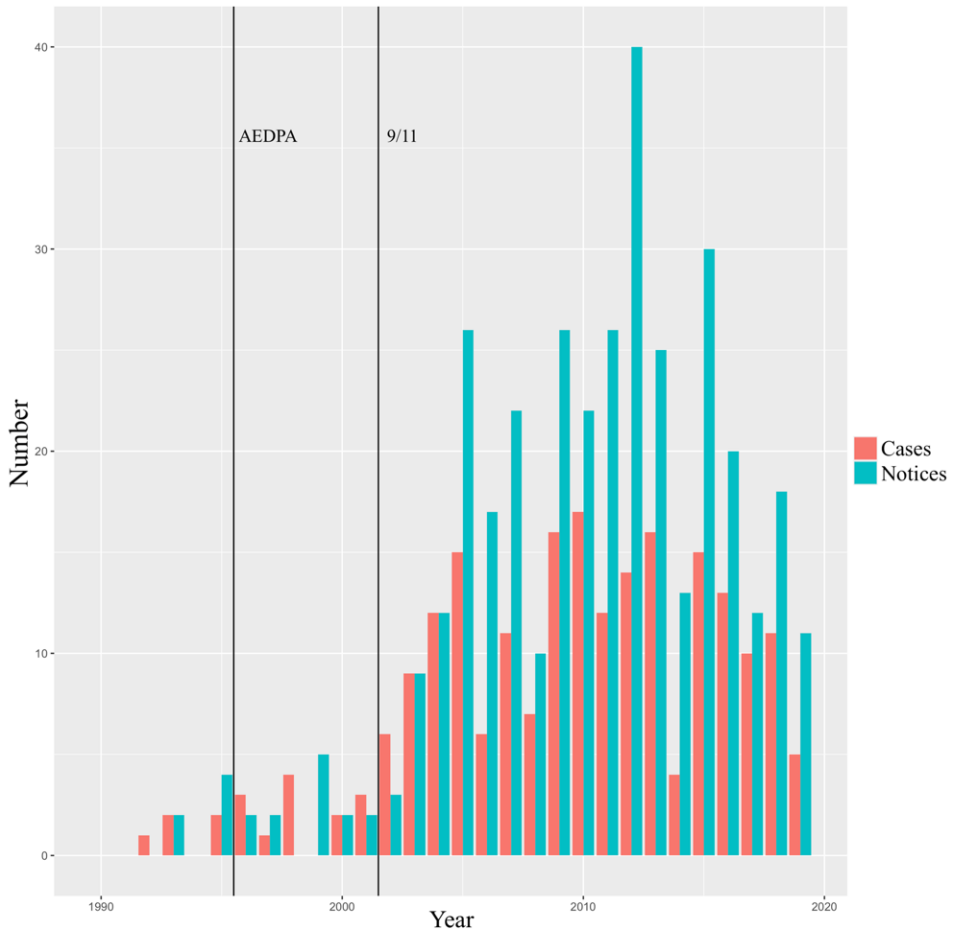

Figure 3: FISA notices and cases by year

There was no significant change in the number of notices given after the material support of terrorism offenses were created in 1994 and 1996,

[53] Complaint, Kindhearts for Charitable Humanitarian Development, Inc. v. Paulsen, No. 3:08-cv-02400 (N.D. Ohio Oct. 9, 2008), ECF No. 1.

[54] Complaint, Atalla v. Kramer, No. 2:09-cv-01610 (D. Ariz. Aug. 4, 2009), ECF No. 1.

[55] Government's Notice of Intent to Use Foreign Intelligence Surveillance Act Information, Estate of Usaamah Abdullah Rahim v. United States, No. 1:18-cv-11152 (D. Mass. Dec. 17, 2018), ECF No. 44 ("In providing notice, the government does not concede that notice was statutorily required in this case; the United States is providing notice in an abundance of caution based on the specific facts and circumstances of this case.").

which might have been expected to provide more bases for surveillance.[56] The Patriot Act of 2001 weakened the requirement that obtaining foreign intelligence be the "primary" purpose of using FISA, switching to "a significant purpose," which led to a noticeable rise in FISA notices along with a rise in warrants.[57] However, the number of notices has not increased markedly since 2005 (excluding one multi-defendant case in 2012).

Orders Granted by FISA Provision

	Electronic & Physical Search	Electronic Search Only	Physical Search Only	Section 702	Pen/Trap
2016	1312	100	39	0	60
2017	1176	96	29	Classified	32
2018	953	85	37	Classified	32
2019	704	73	33	Classified	22

Notices by FISA Provision

	Electronic & Physical Search	Electronic Search Only	Physical Search Only	Section 702	Pen/Trap
2016	12	4	1	1	0
2017	12	0	0	0	0
2018	13	4	0	1	0
2019	6	4	0	0	0

Figure 4: FISA orders granted and notices sent 2016–2019 by statutory provision

As previously explained in Part I, the FISC grants several thousand FISA orders every year, each of which is authorized by one or more specific provisions in FISA. The FISA provision used was specified in 78% of notices, and the number of notices broadly tracks the proportion of FISA orders granted under each individualized surveillance provision. Almost every notice included electronic search, and two-thirds of notices included physical search—while the name implies a search of a place, the provision also applies to physical searches of electronics such as extracting the

[56] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103–322, § 120005, 108 Stat. 1796, 2022–23 (1994) (creating 18 U.S.C. § 2339A); Antiterrorism and Effective Death Penalty Act of 1996, Pub. L. No. 104–132, § 303, 110 Stat. 1214, 1250–53 (creating 18 U.S.C. § 2339B).

[57] RICHARD B. ZABEL & JAMES J. BENJAMIN, JR., HUMAN RIGHTS FIRST, IN PURSUIT OF JUSTICE: PROSECUTING TERRORISM CASES IN THE FEDERAL COURTS 81 (May 2008) ("The adoption of the 'significant purpose' standard has resulted in a marked increase in FISA warrants.").

contents of a hard drive.[58] Very few FISA orders or notices involved pen registers, a twentieth-century device that tracks incoming and outgoing dialed numbers, likely because the government can obtain this information with a simple subpoena,[59] and it is included if the government is already accessing the contents of communications.

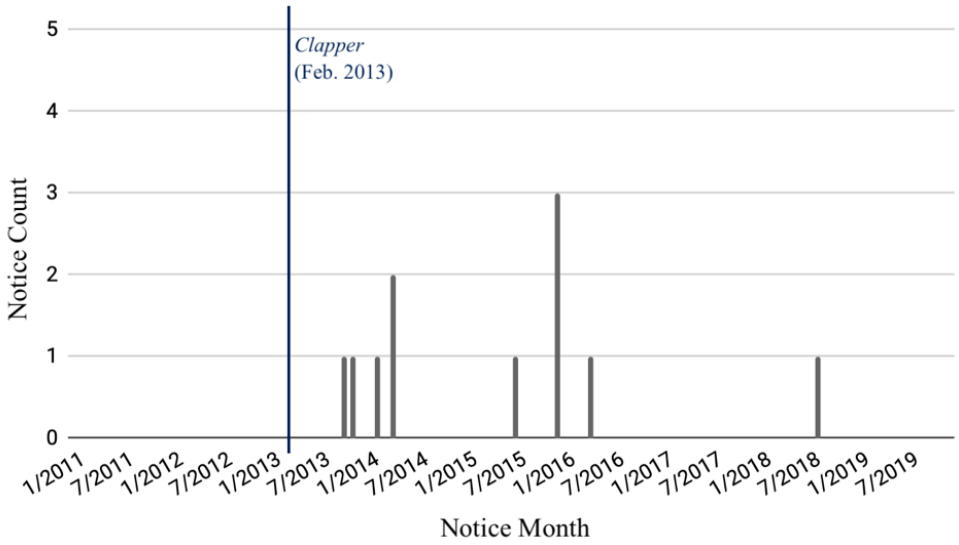

Figure 5: Dates of every FISA Section 702 notice

However, the number of notices that reference bulk surveillance is dramatically lower than the number of people surveilled under Section 702: only eleven notices compared to hundreds of thousands of people spied on. In 2013, the Solicitor General arguing *Clapper* repeatedly represented to the Supreme Court that defendants were receiving Section 702 notice as required.[60] After the Court relied on these representations to deny the plaintiffs standing,[61] it emerged that the DOJ had in fact never provided notice to *any* such defendants.[62] Six of the eleven Section 702 notices were

[58] Valerie Caproni, *Surveillance and Transparency*, 11 LEWIS & CLARK L. REV. 1087, 1088–89 (2007).

[59] *See* Smith v. Maryland, 442 U.S. 735, 745–46 (1979).

[60] Transcript of Oral Argument at 4–5, Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013); Brief for Petitioners at 8, *Clapper*, 568 U.S.

[61] *See Clapper*, 568 U.S. at 421.

[62] Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. TIMES (Oct. 16, 2013), www.nytimes.com/2013/10/17/us/politics/us-legal-shift-may-open-door-for-challenge-to-secret-wiretaps.html [https://perma.cc/EZ44-AHX2]; Patrick Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance–Again?*, JUST SEC. (Dec. 11, 2015), www.justsecurity.org/28256/arent-criminal-defendants-notice-section-

supplemental notices given after the *Clapper* controversy, even though four of those defendants had already been convicted.[63] Five notices were in new cases,[64] but there has not been a Section 702 notice since mid-2018. The government is likely avoiding giving Section 702 notice to protect methods from disclosure and avoid constitutional challenges, despite it being a major source of information.[65]

The next three Parts explore findings from the notice dataset in more depth, looking first at demographic trends in Part III, then at litigation challenges in Parts IV and V.

III. NATIONAL SECURITY THREATS IN FISA CASES

Civil liberties advocates have long warned of disproportionate targeting of Muslims by intelligence and law enforcement agencies, arguing that "the government has embraced a mentality that views individuals from a particular religious minority as akin to an existential threat."[66] This singular focus on Islamic extremism is problematic given research showing the increasingly deadly impact of domestic white supremacists,[67] as the government may be missing a larger domestic threat. In recent years, advocates have also raised similar concerns about disproportionate targeting of immigrants, particularly Chinese-Americans, based on often unfounded fears of economic and military espionage.[68] While these disparities have

---

702-surveillance-again [https://perma.cc/A75R-42FW].

[63] United States v. Zazi, No. 1:09-cr-00663 (E.D.N.Y. Sept. 23, 2009) (§ 1881(e) notice filed almost six years after initial notice); United States v. Mohamud, No. 3:10-cr-00475 (D. Or. Nov. 29, 2010) (almost three years later); United States v. Mihalik, No. 2:11-cr-00833-JLS (C.D. Cal. Aug. 30, 2011) (two and a half years later); United States v. Hasbajrami, No. 1:11-cr-00623 (E.D.N.Y. Sept. 8, 2011) (two and a half years later); United States v. Muhtorov, No. 1:12-cr-00033-JLK (D. Colo. Jan. 23, 2012) (almost two years later); United States v. Khan, No. 3:12-cr-00659 (D. Or. Dec. 28, 2012) (one year later).

[64] United States v. Mohammad, No. 3:15-cr-00358-JZ (N.D. Ohio Sept. 30, 2015); United States v. Al-Jayab, No. 1:16-cr-00181 (N.D. Ill. Mar. 17, 2016); United States v. Kandic, No. 1:17-cr-00449 (E.D.N.Y. Aug. 17, 2017).

[65] Conversation with former DOJ National Security Division employee (Nov. 21, 2019).

[66] SAID, *supra* note 36, at 148.

[67] *Confronting White Supremacy: Hearing Before the H. Subcomm. on Civil Rights and Civil Liberties*, 116th Cong. (2019) (statement of Michael C. McGarrity, Assistant Dir., FBI Counterterrorism Div., and Calvin A. Shivers, Deputy Assistant Dir.., FBI Criminal Investigative Div.) ("Individuals adhering to racially motivated violent extremism ideology have been responsible for the most lethal incidents among domestic terrorists in recent years.").

[68] *See, e.g.*, Apuzzo, *supra* note 1.

been posited for years, there has been little concrete evidence given the secrecy of surveillance decisions. The FISA notice dataset provides quantitative evidence that bolsters these theories and strengthens calls for reform.

This Article does not draw statistical inferences between notice recipients and the larger pool of FISA targets, but instead provides descriptive results about the notice group alone. Many of the observed patterns are troubling and may suggest bias or misplaced priorities. These trends demonstrate the need for the Executive Branch to increase transparency around surveillance decisions to reassure the public that the same biases are not present in FISA surveillance in general.

A. Concerns About Bias and Threat Prioritization in Surveillance Decisions

Advocates and academics have long expressed concerns that the government views Muslim- and Chinese-Americans in particular as security threats, and is conversely disinclined to view white, Christian Americans as threats. This bias leads to poor prioritization, as the intelligence community exaggerates the threat of non-majority groups and underinvests in addressing the threat of white supremacists. This racially tinged classification is magnified by the malleable interpretations of the "foreign power" and "international terrorism" definitions within FISA.[69]

There is broad consensus among advocates that FISA surveillance might disproportionately target Muslim-Americans. Muslims in the United States are the targets of significant government spending on community informants and surveillance, which "fuels the perception that the FBI views all American Muslims as inherently suspect."[70] As Amna Akbar has written about the NYPD's counterterrorism efforts, "[t]he immigrant Muslim neighborhood becomes a site of suspicion," with a particular focus on young Muslim men.[71] Advocates note the government's apparent view that Muslims are "uniquely susceptible to terrorist propaganda," demonstrated by significant government funding of deradicalization programs aimed at

---

[69] 50 U.S.C. § 1801(a), (c).

[70] *See* HUMAN RIGHTS WATCH, ILLUSION OF JUSTICE: HUMAN RIGHTS ABUSES IN US TERRORISM PROSECUTIONS 170 (2014); *see also* Amna Akbar, *Policing "Radicalization,"* 3 U.C. IRVINE L. REV. 809, 811 (2013) (discussing the rise of "programs focused on monitoring and influencing the political and religious cultures of Muslim communities").

[71] Akbar, *supra* note 70, at 836.

Islamic extremism.[72]

Analyzing the foundations of the modern intelligence community, Michael Glennon argues that the national security bureaucracy's "incentive structure encourages the exaggeration of existing threats and the creation of imaginary ones."[73] He explains that such threat inflation increases the power of the bureaucracy and decreases the risk of criticism for missing a future attack, as occurred after 9/11.[74] Since then, domestic counterterrorism efforts "have regularly singled out Muslims,"[75] even though studies show that American Muslims overwhelmingly "reject extremism."[76]

In addition, advocates have noted concerns about undue surveillance of the Chinese-American community. Andrew Kim's research found that more than half of defendants charged with economic espionage offenses were of Asian heritage, and that Asian defendants were twice as likely to be found innocent as defendants of other ethnicities.[77] He has further charted a recent rise in the timbre of "governmental rhetoric about the threat of Chinese spying."[78] Similarly, the *New York Times* reported on two high-profile espionage cases that were ultimately dismissed, noting that they "raise[] questions about whether the Justice Department, in its rush to find Chinese spies, is ensnaring innocent American citizens of Chinese ancestry."[79] Alarmed at these patterns, the U.S. Commission on Civil Rights expressed concerns to the DOJ Inspector General in 2016 about baseless prosecutions of Chinese-Americans.[80]

---

[72] *See* HUMAN RIGHTS WATCH, *supra* note 70, at 18; Akbar, *supra* note 70, at 811.

[73] Michael J. Glennon, *National Security and Double Government*, 5 HARV. NAT'L SEC. J. 1, 26 (2014).

[74] *Id.* at 27–28.

[75] Caroline Mala Corbin, *Terrorists Are Always Muslim but Never White: At the Intersection of Critical Race Theory and Propaganda*, 86 FORDHAM L. REV. 455, 460 (2017).

[76] Richard Wike & Greg Smith, *Little Support for Terrorism Among Muslim Americans*, PEW RSCH. CTR. (Dec. 17, 2009), www.pewforum.org/Politics-and-Elections/Little-Support-for-Terrorism-Among-Muslim-Americans.aspx [https://perma.cc/L9VX-6WA2].

[77] Andrew C. Kim, *Prosecuting Chinese "Spies": An Empirical Analysis of the Economic Espionage Act*, 40 CARDOZO L. REV. 749, 753 (2018).

[78] *Id.* at 751.

[79] Apuzzo, *supra* note 1.

[80] Letter from U.S. Comm'n on Civil Rights to Michael E. Horowitz, Inspector Gen., U.S. Dep't of Just. (July 15, 2016), jeremy-wu.info/wp-content/uploads/2016/07/PR_LetterChineseAmericanProsecutions.pdf [https://perma.cc/NX93-YDP6].

The flipside of these biases is the government's general reluctance to view white supremacists as a serious national security threat.[81] Despite the significant growth in intelligence funding after September 11th, counterterrorism measures are not applied to white supremacists, and budgets for investigating white nationalist militias were slashed after public pressure from conservative groups.[82] In contrast to Muslim-Americans, white supremacists receive less governmental scrutiny[83] and "are charged as terrorists exceedingly rarely."[84] Advocates argue that "[s]omething structural needs to urgently change in the national security bureaucracy to deal with right-wing violence."[85]

This skewed threat assessment is likely mirrored in FISA targets. Scholars do not know how surveillance targets break down by ideology, but posit that white supremacists with global connections are unlikely to be monitored under FISA given the government's current interpretation of the statute.[86] FISA surveillance requires probable cause that a person is a "foreign power" or an "agent of a foreign power."[87] The definition of "foreign power" includes groups engaged in "international terrorism," which includes acts that "transcend national boundaries in terms of the means by which they are accomplished [or] the persons they appear intended to coerce or intimidate."[88] As Shirin Sinnar explains, the statutory distinction between "domestic" and "international" terrorism does "not coincide with the common understanding of 'domestic' terrorism as occurring within the United States and 'international' terrorism as

---

[81] *See generally* Corbin, *supra* note 75 (outlining several narratives in American society that prevent white Christian extremists from being considered "terrorists").

[82] *See* R. Jeffrey Smith, *Homeland Security Department Curtails Home-Grown Terror Analysis*, WASH. POST (June 7, 2011), www.washingtonpost.com/politics/homeland-security-department-curtails-home-grown-terror-analysis/2011/06/02/AGQEaDLH_story.html [https://perma.cc/B76T-HBAJ]; Jesse J. Norris, *Why Dylann Roof Is a Terrorist Under Federal Law, and Why It Matters*, 54 HARV. J. ON LEGIS. 259, 270–71 (2017).

[83] *See* Shirin Sinnar, *Separate and Unequal: The Law of Domestic and International Terrorism*, 117 MICH. L. REV. 1333, 1336 (2019).

[84] Francesca Laguardia, *Considering a Domestic Terrorism Statute and Its Alternatives*, 114 NW. U. L. REV. 1061, 1065 (2020).

[85] Joel Rubin, *Washington Must Treat White Supremacist Terrorism as a Transnational Threat*, FOREIGN POL'Y (Jan. 18, 2021), foreignpolicy.com/2021/01/18/washington-must-treat-white-supremacist-terrorism-as-a-transnational-threat/ [https://perma.cc/VHT3-NMDD].

[86] *See, e.g.*, Sinnar, *supra* note 83, at 1346–47.

[87] *See* 50 U.S.C. § 1805.

[88] *Id.* § 1801(c)(3).

committed abroad."[89] Instead, what often matters is whether the government categorizes the ideology or related group as "domestic" or "international." The definitions of "foreign power" and "international terrorism" are nebulous and have been interpreted to extend to situations where there is no actual contact with any foreign person or group.[90]

Many academics have expressed concerns about the expansive and selectively applied interpretation of the foreign nexus requirement,[91] in large part because it risks missing some internationally supported domestic threats. The Southern Poverty Law Center notes that "the white power movement in this country has sought and maintained international connections with fellow travelers for decades."[92] A recent *New York Times* analysis found that many domestic attackers were inspired by or communicated with foreign extremists, and that "the internet and social media have facilitated the spread of white extremist ideology and violence."[93] In particular, there are growing links between foreign and American neo-Nazi groups,[94] and far-right Russian paramilitaries have cultivated ties to domestic white nationalists, including providing tactical training and support.[95]

Sinnar argues that the government ignores these international links and "often views white supremacists and neo-Nazis as domestic terrorists despite the movements' global dimensions."[96] As just one example, a white

---

[89] Sinnar, *supra* note 83, at 1337.
[90] *Id.*
[91] *See id.* at 1346–47.
[92] *Atomwaffen Division*, S. POVERTY L. CTR., www.splcenter.org/fighting-hate/extremist-files/group/atomwaffen-division [https://perma.cc/H5SH-DKUN].
[93] Weiyi Cai & Simone Landon, *Attacks by White Extremists Are Growing. So Are Their Connections.*, N.Y. TIMES (Apr. 3, 2019), www.nytimes.com/interactive/2019/04/03/world/white-extremist-terrorism-christchurch.html [https://perma.cc/3A24-AM58?type=image] (documenting global connections among white extremists).
[94] *See, e.g.*, TIM LISTER, COMBATING TERRORISM CTR. SENTINEL, THE NEXUS BETWEEN FAR-RIGHT EXTREMISTS IN THE UNITED STATES AND UKRAINE 30 (2020), https://ctc.usma.edu/the-nexus-between-far-right-extremists-in-the-united-states-and-ukraine/ [https://perma.cc/5K7H-TY89] (exploring how "Neo-Nazi and white supremacist groups in the United States and Europe have . . . establish[ed] closer transnational contacts" over the past decade).
[95] Elizabeth Grimm Arsenault & Joseph Stabile, *Confronting Russia's Role in Transnational White Supremacist Extremism*, JUST SEC. (Feb. 6, 2020), www.justsecurity.org/68420/confronting-russias-role-in-transnational-white-supremacist-extremism [https://perma.cc/5QA9-YYWV].
[96] Sinnar, *supra* note 83, at 1337.

supremacist group was not added to the U.S. government's list of sanctioned Specially Designated Global Terrorists until 2020.[97] Under FISA's malleable definition of "international," an American-born Muslim teenager in Minneapolis who has never left the country, but is encouraged to support ISIS by an FBI plant with no actual connection to the group, would likely be considered tied to "international terrorism" and qualify for FISA surveillance. But a white teenager in Charlottesville who is encouraged by Russian white nationalists online to plot a domestic attack is unlikely to fall within FISA's current ambit.

This artificial divide indicates that the government may be under-examining a serious threat to domestic security. While it is difficult to estimate threats precisely,[98] in the fifteen years after 9/11 the Government Accountability Office counted substantially more fatal domestic attacks by white extremists than by Islamic extremists, with a comparable total number of fatalities.[99]

If domestic extremists with similar levels of international connections are treated differently depending on their ideology, it "both undermine[s] the federal government's ability to confront a steadily increasing domestic threat and create[s] inequality in the treatment of terror suspects based on race and religion."[100] This inequity is particularly stark with respect to the procedural imbalances in court between FISA and Wiretap Act evidence discussed in Part IV, placing Muslim-Americans at a disadvantage in court compared with white Christian Americans who are charged with similar criminal conduct.

This Article, as the first exhaustive collection of FISA use in court, sheds light on how FISA is implemented in practice and helps demonstrate that these concerns are warranted.

---

[97] Office of Foreign Assets Control, *Counter Terrorism Designations*, DEP'T OF TREASURY (Apr. 6, 2020), https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions [https://perma.cc/M6MF-LJVG] (adding the Russian Imperial Movement and its leaders to the sanctions list).

[98] Sinnar, *supra* note 83, at 1387–88.

[99] *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-17-300, COUNTERING VIOLENT EXTREMISM: ACTIONS NEEDED TO DEFINE STRATEGY AND ASSESS PROGRESS OF FEDERAL EFFORTS 28–34 (2017).

[100] Laguardia, *supra* note 84, at 1076. *See also* Norris, *supra* note 82, at 283–92 (2017) (exploring the social and policy consequences of the divide).

B. Trends in FISA Notice Cases

1. Demographics

Muslims are significantly overrepresented in the pool of people who received notice. I was able to confirm the religion of 72% of the recipients; of those with known religion, 93% were Muslim and only 5% were Christian. These numbers are skewed since indictments involving Islamic extremism necessarily recite facts relating to the defendant's religious views. Nevertheless, even if we assume that every notice recipient whose religion I could not confirm was not Muslim, Muslims would still make up 67% of the pool, dramatically larger than their proportion of 1.1% of the U.S. population.[101]

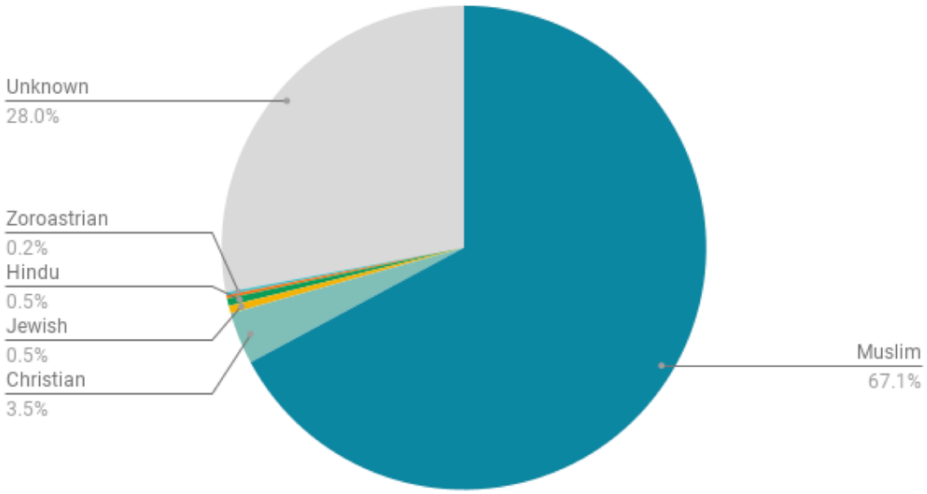

Figure 6: Religion of individuals receiving FISA notice

The notice cases with allegations of links to terrorism focus almost exclusively on Islamic extremism. Almost all purportedly terrorism-linked defendants (96%, or 227 defendants) had alleged ties to Islamic extremist groups. In comparison, there were seven defendants linked to Irish republicanism in the 1990s and one tied to Sikh extremism. There were no cases involving ties to white supremacist groups.

---

[101] Besheer Mohamed, *New Estimates Show U.S. Muslim Population Continues to Grow*, PEW RSCH. CTR. (Jan. 3, 2018), www.pewresearch.org/fact-tank/2018/01/03/new-estimates-show-u-s-muslim-population-continues-to-grow [https://perma.cc/JNU2-GDE8].

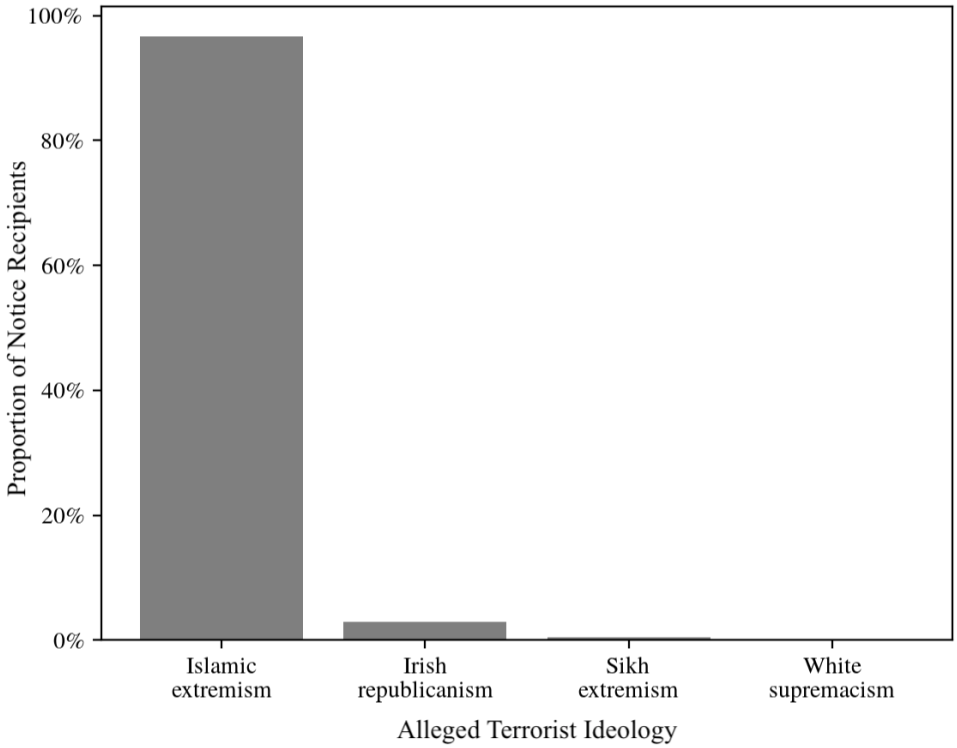

Figure 7: Notice recipients' alleged terrorism-related ideology

The prevalence of Islamic extremism allegations among notice recipients would logically follow if white supremacy were under-investigated in FISA surveillance in general. If domestic white supremacy is not classified as "international" terrorism within the Executive Branch, and is not seen to have any international nexus, it will be investigated using non-FISA methods of surveillance such as monitoring under the Wiretap Act. We would then expect to see very little FISA usage, which would likely translate into few or no notices for charges related to white supremacy.

People from several national origins were also over-represented among those receiving notice. Almost 10% of notice recipients held Chinese citizenship, of whom just over half were dual U.S. citizens. Most of these were espionage cases relating to China, but many resulted in dismissals or acquittals of the headline-grabbing national security charges. For example, Dr. Jianyu Huang, a naturalized U.S. citizen from China, was charged in 2012 with stealing $25,000 of federal property from Sandia National Laboratories and conveying it to various Chinese research

centers.[102] However, the only charges he was convicted of related to bringing his government-issued laptop abroad without permission to show a slideshow at a symposium.[103] Somali-Americans were similarly overrepresented, making up almost 5% of the notice pool. In an unusually overt acknowledgement of bias, the officer detaining Abdiaziz Hussein told him that he was being arrested "to serve as an example to the community."[104] These results are likely undercounts of notice recipients of various backgrounds, since I was able to capture only citizenship objectively, as opposed to the ancestry of native-born defendants.

Relatedly, immigrants outnumbered native-born Americans, accounting for 69% of individuals receiving notice whose immigration status I could ascertain. When their cases were filed, 19% of recipients were legal permanent residents (Green Card holders); 29% percent were naturalized U.S. citizens; and 13% were residents without permanent legal status, including undocumented residents and those on temporary visas. Only 29% were native-born U.S. citizens.

---

[102] Redacted Indictment, United States v. Huang, No. 1:12-cr-01246 (D.N.M. May 23, 2012), ECF No. 2.

[103] Press Release, Dep't of Just., Former Sandia Corporation Scientist Sentenced for Taking Government Property to China (Nov. 24, 2014), www.justice.gov/usao-nm/pr/former-sandia-corporation-scientist-sentenced-taking-government-property-china [https://perma.cc/A3ZC-AQNH].

[104] Motion to Dismiss Based on Outrageous Government Conduct, Selective Prosecution, Vindictive Prosecution and Request Court to Use Its Supervisory Function to Dismiss Stale Charges at 4–5, United States v. Hussein, No. 3:13-cr-01514 (S.D. Cal. Jan. 24, 2014), ECF No. 40-1.

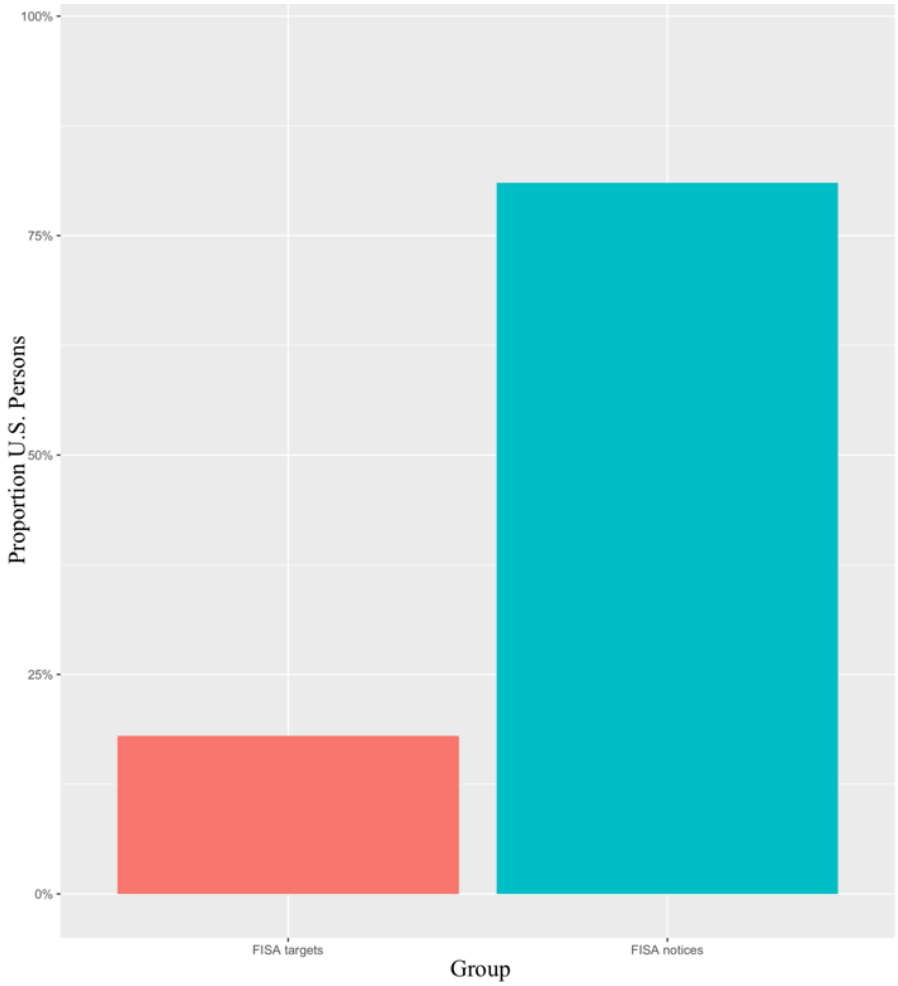

Figure 8: Proportion of U.S. persons among FISA targets[105] *and notice recipients*

FISA requires a slightly higher standard of evidence to surveil "U.S. persons,"[106] meaning American citizens, Green Card holders, substantially-American unincorporated associations, and corporations incorporated in the United States.[107] Because of this, it is easier to surveil foreigners and non-permanent residents, which is borne out in government data showing a large majority of targets are non-U.S. persons.[108] That ratio is flipped among notice recipients: 81% of recipients were U.S. persons, and 60% were American citizens. This difference is likely because U.S. persons can be prosecuted in the United States relatively easily, while foreign citizens are

[105] DIR. OF NAT'L INTELLIGENCE, 2019 TRANSPARENCY REPORT, *supra* note 37, at 10, 26.
[106] 50 U.S.C. § 1801(e)(1), (2).
[107] *See id.* § 1801(i).
[108] DIR. OF NAT'L INTELLIGENCE, 2019 TRANSPARENCY REPORT, *supra* note 37, at 10, 26.

often surveilled without any intent to prosecute or otherwise pose difficulties extraditing for prosecution.

2. Alleged National Security Threats

While the Executive Branch is authorized to use FISA only to obtain "foreign intelligence information,"[109] a concerning number of these notice cases had no alleged link to national security or involved solely allegations of economic harm to American companies. FISA defines "foreign intelligence information" in five categories. The first three categories are fairly common sense forms of intelligence: the information can relate to (1) "hostile acts" by a foreign power; (2) "sabotage, international terrorism, or proliferation of weapons of mass destruction by a foreign power"; or (3) "clandestine intelligence activities" by a foreign power.[110] The final two categories are catch-alls: they include anything related to (4) the national defense or national security; or (5) foreign affairs.[111] I classified the alleged national security threat for each notice recipient based on these allowable purposes: terrorism and military/intelligence espionage fell into the first set of categories, while economic espionage and sanctions violations fell into the catch-all buckets. I categorized based on what the complaint or DOJ press releases alleged, even if it had no relation to the charges filed.

[109] 50 U.S.C. § 1804(a)(6)(A)–(E).
[110] *Id.* § 1801(e)(1).
[111] *See id.* § 1801(e)(2).

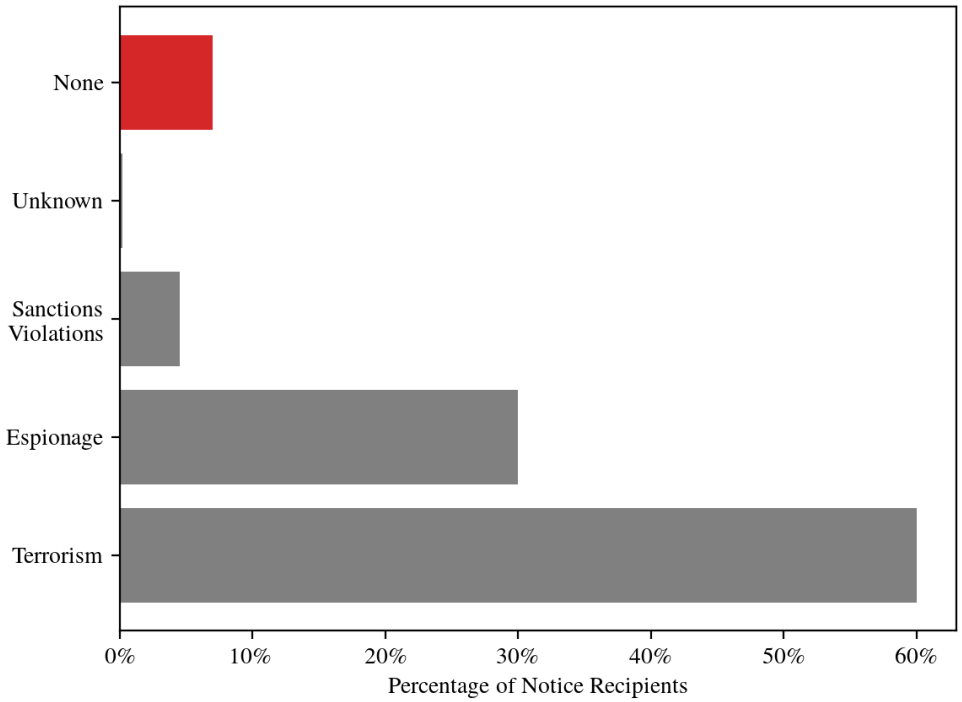

Figure 9: Alleged national security threat of notice recipients

Strikingly, 7% of people who received notice had no national security threat alleged. Most of these cases appear to be the result of FBI investigations that turned up no evidence of national security threats. For example, the government obtained FISA warrants to monitor Amar Tharee, an auto repair shop owner in Texas.[112] Despite the involvement of a local Joint Terrorism Task Force, he was not charged with any violent or terrorism offenses, and the prosecution made no allegations of ties to terrorism or other national security threats in charging documents or court filings.[113] Mr. Tharee was ultimately convicted only of conspiring to distribute anabolic steroids.[114] In California, the FBI surveilled Keith Gartenlaub, a white Boeing engineer married to a Chinese-American woman, for twenty-one months based on suspicions that he might be sharing trade secrets with China. After finding nothing to support their

[112] Notice of Intent to Use Foreign Intelligence Surveillance Act Information, United States v. Tharee, No. 5:13-cr-00367 (W.D. Tex. May 24, 2013), ECF No. 41.

[113] Complaint, United States v. Tharee, No. 5:13-cr-00367 (W.D. Tex. Apr. 23, 2013), ECF No. 1; Guillermo Contreras, *FBI Arrests Men in Anabolic Steroids Case*, HOUSTON CHRON. (Apr. 26, 2013), www.chron.com/default/article/FBI-arrests-men-in-anabolic-steroids-case-4467573.php [https://perma.cc/ETF5-P9UM].

[114] Judgment and Commitment, United States v. Tharee, No. 5:13-cr-00367 (W.D. Tex. Aug. 5, 2013), ECF No. 58.

hunch, they charged him with possession of child pornography due to a single photo found on his computer—which forensic examination showed had never been opened.[115] Mr. Gartenlaub alleged that federal prosecutors promised to dismiss the case if he would provide information about Chinese espionage, a subject about which he had no knowledge.[116] Defendants in these situations face the many procedural barriers that FISA evidence brings, making their cases substantially more difficult than defendants charged with the same offenses but surveilled through non-FISA means. As Patrick Toomey at the ACLU National Security Project explained, "broad searches for foreign intelligence information flip the Fourth Amendment on its head when the government repurposes those searches for domestic criminal prosecutions."[117]

In addition, almost 14% of notice recipients allegedly linked to Islamic extremism had no specific terrorist group mentioned anywhere in the case or in government press releases. If these defendants are truly "lone wolf" domestic extremists radicalized at home, the government's use of FISA against them may suggest an ill-defined view of the "international" nexus needed to fall within FISA's definition of "agent of a foreign power" as discussed above.

Espionage cases are divided between allegations of sharing general government secrets, military intelligence, or military technology, and stealing economic secrets from American companies. Unsurprisingly, China and Russia were linked to almost 70% of alleged espionage defendants. Interestingly, the number of Russia-related FISA defendants is dramatically higher than Andrew Kim found in his analysis of a random dataset of Economic Espionage Act cases.[118] In addition, a significant number (10%) of notice recipients were allegedly linked to Cuban espionage activities, all of whom were prosecuted before the thaw in diplomatic relations under the Obama administration.

The high proportion of economic espionage cases is somewhat

---

[115] Jeff Stein, *How a Chinese Spy Case Turned into One Man's Child Porn Nightmare*, NEWSWEEK (May 24, 2016), www.newsweek.com/2016/06/03/fbi-keith-gartenlaub-chinese-spy-porn-462830.html[https://perma.cc/UR9X-9D45].

[116] *Id*.

[117] Eric Tucker, *How National Security Surveillance Nabs More Than Spies*, ASSOCIATED PRESS (Mar. 15, 2020), apnews.com/d9ac884cc10a21fcaf387ddc4f61104c [https://perma.cc/S5JN-8KQA].

[118] *See* Kim, *supra* note 77, at 781 (Russia not listed among countries making up 93% of EEA cases).

concerning because commercial trade secret theft is qualitatively different from the other types of foreign intelligence information, as it is only connected to national security through its impact on the economy. Extending "national security" and "foreign intelligence information" that far gives a troubling amount of discretion to the Executive Branch and may increase the risk of racial and ethnic profiling.[119]

3. Tenuous Terrorism Charges

The notice cases reinforce the hypothesis that many alleged terrorist threats are exaggerated or based on weak evidence. On top of the almost 10% of recipients who had no national security threat alleged, when notice recipients were charged with terrorism offenses, those charges were rejected by judges and juries and dismissed by the government much more frequently than is usual in federal prosecutions. These findings imply that the DOJ may be overbroad in its allegations of terrorism and its terrorism charging decisions.

Even in those cases in which the prosecution claimed that defendants were tied to terrorist groups, government disclosures show that over 10% of post-9/11 defendants are not *currently* considered within the DOJ to be linked to terrorism.[120] For example, the government alleged that Sabri Benkahla was linked to the Pakistani extremist group Lashkar-e-Taiba, and Mr. Benkahla appears in the DOJ's foreign terrorism-related conviction list, but U.S. District Court Judge James Cacheris (himself a former FISC judge[121]) refused the government's request for a terrorism sentencing enhancement and declared that "Sabri Benkahla is not a terrorist."[122] Given FISA's power as an evidence-gathering tool, it is concerning that the government did not appear to have sufficient evidence

---

[119] *Cf.* Brief in Support of Motion for Disclosure of FISA Applications, Orders, and Related Materials at 14, United States v. Shaoming, No. 4:13-cr-00147-SMR-CFB (S.D. Iowa Mar. 13, 2015), ECF No. 225-1 ("The information that the FISA surveillance sought to obtain—concerning the alleged theft of trade secrets relating to corn germplasm from one company by another—has nothing to do with 'foreign intelligence.'").

[120] *See* NAT'L SEC. DIV., *supra* note 48.

[121] *Foreign Intelligence Surveillance Court & Foreign Intelligence Surveillance Court of Review, Current and Past Members*, U.S. COURTS (June 2021), www.fisc.uscourts.gov/sites/default/files/FISC%20FISCR%20Judges%20June%202021.pdf.

[122] United States v. Benkahla, 501 F. Supp. 2d 748, 759 (E.D. Va. 2007). Mr. Benkahla had previously been acquitted of terrorism charges. Judgment of Acquittal, United States v. Royer, No. 1:03-cr-00296 (E.D. Va. Mar. 9, 2004), ECF No. 481.

to demonstrate a link to terrorism in such a high proportion of alleged terrorism cases.

Even when terrorism charges were filed in FISA notice cases, those charges were frequently weak. A significant percentage of defendants were acquitted or had charges dismissed, including several where the court stepped in to acquit after a guilty jury verdict. Of the 158 defendants charged with material support of terrorism charges under 18 U.S.C. § 2339A and § 2339B, 13% had those charges dismissed and 5% were acquitted of all material support charges. In comparison, only 8% of all federal criminal cases were dismissed and under half a percent were acquitted in 2018.[123]

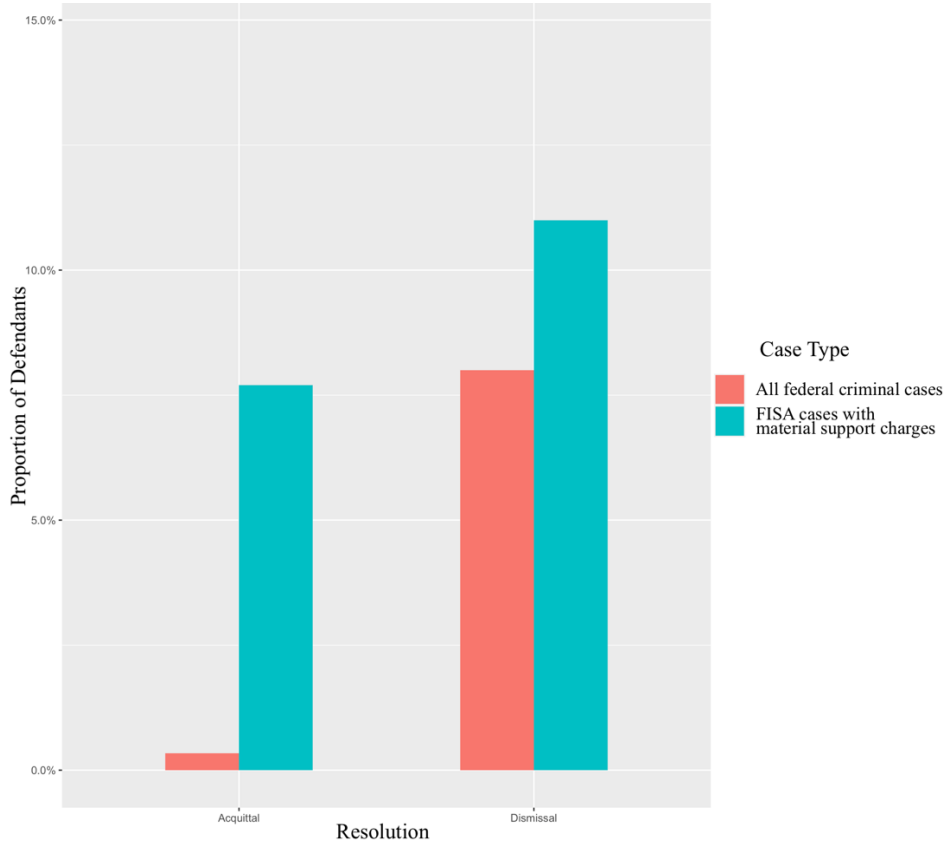

Figure 10: Non-conviction case outcome comparisons

[123] John Gramlich, *Only 2% of Federal Criminal Defendants Go to Trial, and Most Who Do Are Found Guilty*, PEW RSCH. CTR. (June 11, 2019), www.pewresearch.org/fact-tank/2019/06/11/only-2-of-federal-criminal-defendants-go-to-trial-and-most-who-do-are-found-guilty/ [https://perma.cc/V4SS-XWLL].

The dismissals of these weak cases have led to concerns about hasty prosecutions based on minimal or incorrect evidence. For example, as discussed in the Introduction, in 2015 the FBI arrested Professor Xi Xiaoxing, a naturalized American citizen who was the chair of the Temple University Physics Department.[124] He was charged with sending secret equipment plans to Chinese scientists.[125] Once the DOJ shared the schematics with the defense several months later, it became clear that the drawings Professor Xi had sent were of a different unrestricted device and that the DOJ had misunderstood the technology, prompting prosecutors to drop the case.[126]

Notably, courts rebuked the government for the weakness of its evidence in several acquittals. In 2009, a judge overturned a jury conviction of material support of terrorists for Hassan Abu-Jihaad, a former Navy sailor alleged to have disclosed classified information about battle group movements.[127] In a 68-page opinion, the judge found that the government's "theory of guilt puts a strain on the language of the statute" and explained "the Court does not believe that a rational juror could conclude beyond a reasonable doubt that Mr. Abu-Jihaad provided material support [] in the form of a physical asset."[128] In 2013, Izhar Khan, a 24-year-old whose father was convicted of supporting the Pakistani Taliban, was acquitted by a judge who declared, "This Court will not allow the sins of the father to be visited upon the son."[129]

Defendants themselves also seem to view these charges as weak. Individuals who received a FISA notice were twenty times more likely to go to trial than defendants in all federal criminal cases.[130] This might be a sign that defendants feel the cases against them are fragile and worth fighting at trial; it might also be an acknowledgement that the terrorism sentencing enhancement is the harshest of the upward adjustments in the

---

[124] *See supra* text accompanying notes 1–7.
[125] *See* Indictment, United States v. Xi, No. 2:15-cr-00204 (E.D. Pa. May 14, 2015), ECF No. 1.
[126] Government's Unopposed Motion to Dismiss, *Xi* (E.D. Pa. Sept. 11, 2015), ECF No. 29.
[127] *See* Complaint Affidavit, United States v. Abu-Jihaad, No. 3:07-cr-00057 (D. Conn. Mar. 7, 2007), ECF No. 1-2.
[128] United States v. Abu-Jihaad, 600 F. Supp. 2d 362, 394, 401 (D. Conn. 2009).
[129] Order on Defendant Izhar Khan's *Ore Tenus* Motion for Judgment of Acquittal at 1, United States v. Khan, No. 1:11-cr-20331 (S.D. Fla. Jan. 17, 2013), ECF No. 690.
[130] Gramlich, *supra* note 123 (calculating litigation statistics for all federal criminal defendants).

federal Sentencing Guidelines,[131] or that DOJ may not make tempting plea offers in terrorism cases, so a defendant might not have much to lose by taking a chance at trial.

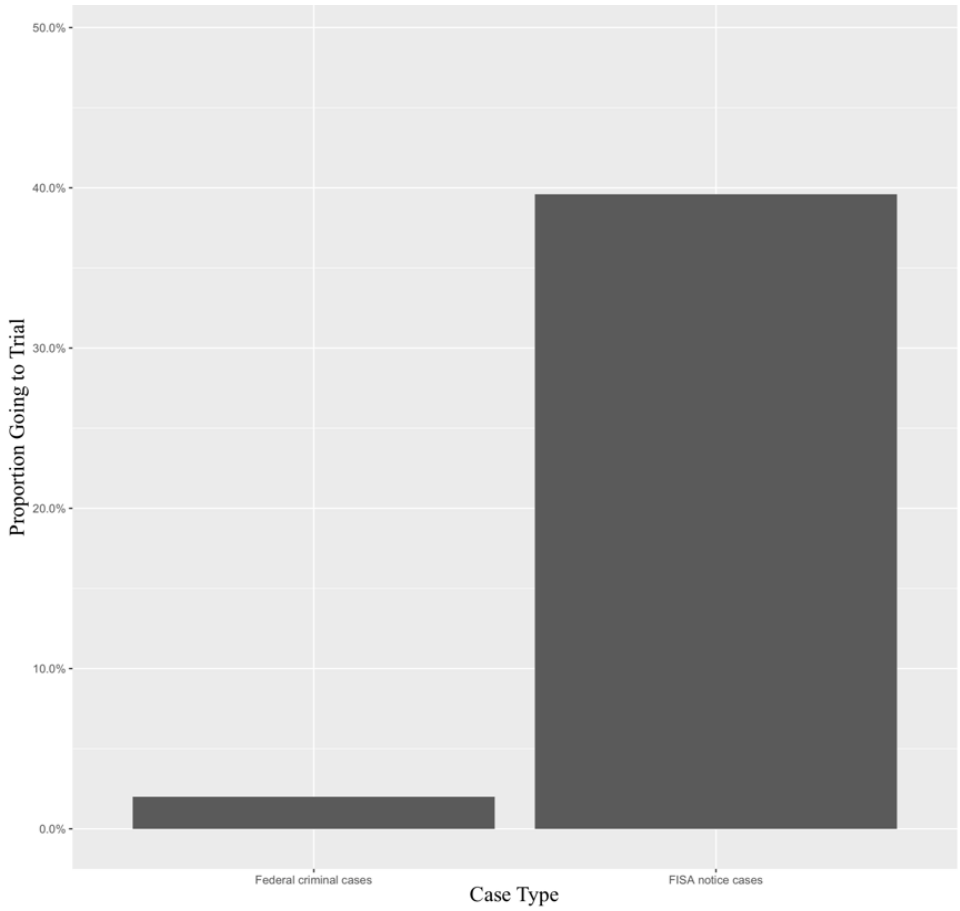

Figure 11: Trial proportion comparison

Finally, even those convicted of terrorism charges may have negligible connections to terrorist groups and present minimal danger to the public. At Mohamed Warsame's sentencing after pleading guilty to conspiring to provide material support to a foreign terrorist organization, the judge noted, "I have found no evidence whatsoever that you were involved in a specific terrorist plot against the United States . . . . To me you don't

[131] *See* U.S. SENT'G GUIDELINES MANUAL § 3A1.4 (U.S. SENT'G COMM'N 2018); HUMAN RIGHTS WATCH, *supra* note 70, at 124 n.558 ("Though some specific offenses also involve upward adjustments, none exceeds the severity of the terrorism enhancement since it increases both the offense level increase and criminal history category assignment.").

seem capable of committing terrorist acts."[132]

C. Implications of Results for FISA Reform

While the notice recipient results do not prove that the same trends are true among all FISA surveillance targets, they are sufficiently troubling to support calls for increased transparency, oversight, and reform of FISA surveillance in general.

The demographic disparities among these individuals are concerning and would be worrying if they were paralleled in the broader FISA numbers. To be clear, these patterns do not prove that FISA surveillance writ large disproportionately targets Muslims, Chinese-Americans, or immigrants. However, the differences in representation among notice recipients raise questions about whether biases about particular groups, or fears of Islamic terrorism and economic espionage, have led to a "self-fulfilling prophecy" with respect to investigation and prosecution.[133] Studies have found that almost half of terrorism convictions arose from plots created or assisted by informants in sting operations,[134] further demonstrating that such investigations may not be uncovering true threats.

The fact that immigrants make up the majority of the notice pool suggests that the government might be using foreign birth or dual citizenship as a proxy for the foreign ties required for FISA surveillance.[135] It is difficult to imagine why people holding specific other citizenships (such as Chinese or Somali) would be significantly differently represented in the pool of people prosecuted using FISA evidence. In addition, the United States has no extradition treaty with China,[136] making it even more striking that many Chinese nationals without American citizenship—many

---

[132] Sentencing Hearing Transcript at 37, United States v. Warsame, No. 0:04-cr-00029 (D. Minn. Aug. 10, 2009), ECF No. 179.

[133] Kim, *supra* note 77, at 796 (quoting David A. Harris, *The Stories, the Statistics, and the Law: Why "Driving While Black" Matters*, 84 MINN. L. REV. 265, 297 (1999)).

[134] HUMAN RIGHTS WATCH, *supra* note 70, at 21.

[135] *See* William Pollak, Note, *Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J. L. REFORM 221, 222 (2008) ("Muslim Americans and recent immigrants . . . could easily be characterized as agents of foreign powers simply because they continue to associate with their native countries.").

[136] Jonathan Masters, *Extradition Backgrounder*, COUNCIL ON FOREIGN REL., www.cfr.org/backgrounder/what-extradition [https://perma.cc/NDX5-NVEV] (last updated Jan. 8, 2020).

of whom remain fugitives in China—appear in the notice dataset. Given how few people monitored under FISA are ever prosecuted (and therefore notified of surveillance), it is surprising that the government chooses to prosecute so many effectively litigation-proof foreigners.

The use of FISA to investigate Islamic extremism but not white supremacist groups has led many advocates to suggest legislative reform, such as increasing the FISC's level of scrutiny to require a substantial connection to an international group before authorizing surveillance, and requiring the FISC to publish opinions interpreting the "agent of a foreign power" requirement.[137] In addition, Congress could require reporting on domestic and international terrorism threats to ensure enforcement resources match risk levels. To remedy this perceived imbalance, scholars have suggested either "ratcheting up" treatment of globally connected white supremacists[138] or "ratcheting down" treatment of solely domestic Islamic extremists.[139] More generally, Congress could consider removing the "legal binary" between domestic and international terrorism laws to promote more equal treatment.[140]

Next, while the proportion of notice recipients without any alleged terrorism or espionage link is substantial, it does not erase the possibility that FISA is generally used to surveil people the government views as terrorism- or espionage-related. If FISA were used within its intended scope, the government might not choose to prosecute most suspects, instead focusing on other tactics. In that case, the government might prosecute mainly for incidentally overheard crimes that were not terrorism-related, or might use incidental charges as a way to pressure the main target. However, the relatively frequent non-conviction outcomes of the notice cases bolster the concern that FISA surveillance may be overbroad with respect to the strength of the perceived national security threat.

In addition, the findings are consistent with advocates' concerns that a significant proportion of claimed counterterrorism "wins" involve plots manufactured or aided by the government. Given the procedural

---

[137] Sinnar, *supra* note 83, at 1403.
[138] *E.g.*, Mary B. McCord & Jason M. Blazakis, *A Road Map for Congress to Address Domestic Terrorism*,
LAWFARE (Feb. 27, 2019), www.lawfareblog.com/road-map-congress-address-domestic-terrorism [https://perma.cc/XC55-JLGG].
[139] *E.g.*, Sinnar, *supra* note 83, at 1402–04.
[140] *Id.* at 1398.

disadvantages faced by defendants in FISA cases, it is particularly worrying that so many of the notice cases involve fairly weak evidence of national security risks.

Beyond demographic and ideological disparities, procedural hurdles during litigation strip FISA defendants of the ability to fight their prosecutions and vindicate their constitutional rights. The next two Parts explore these difficulties and how they function to limit oversight of this broad surveillance statute.

IV. LITIGATING AGAINST FISA EVIDENCE

Congress intended that people spied on by the government would be able to see the evidence against them and challenge illegal surveillance.[141] But federal courts have interpreted FISA so narrowly that no one has ever been allowed to see the FISA warrant that led to their prosecution, and the government exploits its classification power to avoid releasing evidence critical to people's defense.[142]

A. Litigating FISA in Theory

Congress created a disclosure mechanism within FISA for defendants to challenge surveillance through the adversary process. If "the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security," judges first examine the warrant application and how the surveillance was conducted *in camera* without defense participation.[143] However, the Senate Judiciary and Intelligence Committees explained that if the materials include "indications of possible misrepresentation of fact, vague identification of the persons to be surveilled or surveillance records which include[] a significant amount of nonforeign intelligence information," the court should disclose the materials to the defense to help determine whether the surveillance was legal.[144] The law frames this process as the judge deciding whether "such disclosure is necessary to make an accurate determination of the legality of the surveillance."[145]

---

[141] *See infra* Subpart A.
[142] *See infra* Subpart B.
[143] 50 U.S.C. § 1806(f).
[144] S. REP. NO. 95-604, pt. I, at 58 (1977); S. REP. NO. 95-701, at 64 (1978).
[145] 50 U.S.C. § 1806(f).

Congress expected this "necessary" determination to result in regular defense access to FISA materials: it noted that in the kinds of "more complex" situations noted above, "the court will likely decide to order disclosure to the defendant."[146] The House Intelligence Committee further explained that when the government uses evidence "obtained or derived from an electronic surveillance," "simple justice dictates that the defendant not be denied the use of our traditional means for reaching the truth—the adversary process."[147] As a final backstop, the court must consider whether "due process requires discovery or disclosure."[148]

In addition to this statutory disclosure provision, defendants have the judge-made *Franks* hearing as another avenue to see FISA warrants. A *Franks* hearing allows the defense to present evidence that a warrant was based on recklessly false or omitted information that undercuts probable cause, which would render the warrant invalid.[149]

Once discovery begins, the government and defendants' interests are balanced by the Classified Information Procedures Act ("CIPA"), a statute controlling the use of classified evidence in criminal proceedings.[150] Critically, Congress explained that a defendant "should not stand in a worse position, because of the fact that classified information is involved, than he would without" CIPA.[151]

B. FISA Litigation in Practice

Despite Congress's intent that spying victims be able to use the adversary process to vindicate their rights, in reality, defendants have no ability to see or challenge FISA warrants and have limited access to classified evidence.

1. Courts have so narrowly construed FISA's disclosure mechanism and the *Franks* standard that no defendant has ever seen their FISA warrant or affidavit.

---

[146] S. REP. NO. 95-604(I), at 58; S. REP. NO. 95-701, at 64.
[147] H.R. REP. NO. 95-1283, pt. I, at 92 (1978).
[148] 50 U.S.C. § 1806(g).
[149] 1 CHARLES ALAN WRIGHT & ARTHUR R. MILLER, FEDERAL PRACTICE AND PROCEDURE § 42 (4th ed. 2008) (citing Franks v. Delaware, 438 U.S. 154 (1978)).
[150] Classified Information Procedures Act, Pub L. No. 96-456, 94 Stat. 2025 (1980) (codified as amended at 18 U.S.C. app. §§ 1–16).
[151] S. REP. NO. 96-823, at 9 (1980).

Imagine if the government obtained a FISA warrant by telling a FISC judge the following facts: a Muslim teenager, Sadiq, ran away from a family vacation to Egypt, got a plane ticket to Syria to join an older Muslim man, and is now believed to have joined ISIS. A district court judge looking at that warrant affidavit would likely determine it shows probable cause that Sadiq qualified as an agent of a foreign power under FISA.

Now imagine the teenager's version of the story. After finishing his freshman year studying archaeology, Sadiq was thrilled to learn that his parents were taking the family to Egypt. When a classmate texted that he had found a guide and was going to explore Palmyra, an ancient Near Eastern city in central Syria, Sadiq bought a cheap ticket to join him for a few days at the ruins.

With that additional context, the government's assertions that Sadiq has joined ISIS seem suspect. But if Sadiq and his lawyers are forbidden from seeing the original warrant, they have no way of knowing what the government missed and what it got wrong.

As in Sadiq's imaginary case, FISA defendants face two impossible tasks: they cannot make a specific enough showing for a *Franks* hearing, and FISA's disclosure provision is read so narrowly that it is impossible to satisfy. As a result, courts have granted no suppression motions and only one disclosure motion, leaving these individuals at a huge disadvantage compared with similarly situated defendants who have full access to warrants.

To challenge a warrant in a *Franks* hearing, a defendant must make a "substantial preliminary showing" of particular false or omitted statements in the warrant affidavit.[152] This is problematic in the FISA context, where defendants do not have access to the contents of the warrant or affidavit. As Judge Rovner of the Seventh Circuit admitted, "it is well past time to recognize that it is virtually impossible for a FISA defendant to make the showing that *Franks* requires in order to convene an evidentiary hearing."[153] But rather than craft a modified *Franks* process that has meaning in the FISA context, courts routinely deny defendants' motions while paying lip service to the fact that their burden is "all but insurmountable."[154]

---

[152] *Franks*, 438 U.S. at 155–56.
[153] United States v. Daoud, 755 F.3d 479, 496 (7th Cir. 2014) (Rovner, J., concurring).
[154] United States v. Aziz, 228 F. Supp. 3d 363, 371 (M.D. Pa. 2017).

With the *Franks* process foreclosed, FISA defendants have only the statute's disclosure mechanism to help them challenge illegal surveillance. But this too has been interpreted so as never to apply. As a baseline, courts are required to review FISA materials *in camera* only if the Attorney General files a sworn affidavit "that disclosure or an adversary hearing would harm the national security."[155] The government has filed such an affidavit raising the specter of imminent harm in every FISA case to date.[156] As discussed above, once the judge reviews the materials *in camera*, Congress deemed disclosure to the defense "necessary" when there are inconsistencies in application materials, signs of over-broad surveillance, or if the case is otherwise complex.[157] In practice, courts appear to balk at the "necessary" wording, which effectively admits that they are not omniscient and need defense input.

Only one judge has ever granted defense counsel access to FISA applications. When asked about the national security risk of disclosure to defense counsel with appropriate security clearances, the government in *Daoud* argued merely that "it has never been done."[158] Judge Coleman found that position "unpersuasive"[159] and ordered disclosure since "an accurate determination of the legality of the surveillance is best made in this case as part of an adversarial proceeding."[160] The Seventh Circuit promptly overturned Judge Coleman's order, largely because the district court "did not find that disclosure was necessary, only that it 'may be necessary.'"[161]

The government uses the almost unbroken line of denials to pressure judges to continue blocking access to FISA applications and warrants. In 2012, the DOJ argued that "there is nothing . . . that would justify this case becoming the first 'exception' to the rule of all previous FISA litigation—that is, the first-ever to order the production and disclosure of highly sensitive and classified FISA materials or the suppression of FISA-obtained

---

[155] 50 U.S.C. § 1806(f).
[156] DAVIS S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS AND PROSECUTIONS § 30:7.
[157] *See* discussion *supra* Part IV.A (citing S. REP. NO. 95-604, pt. I, at 58 (1977) and S. REP. NO. 95-701 at 64 (1978)).
[158] United States v. Daoud, No. 12-cr-00723, 2014 WL 321384, at *2 (N.D. Ill. Jan. 29, 2014), *rev'd*, 755 F.3d 479 (7th Cir. 2014).
[159] *Id.*
[160] *Id.* at *3.
[161] United States v. Daoud, 755 F.3d 479, 482 (7th Cir. 2014), *supplemented*, 761 F.3d 678 (7th Cir. 2014).

or -derived evidence."[162] While some judges have pushed back on this reasoning,[163] it is no doubt persuasive, as ordering disclosure of a FISA application guarantees immediate interlocutory appeal and almost certain reversal.

The uniform denial of disclosure appears to discourage defense counsel from filing FISA motions in the first place. Most defense attorneys do not file any FISA-related motions: only 38% filed a motion to disclose the FISA application or warrant, and only 50% filed a FISA-related suppression motion. Without access to the underlying affidavits and warrants, the defense must "operate blindly" in challenging the warrant or complying with it.[164] The stream of denials renders FISA's statutory disclosure mechanism and suppression remedy effectively inaccessible.

2. The government uses its classification power to defendants' detriment.

Defense counsel often cannot access evidence critical to their client's case because the government deems the information classified, thereby shielding many national security surveillance programs from legal challenges. As one experienced terrorism defense attorney has written, "a growing two-tiered system of procedural due process is becoming the everyday reality."[165] This issue has led scholars to conclude that secret evidence raises procedural justice concerns and "distort[s] the adversary system."[166]

FISA-notice recipients within the dataset had little to no access to classified evidence through counsel—and their defense was hindered further

---

[162] Gov't's Unclassified Memorandum in Opposition to Defendant's Motion to Suppress the Fruits of Electronic Surveillance Pursuant to FISA at 19, United States v. Abdul-Latif, No. 2:11-cr-00228 (W.D. Wash. July 27, 2012), ECF No. 111.

[163] *E.g.*, United States v. Aziz, 228 F. Supp. 3d 363, 368 (M.D. Pa. 2017) ("[T]o the extent the government intimates that disclosure is inappropriate merely because it is unprecedented, we reject the suggestion. That disclosure has not previously been ordered does not foreclose the possibility. Moreover, the court questions whether this consensus accurately reflects Congressional intent.").

[164] HUMAN RIGHTS WATCH, *supra* note 70, at 102.

[165] Thomas A. Durkin, *Permanent States of Exception: A Two-Tiered System of Criminal Justice Courtesy of the Double Government Wars on Crime, Drugs & Terror*, 50 VALPARAISO L. REV. 419, 420 (2016).

[166] HUMAN RIGHTS WATCH, *supra* note 70, at 107; *see also* Ellen Yaroshefsky, *Secret Evidence Is Slowly Eroding the Adversary System: CIPA and FISA in the Courts*, 34 HOFSTRA L. REV. 1063, 1066 (2006).

by the government's exploitation of CIPA, which was applied in almost three-quarters of the criminal cases in the dataset.

I was able to find the security clearance status of only just over one-third of defense attorneys. Of those, 112 (28% of the total set of defense attorneys) either had clearances at the time of the case or obtained them while working on the case. Uncleared counsel struggled to put together a defense without access to key evidence. And without access to the full classified documents or recordings, they also cannot hope to challenge the summary of classified evidence allowed under CIPA,[167] even though appellate courts have found some summaries "deficient" and lacking "crucial context."[168] Without the informed advocacy of defense counsel, courts are ill-equipped to challenge the government's assertions.[169]

Yet even with a clearance, counsel still might not receive access to relevant classified evidence. In addition to possessing the required clearance, an individual must have a "need-to-know" with respect to a particular document.[170] That determination is made by the Executive Branch alone—without judicial review.[171] The government often decides that defense counsel lack sufficient need-to-know, despite CIPA's assumption that cleared attorneys do not generally pose a risk of disclosing classified information,[172] and the fact that defense counsel often obtain the same or higher clearances than do judges and prosecutors.[173]

Even when counsel obtain clearances and receive discovery materials, that may not be enough to enable a meaningful defense. *Al-*

---

[167] *See* 18 U.S.C. app. 3 § 4.

[168] United States v. Sedaghaty, 728 F.3d 885, 906–07 (9th Cir. 2013); HUMAN RIGHTS WATCH, *supra* note 70, at 11.

[169] *See* Yaroshefsky, *supra* note 166, at 1071–72.

[170] Exec. Order No. 13,526 § 4.1(a)(3), 75 Fed. Reg. 707, 720 (Dec. 29, 2009).

[171] *Id.* § 6.1(dd) ("'Need-to-know' means a determination within the executive branch . . . .").

[172] *See* Thomas R. Bowman, *Conflicts in Withholding Classified Evidence from Criminal Defendants: Looking Beyond Statutory Compliance in* United States v. Daoud, 42 S. ILL. U. L.J. 99, 110 (2018).

[173] *See* Joshua L. Dratel, *Section 4 of the Classified Information Procedures Act: The Growing Threat to the Adversary Process*, 53 WAYNE L. REV. 1041, 1053 (2007); Durkin, *supra* note 165, at 452 ("[T]here is something horribly foreboding about being asked to leave an American courtroom in the name of "national security"—despite my having even higher security clearances than most prosecutors—so that those prosecutors can tell the court in an ex parte non-public secret proceeding what transpired with respect to how they obtained evidence to be used against one's client.").

Hussayen, discussed briefly in the Introduction, demonstrates the asymmetric power that classification gives the prosecution. In that case, the government declassified all intercepts that it planned to use at trial but refused to declassify any material helpful to the defense. Mr. Al-Hussayen's counsel could not find local, cleared Arabic speakers to translate the huge volume of classified discovery material, making it impossible to flesh out their defense.[174] The weekend before trial, the government ultimately declassified the entirety of the discovery, showing that its prior protestations of grave national security harm were simply a litigation tactic.[175]

In terrorism cases like Mr. Al-Hussayen's, the government wields CIPA as a weapon against defendants. CIPA was created for prosecuting American intelligence officers who had shared classified material without authorization; those defendants were aware of the classified documents they had accessed, so they were not prejudiced in the same way when access to that evidence was blocked. [176] In contrast, terrorism defendants are unlikely to remember details of their daily communications over long periods of surveillance, or know what communications the government has deemed classified. Yet even when the classified evidence is solely the contents of a defendant's own conversations, the government often will not allow access, deepening defendants' disadvantage.[177] In a significant proportion of cases, defense counsel are thus unable to see or challenge evidence against their clients, preventing a fair trial.

---

[174] Memorandum in Support of Motion to Declare CIPA Unconstitutional as Applied in This Case at 1–2, 4, United States v. Al-Hussayen, No. 3:03-cr-00048 (D. Idaho Feb. 17, 2004), ECF No. 446.

[175] *Id.* ("As a result of the government's tactical refusal to declassify the entirety of Mr. Al-Hussayen's intercepted communications—instead opting to declassify only those intercepts the government deems helpful to the prosecution—Mr. Al-Hussayen will be effectively deprived of the use of invaluable exculpatory information that is material to his defense."); *see also* Joshua L. Dratel, *Sword or Shield? The Government's Selective Use of Its Declassification Authority for Tactical Advantage in Criminal Prosecutions*, 5 CARDOZO PUB. L. POL'Y & ETHICS J. 171, 176–79 (2006) (discussing *Al-Hussayen* and similar declassification gymnastics in other terrorism cases and noting that the Southern District of New York's policy instead declassifies all intercepts for the defense).

[176] *See* Dratel, *supra* note 173, at 1045 n.24.

[177] *See, e.g.*, Government's Objections in Opposition to Defendants' Proposed Protective Order at 8–9, United States v. Islamic American Relief Agency, No. 4:07-cr-00087 (W.D. Mo. Sept. 17, 2007), ECF No. 90 (arguing that a "defendant's right to the discovery of his own recorded statements . . . when such evidence may arguably include classified information . . . will irreparably erode the Government's ability to protect classified materials"); Dratel, *supra* note 173, at 171.

C. Implications of Results of Litigation

The use of secret warrants and evidence hurts defendants' due process rights and eviscerates the adversary process. In large part due to these procedural hurdles and uncontestable classified evidence, Human Rights Watch has found "serious fair trial concerns" in American terrorism cases.[178]

More generally, litigation secrecy removes a key check on the government's use of powerful surveillance tools. FISC judges are circumscribed in how much scrutiny they apply to warrant applications and may only review certifications for clear error,[179] so examination in the adversarial setting of a public court is important.

The low volume of FISA motions practice is particularly concerning because errors in the FISA application process are prevalent. In 2020, the Justice Department's Inspector General ("IG") published an audit of a sample of FISA applications, focusing on documentation supporting factual assertions in affidavits.[180] The IG "identified apparent errors or inadequately supported facts in all of the 25 applications [he] reviewed" with "an average of about 20 issues per application."[181] The IG concluded that his office lacked "confidence that the FBI has executed its Woods Procedures in compliance with FBI policy."[182]

Errors have been the status quo for decades. In 2002, the FISC castigated the government for belatedly admitting "misstatements and omissions of material facts" in 75 FISA applications.[183] A decade later, the FISC wrote that it was "troubled that the government's revelations regarding [the] NSA's acquisition of Internet transactions mark the third

---

[178] HUMAN RIGHTS WATCH, *supra* note 70, at 76.

[179] *See* 50 U.S.C. § 1805(a).

[180] OFFICE OF THE INSPECTOR GEN., DEP'T OF JUSTICE, MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS (Mar. 2020) [hereinafter WOODS PROCEDURES AUDIT REPORT]; *see also* Charlie Savage, *Problems in F.B.I. Wiretap Applications Go Beyond Trump Aide Surveillance, Review Finds*, N.Y. TIMES (Mar. 31, 2020), https://www.nytimes.com/2020/03/31/us/politics/fbi-fisa-wiretap-trump.html[https://perma.cc/4622-VV35].

[181] WOODS PROCEDURES AUDIT REPORT, *supra* note 180, at 3, 7.

[182] *Id.* at 2.

[183] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002).

instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."[184]

If the expert judges on the FISC are unable to catch these numerous errors in the FISA application process, it is highly unlikely that a generalist district court judge would be able to find issues in applications without defense input. As Judge Rovner explained, "I view it as mistaken to believe that a judge will be able on his or her own to ferret out any potential misrepresentations or omissions in the FISA application, given that the judge lacks a defendant's knowledge as to the facts underlying the application and has only the government's version of the facts."[185] The inability to challenge FISA warrants or evidence places these defendants at a significant disadvantage compared to defendants surveilled under ordinary law enforcement authorities, who can read the warrants approved against them and challenge them from a place of knowledge.

Advocates and judges have proposed an array of solutions to these issues, although an extensive discussion of those proposals is beyond the scope of this Article. Judge Rovner has suggested one small improvement that bears mention: requiring the government to produce a complete record of a defendant's statements when portions of those statements were used to support a FISA application so that the court can review for omissions or mischaracterizations.[186] Advocates have also argued for allowing cleared defense counsel to receive full access to relevant classified material[187]—which, in addition to enabling a fair trial, would streamline litigation by avoiding blind motions practice.[188] To increase the accessibility of cleared defense counsel, the Brennan Center has suggested that Congress establish a permanent cadre of pre-cleared attorneys for terrorism cases involving classified information.[189] With respect to defendants themselves, many advocates argue that FISA intercepts of a defendant's own communications should be declassified, with judicial discretion as to a protective order to govern defendant access.[190] While courts lack the ability to order evidence declassified, judges could dismiss charges or suppress evidence if the

---

[184] Redacted, 2011 WL 10945618, at *5 n.14 (FISA Ct. Oct. 3, 2011).
[185] United States v. Daoud, 755 F.3d 479, 494 (7th Cir. 2014) (Rovner, J., concurring).
[186] *Id.* at 494–95.
[187] Yaroshefsky, *supra* note 166, at 1086–87.
[188] *See* conversation with former DOJ NSD employee, *supra* note 65.
[189] SERRIN TURNER & STEPHEN J. SCHULHOFER, BRENNAN CENTER FOR JUSTICE, THE SECRECY PROBLEM IN TERRORISM TRIALS 27 (2005).
[190] Dratel, *supra* note 173, at 186–87.

government refused declassification.[191]

V. CONSTITUTIONAL CHALLENGES

In addition to the procedural justice problems raised by secret evidence, academics and judges have outlined numerous ways that FISA might violate the Fourth Amendment's guarantees.[192] Despite repeatedly raising these concerns, federal appellate courts seem loath to investigate how FISA operates in practice, instead relying on decades-old precedent to allow domestic surveillance outside the bounds of the Fourth Amendment.[193] More critically, after the Supreme Court's 2013 decision in *Clapper*, notice recipients (i.e., people who can prove with certainty they were surveilled) are the only litigants with standing to attack FISA's constitutionality.[194] But this group rarely files challenges, leaving the status quo unquestioned and unexamined in the courts.[195]

A. Squaring FISA and the Fourth Amendment

Academics disagree on whether FISA complies with the Fourth Amendment, particularly with respect to its probable cause, particularity, and notice requirements.

The Fourth Amendment requires warrants for "unreasonable searches and seizures" to be issued by a neutral judge based "upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."[196] To obtain a warrant, the government must demonstrate probable cause that it expects to find "contraband or evidence of a crime,"[197] and the warrant must be particularized as to the person and place to be searched.[198] In general, the person searched must receive notice of the search.[199]

Each of these Fourth Amendment requirements apply to domestic

---

[191] *See* conversation with former DOJ NSD employee, *supra* note 65.
[192] *See infra* Subpart A.
[193] *See infra* Subpart B.
[194] *See infra* Subpart C.
[195] *See id.*
[196] U.S. CONST. amend. IV.
[197] Ornelas v. United States, 517 U.S. 690, 696 (1996).
[198] Ybarra v. Illinois, 444 U.S. 85, 91 (1979).
[199] *See* 3 WAYNE R. LAFAVE, SEARCH & SEIZURE § 6.2(a) (6th ed. 2020) (citing Ker v. California, 374 U.S. 23 (1963)).

electronic and other surveillance. As the Supreme Court explained in *Berger*, "[t]he need for particularity and evidence of reliability . . . is especially great in the case of eavesdropping."[200] Surprisingly, the notice requirement also generally applies to secret surveillance, although ex post notice is sufficient. When the Wiretap Act was challenged for its lack of an advance-notice requirement, the Supreme Court upheld the law because its judicially enforced post-wiretap notice was "a constitutionally adequate substitute for advance notice."[201]

I explore below the academic consensus that FISA's requirements differ meaningfully from those of the Fourth Amendment. Even a former FISC judge has emphasized that "[w]hat FISA does is not adjudication, but approval."[202] Nevertheless, some commentators believe that FISA's focus on foreign surveillance is an acceptable compromise given the danger of international terrorism.[203] In this Subpart I briefly canvass four categories of Fourth Amendment concerns.

1. Probable Cause

FISA does not meet the Fourth Amendment's probable cause requirement. The statute instead uses a lower "foreign intelligence standard"[204] that Congress admitted was "not, of course, comparable to a probable cause finding by the judge."[205] These minimally scrutinized applications lead to "surveillances and searches for extensive periods of time; based on a standard that the U.S. person is only using or about to use the places to be surveilled and searched," with no need to prove criminal activity.[206]

Academics hold a variety of opinions about the propriety of this lower standard. Stephen Schulhofer argues the "substantially diluted" cause

---

[200] Berger v. New York, 388 U.S. 41, 56 (1967).
[201] Dalia v. United States, 441 U.S. 238, 248 (1979) (citing United States v. Donovan, 429 U.S. 413, 429 n.19 (1977)).
[202] Dan Roberts, *US Must Fix Secret FISA Courts, Says Top Judge Who Granted Surveillance Orders*, THE GUARDIAN (July 9, 2013), https://www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance [https://perma.cc/LKH3-AD4R] (quoting Judge James Robertson).
[203] *See, e.g.*, William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1220 (2007).
[204] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624 (FISA Ct. 2002).
[205] H.R. REP. NO. 95-1283, pt. I, at 80 (1978).
[206] *In re All Matters*, 218 F. Supp. 2d at 624.

requirement compared to ordinary searches gives the government potentially "troubling" discretion.[207] Steve Vladeck argues that the standard "shift[s] the requisite burden" from demonstrating probable cause of criminal activity to demonstrating merely that the target is an "agent of a foreign power."[208] Some view this lower bar as an acceptable compromise: allowing a cause standard lower than the Fourth Amendment's in return for some regulation of foreign intelligence surveillance.[209] Others note the slightly higher bar for demonstrating that a U.S. person is an agent of a foreign power, under which the government must have probable cause that they are engaged in intelligence gathering, terrorism, or identity fraud.[210]

FISA originally required that the "purpose" of surveillance under the Act be to obtain foreign intelligence information; courts subsequently interpreted "purpose" to mean "primary purpose."[211] The Patriot Act broadened FISA's scope by replacing that language with "a significant purpose."[212] This semantic change has been criticized, even by those supportive of the original bill, as allowing the government to "circumvent" and "skirt" the Fourth Amendment by using FISA as a domestic law enforcement tool.[213]

2. Particularity

Second, FISA does not satisfy the Fourth Amendment's particularity requirement. To obtain a search warrant, the government must demonstrate probable cause that the particular communications or items to be searched will yield evidence of a crime.[214] Under FISA, the government instead

---

[207] Stephen J. Schulhofer, *The New World of Foreign Intelligence Surveillance*, 17 STAN. L. & POL'Y REV. 531, 533, 543 (2006).

[208] Steve Vladeck, *Why Clapper Matters: The Future of Programmatic Surveillance*, LAWFARE (May 22, 2012), https://www.lawfareblog.com/why-clapper-matters-future-programmatic-surveillance/ [https://perma.cc/8SZ7-8Q8T].

[209] *See* Banks, *supra* note 203, at 1231.

[210] *See* Schulhofer, *supra* note 207, at 533 (citing 50 U.S.C. § 1801(b)(2) (2006)).

[211] *See* United States v. Truong, 629 F.2d 908, 915 (4th Cir. 1980) ("The executive should be excused from securing a warrant only when the surveillance is conducted 'primarily' for foreign intelligence reasons.").

[212] USA PATRIOT Act, H.R. 3162, 107th Cong. § 218 (2001) (amending 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B)).

[213] *See, e.g.*, Banks, *supra* note 203, at 1215; *Surveillance Under the USA/PATRIOT Act*, AM. CIVIL LIBERTIES UNION (2020), www.aclu.org/other/surveillance-under-usapatriot-act [https://perma.cc/H3VL-7YXZ].

[214] *See, e.g.*, WAYNE R. LAFAVE ET AL., 2 CRIM. PROC. § 3.3(a) (4th ed. 2020); Illinois v. Gates, 462 U.S. 213, 238 (1983); Dumbra v. United States, 268 U.S. 435, 441 (1925).

specifies only the target of surveillance, and the FISC has what Schulhofer calls "minimal judicial control of particularity and the scope of surveillance."[215] As another academic explains, FISA thus enables the government to monitor *all* of a target's communications and search *all* of their possessions, regardless of those communications' or possessions' relation, or lack thereof, to foreign intelligence gathering.[216]

3. Notice

Third, FISA does not require notice to the person searched, either during or after a search, unless FISA surveillance is subsequently used against them in court.[217] Academics contrast FISA's secrecy with the Wiretap Act, which requires post hoc notice "in line with the Fourth Amendment requirement," demonstrating that even clandestine surveillance can include retroactive notice without issue.[218]

4. Warrantless Surveillance under Section 702

Finally, the warrantless surveillance provisions of FISA raise the most significant constitutional concerns. Section 702 of the FISA Amendments Act allows surveillance of any "non-U.S. persons located abroad" without the government having probable cause or showing any specific link to foreign intelligence.[219] Amendments to the Patriot Act also eradicated FISA's already weak particularity showing: the FISC neither reviews individual targeting nor issues individual warrants under Section 702.[220] As the ACLU explains, the government need not specify to the

---

[215] Schulhofer, *supra* note 207, at 538 n.32.

[216] *See* Matthew R. Hall, *Constitutional Regulation of National Security Investigation: Minimizing the Use of Unrelated Evidence*, 41 WAKE FOREST L. REV. 61, 83, 85 (2006).

[217] In re All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 624 (FISA Ct. 2002). FISA requires notice after emergency surveillance that is not subsequently authorized, but this too is waived if the government twice shows "good cause." 50 U.S.C. § 1806(j).

[218] Peter P. Swire, *The System of Foreign Intelligence Surveillance Law*, 72 GEO. WASH. L. REV. 1306, 1323 (2004); Benjamin Wittes, *The Inspector General's Disturbing FISA Memo*, LAWFARE (Mar. 31, 2020), www.lawfareblog.com/inspector-generals-disturbing-fisa-memo [https://perma.cc/8REJ-5263].

[219] *Cf.* 50 U.S.C. § 1881a(h)(2)(A)(v) (government must merely "attest" that "a significant purpose of the acquisition is to obtain foreign intelligence information"); *see also* Clapper v. Amnesty Int'l USA, 568 U.S. 398, 404 (2013).

[220] *See* 50 U.S.C. § 1881a(j)(1)(A) (FISC "shall have jurisdiction to review" only the government's certification, targeting procedures, minimization procedures, and querying procedures).

Court "who it intends to surveil, what phone lines and email addresses it intends to monitor, where its surveillance targets are located, or why it's conducting the surveillance."[221]

More recently, the FISA Amendments Act ("FAA") also "eliminated," as Justice Breyer described it, the requirement to state "each specific target and identify each facility at which . . . surveillance would be directed, thus permitting surveillance on a programmatic, not necessarily individualized, basis."[222] The result is that the government can monitor any communications facility, including those within the United States, and monitor Americans' communications with or about foreigners.[223] Because bulk foreign surveillance incidentally collects U.S. persons' communications without a specific court authorization or any evidence that they are involved in criminal activity, Steve Vladeck argues it is possible that "warrantless collection of US person content under section 702 violates the Warrant Clause" of the Fourth Amendment.[224]

B. Adjudicating FISA's Constitutionality

These competing theories about whether FISA complies with the Fourth Amendment have played out in the courts at a high level, but public appellate courts appear unwilling to adjudicate the constitutionality of its surveillance provisions in a meaningful way. Only twelve cases have discussed FISA's constitutionality under the Fourth Amendment in any depth.[225]

---

[221] ACLU, WHY THE FISA AMENDMENTS ACT IS UNCONSTITUTIONAL 2 (Feb. 5, 2008), https://www.aclu.org/other/extended-analysis-why-faa-unconstitutional [https://perma.cc/KF5G-FW58].

[222] *Clapper*, 568 U.S. at 425 (Breyer, J., dissenting).

[223] *See* Jennifer Granick, *The FISA Amendments Act Authorizes Warrantless Spying on Americans*, CTR. FOR INTERNET AND SOC'Y (Nov. 5, 2012), cyberlaw.stanford.edu/blog/2012/11/fisa-amendments-act-authorizes-warrantless-spying-americans [https://perma.cc/3EK2-S7D4].

[224] Steve Vladeck, *Section 702, the Fourth Amendment, and Article III: The Muhtorov (Non-)Decision*, JUST SEC. (Nov. 20, 2015), www.justsecurity.org/27784/section-702-fourth-amendment-article-iii-muhtorov-non-decision/ [https://perma.cc/FC22-TS3V].

[225] United States v. Moalin, 973 F.3d 977 (9th Cir. 2020); United States v. Hasbajrami, 945 F.3d 641 (2d Cir. 2019); United States v. Wright, 937 F.3d 8 (1st Cir. 2019); United States v. Mohamud, 843 F.3d 420 (9th Cir. 2016); United States v. Ali, 799 F.3d 1008, 1021 (8th Cir. 2015); United States v. Duka, 671 F.3d 329 (3d Cir. 2011); United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010); In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157 (2d Cir. 2008); United States v. Ning Wen, 477 F.3d 896 (7th Cir. 2007); United States v. Pelton, 835 F.2d 1067 (4th Cir. 1987); United States v. Cavanagh, 807

In the seminal 1974 *Keith* case, the Supreme Court refused to read in a domestic intelligence exception to the Fourth Amendment, while leaving undecided the question of a foreign intelligence grey area.[226] Subsequently, several circuits recognized a qualified foreign intelligence surveillance exception to the Fourth Amendment's Warrant Clause.[227] In 1984, the Second Circuit held in *Duggan* that FISA's procedures were "a constitutionally adequate balancing of the individual's Fourth Amendment rights against the nation's need to obtain foreign intelligence information."[228] Seven years later, the First Circuit rejected constitutional concerns with a mere one-sentence citation to *Duggan* instead of its own analysis,[229] while in 2007, the Seventh Circuit considered and accepted FISA's constitutionality in all of two pages.[230]

Circuit and district courts have repeatedly suggested that FISA may be unconstitutional in some applications, but judges almost never hold it to be unlawful in any specific case. For example, one judge explained that though he was "convinced the FAA is susceptible to unconstitutional application as an end-run around the Wiretap Act and the Fourth Amendment's prohibition against warrantless or unreasonable searches, [he was] equally convinced that it was not unconstitutionally applied."[231] The Ninth Circuit illuminated the high stakes of the debate over FISA's constitutionality while refusing to engage itself:

> The idea that the government can decide that someone is a foreign agent based on secret information; on that basis obtain computers containing "[t]he sum of [that] individual's private life," *Riley v. California*, 134 S. Ct. 2473, 2489 (2014); and then prosecute that individual for completely unrelated crimes discovered as a result of rummaging through that computer comes perilously close to the exact abuses against which the Fourth Amendment was designed

---

F.2d 787 (9th Cir. 1987); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[226] *See* United States v. U.S. District Court (*Keith*), 407 U.S. 297, 316–22 (1972).

[227] *See* Steve Vladeck, *More on Clapper and the Foreign Intelligence Surveillance Exception*, LAWFARE (May 23, 2012), www.lawfareblog.com/more-clapper-and-foreign-intelligence-surveillance-exception [https://perma.cc/ZJ75-YCQQ].

[228] *Duggan*, 743 F.2d at 73.

[229] United States v. Johnson, 952 F.2d 565, 573 (1st Cir. 1991) (citing *Duggan*, 743 F.2d at 72–74).

[230] *Ning Wen*, 477 F.3d at 897–99.

[231] United States v. Muhtorov, 187 F. Supp. 3d 1240, 1243 (D. Colo. 2015).

> to protect. However, the district court did not commit plain error by concluding otherwise.[232]

In contrast, the specialized courts with access to classified information and which deal with FISA routinely have questioned more directly whether the statute meets constitutional requirements. When the Foreign Intelligence Surveillance Court of Review ("FISCR"), the Article III court that hears appeals from the FISC, examined the Patriot Act's removal of the "primary purpose" requirement, only government attorneys participated in the secret oral argument.[233] The FISCR acknowledged that in terms of the probable cause and particularity requirements, "a FISA order may not be a 'warrant' contemplated by the Fourth Amendment,"[234] though it held that "the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close."[235] But by 2008 the FISCR had given up on Fourth Amendment critiques, instead "formally recognizing for the first time a 'foreign intelligence surveillance' exception to the Fourth Amendment."[236]

Despite these theoretical acknowledgements of FISA's infirmities, only one judge has ever held FISA to be unconstitutional. In *Mayfield*, Judge Aiken explained that the "significant purpose" change under the Patriot Act means that "for the first time in our Nation's history, the government can conduct surveillance to gather evidence for use in a criminal case without a traditional warrant, as long as it presents a non-reviewable assertion that it also has a significant interest in the targeted person for foreign intelligence purposes."[237] She found that the amendments to FISA created "extra-constitutional authority" that deprived the Fourth Amendment of "of any real meaning."[238] And she explained that "the Supreme Court has never upheld a statute that, like FISA, authorizes the government to search a person's home or intercept his communications without ever informing the person that his or her privacy has been

---

[232] United States v. Gartenlaub, 751 Fed. App'x 998, 1000 (9th Cir. 2018).
[233] In re Sealed Case No. 02-001, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).
[234] *Id.* at 741.
[235] *Id.* at 746.
[236] Vladeck, *supra* note 208 (citing In re Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008)).
[237] Mayfield v. United States, 504 F. Supp. 2d 1023, 1036 (D. Or. 2007), *vacated on other grounds*, 588 F.3d 1252 (9th Cir. 2009), *opinion vacated and superseded*, 599 F.3d 964 (9th Cir. 2010).
[238] *Id.* at 1042.

violated."[239] The Ninth Circuit vacated Judge Aiken's decision for lack of standing after the plaintiffs settled with the government, so the appellate court did not address the constitutional questions.[240]

Given these persistent, unanswered constitutional issues, it is surprising that so few FISA notice recipients challenge the statute's constitutionality. Only 17% of recipients made constitutional challenges to FISA based on the Fourth Amendment (including defendants who joined in their co-defendants' constitutional challenges). Encouragingly, those challenges were more fully argued than other motions, averaging ten pages of argument on Fourth Amendment issues alone. However, patterns in which attorneys filed challenges suggest differential access to relevant experience. More than a quarter of these Fourth Amendment motions were filed by federal public defenders or one of two lawyers, Joshua Dratel and Thomas Durkin, both of whom are frequently appointed as free counsel under the Criminal Justice Act ("CJA"). Indigent defendants who were appointed other CJA attorneys filed challenges at a much lower rate. In multi-defendant cases, only one defendant can be represented by the federal public defender, meaning that defendants who do not happen to be assigned one of these attorneys may be receiving less zealous representation. In addition, cleared counsel were twice as likely to file constitutional challenges—over a quarter filed motions, comprising almost half of all challenges. Clearances are often a proxy for attorneys with more national security litigation experience, leading to a similar imbalance in representation.

C. Implications for Accountability

The combination of minimal judicial scrutiny and few litigated constitutional challenges is concerning because at minimum, hundreds of thousands of American residents are currently surveilled under a plausibly unconstitutional legal authority. Unlike much of the statutory regime that governs Americans' day-to-day lives, FISA has not faced searching judicial scrutiny or had its legality definitively confirmed by public courts with an opportunity to hear adversarial argument. Courts reviewing the "primary purpose" change in the Patriot Act have largely cited to the FISCR's *ex parte* analysis. As one of the drafters of FISA has argued, "[t]he real test, however, should be at least in a traditional adversarial proceeding and

---

[239] *Id.* at 1039.
[240] *Id.* at 1254.

preferably in an as-applied case."[241]

The dearth of in-depth constitutional analysis of FISA and its recent amendments places a statute that affects a huge number of people above the law and "undercuts deterrence of law enforcement misconduct."[242] Without public adjudication, there is no way to check errors in the surveillance process or ensure accountability for congressional power creation or executive use of power.

The absence of constitutional challenges in these cases is especially concerning since notice recipients are now the only individuals who have standing to challenge FISA itself. When the Supreme Court rejected a constitutional challenge to FISA in *Clapper*, it attempted to allay fears about creating an unreviewable statute by claiming that criminal defendants would receive notification of surveillance and thus have sufficient standing.[243] After this case, notice recipients are likely the only people "*Clapper*-qualified" to challenge FISA.[244]

If more notice recipients challenged FISA's constitutionality, more judges could consider these potential issues, opening more debate and casting light on a shadowy law. In the absence of people filing challenges, the secret and unappealable decisions of the FISCR are the only ones on point.[245] Without a change to relax *Clapper*'s standing requirements, people who receive notice hold the only keys to public adjudication of critical constitutional questions.

CONCLUSION

At least tens of thousands of American citizens and residents, and hundreds of thousands of others, are surveilled under FISA every year without probable cause that they are involved in criminal activity or connected to any foreign entity. The vast majority of them will never know that they were spied upon and have "no way of challenging the legality of the surveillance or obtaining any remedy for violations of their

---

[241] William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma*, 11 LEWIS & CLARK L. REV. 1099, 1136 (2007).
[242] Sinnar, *supra* note 83, at 1346.
[243] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 421 (2013).
[244] *See* Order Denying Motion to Suppress Evidence Obtained or Derived Under FISA Amendments Act or for Discovery at 3, United States v. Muhtorov, No. 12-cr-00033 (D. Colo. Nov. 19, 2015), ECF No. 885.
[245] *See* Schulhofer, *supra* note 207, at 539.

constitutional rights."[246] For a tiny fraction, receiving notice of FISA surveillance begins a Kafkaesque, dystopian nightmare of secret evidence and unreviewable warrants.

The 401 notice recipients collected and analyzed here represent the tip of the FISA iceberg. These cases reveal demographic and ideological disparities that should spur advocates and politicians to push for transparency throughout the FISA application process and subsequent prosecutorial decisions. The patterns visible in the notice dataset bolster calls to increase the level of international connection required for FISA warrants and to refocus resources across domestic terror threats. The procedural and evidentiary challenges in FISA cases should be addressed by including defense counsel in a true adversarial process, allowing disclosure of FISA applications in more circumstances, and increasing the scrutiny given to government assertions of national security risks. Congress should also add a provision to FISA to allow legal challenges with a lower injury bar than *Clapper* required for standing, countering the government's ability to control whether notice is filed and thus who may challenge surveillance practices.

Before FISA was enacted, Senator Frank Church warned the country that "[w]e have a particular obligation to examine the NSA, in light of its tremendous potential for abuse" when it "turn[s] its awesome technology against domestic communications."[247] Forty years later, his warning remains just as urgent.

---

[246] Mayfield v. United States, 504 F. Supp. 2d 1023, 1039 (D. Or. 2007), *vacated on other grounds*, 588 F.3d 1252 (9th Cir. 2009), *opinion vacated and superseded*, 599 F.3d 964 (9th Cir. 2010).

[247] *Intelligence Activities: The National Security Agency and Fourth Amendment Rights*: *Hearings Before the Select Comm. to Study Governmental Operations with Respect to Intelligence Activities*, 94th Cong. 2 (1975) (statement of Sen. Church, Chairman).

APPENDIX

A. Notice Collection

To compile an exhaustive list of all notice recipients, I used multiple sources: Bloomberg and LexisNexis docket searches, Bloomberg and Westlaw opinion searches, an ACLU dataset, the *Intercept*'s *Trial and Terror* database, national security treatises, newspaper articles, Westlaw Key Numbers, and citations to significant FISA cases.

1. Docket Searches

I began with a series of keyword searches in Bloomberg, which provides searchable access to the U.S. Courts' PACER system. My first search was for the terms *FISA OR "Foreign Intelligence Surveillance Act"* in federal criminal cases between 1990 and 2020, which produced 330 results. I searched within each of these cases' dockets for the terms *FISA*, *surveillance*, *intent*, and *notice*. This yielded actual notice for 253 defendants; twenty-two defendants where notice was docketed but not available online; and forty cases where the government and/or judge noted that FISA was used but no notice was docketed. For the remaining cases, I looked through each case's entire docket to find notices that did not appear in searches. This yielded eighteen more defendants who had received a notice that was not surfaced by Bloomberg's often inconsistent within-case docket search.

Next, I searched within federal criminal cases for mentions of each relevant statutory provision: *"50 U.S.C. 1801"*; *"50 U.S.C. 1806"*; *"50 U.S.C. 1825"*; *"50 U.S.C. 1845"*; and *"50 U.S.C. 1881"*. This yielded one additional case where the government referenced having provided notice during discovery.[248] I also searched for a different permutation of the following provisions: *"section 1801"*; *"section 1806"*; *"section 1825"*; *"section 1845"*; and *"section 1881."* This unearthed three cases, including a court-martial.[249]

---

[248] Memorandum of Law of the U.S. in Opposition to Sabirhan Hasanoff's Motion Pursuant to 28 U.S.C. § 2255 to Correct, Vacate, or Set Aside His Conviction at 11 n.7, United States v. El-Hanafi, No. 1:10-cr-00162 (S.D.N.Y. Feb. 11, 2015), ECF No. 208 ("During discovery, the Government provided Hasanoff's counsel with notice for purposes of 50 U.S.C. §§ 1806(c) and 1825(d).").

[249] United States v. Millay, No. 3:13-mc-00005 (D. Alaska Jan. 17, 2013).

I then searched all of the previous terms in federal civil cases, which led to two more cases: a Specially Designated Global Terrorist dispute[250] and a wrongful death claim where a dead man's estate received notice on his behalf.[251]

I repeated all of the previous searches for state dockets. Almost all state results were typos or incorrectly scanned versions of "visa," "FLSA," "FSIA," or "USA"; I found no additional state cases with actual FISA notice in this search.

I repeated all of the prior searches on LexisNexis, which also indexes PACER. The search of federal and state criminal dockets yielded thirty-seven federal criminal cases that had not appeared in my Bloomberg searches. I also searched the previous terms in civil cases, which led to a link to a state case.[252] There seem to be two reasons for these cases being missed earlier. First, in many of the cases, FISA notice was filed after Bloomberg had last updated the docket, meaning it was not indexed or searchable.[253] Second, and more concerningly, some of the cases were missing entirely from Bloomberg.[254]

2. ACLU Compilation

Patrick Toomey at the ACLU National Security Project was kind enough to provide me with a compilation of notable FISA cases from 2009 onwards, which contained 72 notice recipients. The compilation yielded one additional case that had not appeared in my prior searches.[255]

3. The *Intercept*'s Trial and Terror Database

---

[250] Kindhearts for Charitable Humanitarian Development, Inc. v. Paulsen, No. 3:08-cv-02400 (N.D. Ohio Oct. 9, 2008).
[251] Estate of Usaamah Abdullah Rahim v. United States, No. 1:18-cv-11152 (D. Mass. May 31, 2018).
[252] People v. El-Astal, No. 07-15092 (3d Jud. Cir. Mich., Crim. Div., Feb. 2, 2007).
[253] *E.g.*, United States v. Al Sadawi, No. 1:02-cr-00901 (E.D.N.Y. July 26, 2002).
[254] *E.g.*, United States v. Hanssen, No. 1:01-cr-00188 (E.D. Va. May 16, 2001) (Bloomberg Law database has magistrate case but not district court case, and notice was not filed until after transfer to the district court judge); United States v. Jones, No. 1:93-cr-00322 (D.D.C. Aug. 31, 1993).
[255] United States v. Khan, No. 3:12-cr-00659 (D. Or. Dec. 28, 2012). Bloomberg does not have the case once it was transferred from the magistrate judge to the district court; it is unclear why the case did not appear in my LexisNexis searches.

The *Intercept*, an online investigative journalism outlet, has compiled a database of post-9/11 terrorism prosecutions entitled *Trial and Terror*.[256] The database contains information of 911 people whose cases are classified by the DOJ as related to international terrorism. The database lists 133 defendants who received FISA notice.

Four defendants in the *Trial and Terror* database had been in my "unsure" collection of cases that referenced FISA, but where I had found no trustworthy indications that there had been notice in the docket or public filings.[257] In addition, I had entirely missed one person in the database; I had included his co-defendants, but the notice was not docketed and he did not make any surveillance-related motions, so he had slipped through my searches.[258] There may well be other similarly-situated defendants in the cases where notice is docketed but not publicly available; there are at most ninety-four defendants who could be in this situation from the cases in my dataset.[259]

4. Treatises

I went through every FISA case cited in *National Security Investigations and Prosecutions*, a leading national security treatise co-authored by David Kris, a former Assistant Attorney General for National Security and current amicus to the FISC.[260] This review yielded three new

---

[256] Trevor Aaronson & Margot Williams, *Trial and Terror*, INTERCEPT, trial-and-terror.theintercept.com/ [https://perma.cc/9TP2-4PF4] (last updated Apr. 30, 2020).

[257] United States v. Al-Timimi, No. 1:04-cr-00385 (E.D. Va. Sept. 23, 2004); United States v. Abdi, No. 2:04-cr-00088 (S.D. Ohio June 10, 2004); United States v. Marzook, No. 1:03-cr-00978 (N.D. Ill. Oct. 9, 2003) (two defendants received notice).

[258] This was Khalid Al-Sudanee, one of seven defendants in United States v. Islamic American Relief Agency, No. 4:07-cr-00087 (W.D. Mo. Mar. 6, 2007).

[259] This is a count of instances where notice is not docketed but is explicitly referenced in government and/or judicial filings, and where at least one defendant from the case is not included in my dataset. United States v. Maguire, No. 4:92-cr-00587 (D. Ariz. Aug. 26, 1992) (8 co-defendants); United States v. Kota, No. 1:95-cr-10015 (D. Mass. Jan. 13, 1995) (1); United States v. Hage, No. 1:98-cr-01023 (S.D.N.Y. Sept. 21, 1998) (24); United States v. Hammoud, No. 3:00-cr-00147 (W.D.N.C. July 31, 2000) (19); United States v. Berkeley Nucleonics, No. 4:01-cr-00315 (N.D. Cal. Aug. 28, 2001) (1); United States v. Elashi, No. 3:02-cr-00052 (N.D. Tex. Feb. 2, 2002) (2); United States v. Battle, No. 3:02-cr-00399 (D. Or. Oct. 3, 2002) (2); United States v. Jamal, No. 2:03-cr-00261 (D. Ariz. Mar. 13, 2003) (26); United States v. Marzook, No. 1:03-cr-00978 (N.D. Ill. Oct. 9, 2003) (1); United States v. Mak, No. 8:05-cr-00293 (C.D. Cal. June 15, 2006) (4); United States v. El-Hanafi, No. 1:10-cr-00162 (S.D.N.Y. Mar. 2, 2010) (1); United States v. Ashe, No. 1:15-cr-00706 (S.D.N.Y. Oct. 20, 2015) (5).

[260] *See generally* KRIS & WILSON, *supra* note 156. I confined my search to chapters 4–19

cases. *Mayfield* was a civil case that I had missed in my earlier docket searches.[261] *Hasan* had been given notice in a court-martial proceeding, with a subsequent civil district court case to adjudicate the legality of the surveillance.[262] Finally, notice was given in *Jamal*[263] "shortly after arrest or before the detention hearing,"[264] so the notice was not docketed. The Kris treatise also produced a state case with FISA notice, but I did not include it as notice had almost certainly been given before my 1990 cutoff.[265]

I then looked at all cases cited in *Law of Electronic Surveillance*, a treatise co-authored by Judge James Carr, a former FISC member.[266] This search yielded no new cases.

I was maximally inclusive and marked rows in the dataset as included in these treatises if the treatise cited an appeal or a later renaming of the case.

5. Opinion Searches

Next, I searched the keywords from my docket searches in federal and state opinions, both criminal and civil. I found one new civil case, a naturalization claim, in these opinions.[267] I did the same opinion searches on Westlaw without finding any new results.

I then looked at all opinions that cited to important FISA decisions. I looked at the early cases of *Megahey*,[268] *Belfield*,[269] *Duggan*,[270] *Johnson*,[271] and *Rahman*,[272] which range from 1982 to 1999. I also looked at more

---

(FISA usage) and chapters 23 and 28–33 (FISA litigation).

[261] Mayfield v. United States, No. 6:04-cv-01427 (D. Or. Oct. 4, 2004).

[262] United States v. Hasan, No. 6:12-cv-00195 (W.D. Tex. July 27, 2012).

[263] United States v. Jamal, No. 2:03-cr-00261 (D. Ariz. Mar. 13, 2003).

[264] *See* KRIS & WILSON, *supra* note 156, § 29:6.

[265] State v. Isa, 850 S.W. 2d 876 (Mo. 1993) (en banc); United States v. Isa, No. 90-73CR (E.D. Mo. June 18, 1990), *aff'd*, 923 F.2d 1300 (8th Cir. 1991) (adjudicating legality of surveillance in state case).

[266] 2 JAMES G. CARR, PATRICIA L. BELLIA & EVAN A. CREUTZ, LAW OF ELECTRONIC SURVEILLANCE § 9 (Nov. 2019 update); *Foreign Intelligence Surveillance Court*, *supra* note 121.

[267] Atalla v. Kramer, No. 2:09-cv-01610 (D. Ariz. Aug. 4, 2009).

[268] United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. Dec. 1, 1982).

[269] United States v. Belfield, 692 F.2d 141 (D.C. Cir. 1982).

[270] United States v. Duggan, 743 F.2d 59 (2d Cir. 1984).

[271] United States v. Johnson, 952 F.2d 565 (1st Cir. 1991).

[272] United States v. Rahman, 189 F.3d 88 (2d Cir. 1999).

recent (post-9/11) cases from every circuit with a published FISA case: *Stewart*,[273] *Abu-Jihaad*,[274] *Duka*,[275] *Benkahla*,[276] *El-Mezain*,[277] *Amawi*,[278] *Daoud*,[279] *Ali*,[280] *Mayfield*,[281] *Campa*,[282] and *Klayman*.[283] I also looked at citations to *Clapper*,[284] the latest Supreme Court case on FISA. The citation references did not produce any previously undiscovered cases.

6. News Articles

I then searched several news outlets (the *New York Times*, the *Washington Post*, and the *Intercept*) to find references to additional FISA cases in articles. This search yielded two supplemental notices that I had missed in cases where I had already found an earlier notice.[285]

7. Westlaw Key Numbers

Westlaw's Key Number System classifies cases by legal topic and issue. I searched all cases under twenty-three Key Numbers that appeared related to FISA from search results:

---

[273] United States v. Stewart, 590 F.3d 93 (2d Cir. 2009).
[274] United States v. Abu-Jihaad, 630 F.3d 102 (2d Cir. 2010).
[275] United States v. Duka, 671 F.3d 329 (3d Cir. 2011).
[276] United States v. Benkahla, 530 F.3d 300 (4th Cir. 2008).
[277] United States v. El-Mezain, 664 F.3d 467 (5th Cir. 2011).
[278] United States v. Amawi, 695 F.3d 457 (6th Cir. 2012).
[279] I searched the district court ruling ordering disclosure of FISA applications to defense counsel, United States v. Daoud, 2014 WL 321384 (N.D. Ill. Jan. 29, 2014), and the appellate decision overturning it, 755 F.3d 479 (7th Cir. 2014).
[280] United States v. Ali, 799 F.3d 1008 (8th Cir. 2015).
[281] I searched the district court ruling declaring FISA as amended unconstitutional, Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007), and the appellate decision overturning it, 599 F.3d 964 (9th Cir. 2010).
[282] United States v. Campa, 529 F.3d 980 (11th Cir. 2008).
[283] Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015).
[284] Clapper v. Amnesty Int'l USA, 568 U.S. 398 (2013).
[285] Charlie Savage, *Terrorism Conviction of a Wiretapped American Is Upheld on Appeal*, N.Y. TIMES (Dec. 5, 2016), www.nytimes.com/2016/12/05/us/politics/mohamed-mohamud-terrorism-conviction-upheld.html [https://perma.cc/7X8A-G44A] (yielding supplemental FAA notification in United States v. Mohamud, No. 3:10-cr-00475 (D. Or. Nov. 29, 2010)); Trevor Aaronson, *NSA Secretly Helped Convict Defendants in U.S. Courts, Classified Documents Reveal*, INTERCEPT (Nov. 30, 2017), theintercept.com/2017/11/30/nsa-surveillance-fisa-section-702/ [https://perma.cc/53ES-MZAA] (yielding supplemental FAA notification in United States v. *Zazi*, No. 1:09-cr-00663 (E.D.N.Y. Sept. 23, 2009)).

92-4462: Search, seizure, and confiscation > Electronic surveillance or eavesdropping
92-4252: War and national security > Terrorism
110-2001: Disclosure of information > Other particular issues
349-199: Searches and seizures > Hearing; in camera inspection
372-1428: Constitutional and statutory provisions > In general
372-1429: Constitutional and statutory provisions > Purpose
372-1430: Constitutional and statutory provisions > Validity
372-1434: Interception or disclosure of electronic communications > Wiretapping in general
372-1460: Authorization by courts of public officers > In general
372-1461: Authorization by courts of public officers > Executive authorization or application
372-1462: Authorization by courts of public officers > Necessity for judicial approval; emergency interception
372-1462: Authorization by courts of public officers > Judicial authorization in general
372-1465: Application or affidavit > In general
372-1466: Application or affidavit > Probable cause
372-1468: Application or affidavit > Necessity; inadequacy of other procedures
372-1469: Application or affidavit > Identification of persons subject to interception
372-1470: Authorization by courts of public officers > Order or warrant in general
372-1472: Conduct and duration of surveillance > In general
372-1473: Conduct and duration of surveillance > Scope; minimization
372-1477: Authorization by courts of public officers > Notice and disclosure to parties
372-1478: Authorization by courts of public officers > Use of information obtained
372-1479: Authorization by courts of public officers > Review of proceedings; standing
402-1133: Protection against subversive activities > Foreign intelligence surveillance

I marked rows in the dataset as being included in the Key Number if it returned an appeal or later renaming. Searching all cases under these Key Numbers for references to *FISA OR "foreign intelligence surveillance act"* yielded only previously identified recipients.

8. Potential Reasons for Missing Notices

There are several factors that might have led me to miss notices. First, spotty digitization through the early 2000s means that searches of docket entries miss notices when the docket entry's text is ambiguous and lacks relevant wording (e.g. only stating "Notice"). PACER indexes federal court records going back to 1993, but many districts did not complete digitization until the mid-2000s.[286] Any undercount from the 1990s is likely

[286] Margo Schlanger & Theodore Eisenberg, *The Reliability of the Administrative Office of the U.S. Courts Database: An Initial Empirical Analysis*, 78 NOTRE DAME L. REV 1455, 1459 & n.24 (2003) (noting that thirteen of ninety-four federal district courts still "did not have Internet-accessible records" in 2000); *see also* David Freeman Engstrom, *The* Twiqbal *Puzzle and Empirical Study of Civil Procedure*, 65 STAN. L. REV. 1203, 1208

to be small; a DOJ source confirmed that post-1996 cases are the vast bulk of FISA usage.[287] Second, Bloomberg and LexisNexis have incomplete indexing of cases and docket entries. I found several cases that were in one of Bloomberg or Lexis but were missing entirely from the other database. Lexis does not index the documents contained in docket entries, only the titles of the entries themselves. This indicates that in the worst case, I may have missed notices in search results (e.g., if the title were simply "Notice"), while a common middle-ground case involved seeing a docket entry entitled "FISA Notice" where I could not see which defendants received the notice or which statutory provisions were referenced. In addition, Bloomberg sometimes arbitrarily stops indexing new docket entries while a case is in progress, meaning that subsequent docket entries are not returned in searches. Third, opinion collection on Bloomberg, Lexis, and Westlaw is patchy. "Commentators have long warned of the perils of generalizing to the population of all disputes from . . . the mix of published and unpublished cases available through legal research tools such as Westlaw and Lexis."[288] And a 2007 study found that 60% of a sample of summary judgment cases from eight districts were missing from both Lexis and Westlaw.[289] Fourth, there is significant variability in digitization of state records and coverage on Bloomberg and Lexis. Finally, we do not know the proportion of prosecutions in which defendants plead guilty before notice is given, although this number is likely to be very small since notice generally appears to be filed soon after indictment.[290] Despite these caveats, the number of independent sources I searched makes me confident that this is the most comprehensive set of notice recipients ever collected.

B. Recipient Information Collection

My time window was January 1, 1990 to January 1, 2020 to get a full thirty-year period. I included all notices found within that time period, meaning that it was possible for a case to be filed before 1990 or not to have a final judgment by 2020.

I created one row in my dataset per notice recipient. In a given case,

---

(2013) ("[M]andatory electronic docketing within the federal district courts . . . was mostly complete by the mid-2000s . . . .").

[287] Conversation with former DOJ National Security Division employee, *supra* note 65.

[288] Engstrom, *supra* note 286, at 1209 n.24.

[289] *See* Brian N. Lizotte, *Publish or Perish: The Electronic Availability of Summary Judgments by Eight District Courts*, 2007 WIS. L. REV. 107, 130 (2007).

[290] *See, e.g.*, United States v. Yun, No. 5:18-cr-00492 (N.D. Ala. Oct. 11, 2018) (notice filed concurrently with criminal information and plea agreement).

not all defendants may receive notice, and the notice can differ between defendants (e.g., date or FISA provision). In addition, defendants almost always have different counsel, so separating them allows tracking of defense strategy.

Twenty-six cases had duplicated notices from when a case was transferred from a magistrate to a district court judge (e.g., when moving from complaint to information or indictment). I included only the district court case in my dataset so as not to double-count those recipients; the magistrate judge duplicates are stored separately for reference.

I then chose information to collect for each recipient based on what would be useful for advocates and policymakers.

- *Biography*: birth date, gender, nationality, immigration status, and religion.
- *The notice itself*: the date(s) of notice and which FISA provision was used.
- *Charging*: in criminal cases, all charges and whether the defendant appeared on the DOJ National Security Division's international terrorism-related prosecution list.
- *Ideology*: allegedly related groups, whether they were on the State Department's list of Designated Terrorist Organizations, and their ideology.
- *Procedure*: whether a defendant was extradited, whether counsel was retained or appointed, whether CIPA was used, and whether the defendant pleaded guilty or went to trial.
- *Litigation strategy*: whether counsel obtained a security clearance, and whether counsel filed motions to compel disclosure of FISA applications or motions to suppress FISA evidence.
- *Final disposition*: final outcome of the case, any jury verdicts of acquittal, disposition of material support of terrorism charges specifically, and sentence.

I pulled the information from court filings when possible. I then looked to DOJ press releases, before turning to institutional reports and local news sources.

Cases before 2000 rarely have OCR'd docket entries, so text searches do not return any results. Similarly, cases with a docket on LexisNexis but not Bloomberg do not provide access to the underlying docket entry contents. For those cases, I used contemporaneous news articles for information on the defendants and case, but in general, I have

less complete information on how those cases proceeded.

I then computed new columns based on the existing information for each notice recipient. For example, I computed whether a recipient was a "U.S. person" within the meaning of FISA by determining if they were either an American citizen or a legal permanent resident. I computed various helper columns relating to whether multiple FISA provisions were used, or multiple notices given. I also standardized charges, which varied widely in format by jurisdiction and date. This enabled analysis of charges across the entire notice dataset.

The full dataset, both before and after transformations, is publicly available at https://purl.stanford.edu/gw191zv5762. The posted dataset includes a data dictionary that explains the range of possible values for each column, as well as the code used to clean and transform the data.

C. Dataset Representativeness

As discussed above, the notice recipients are almost certainly not representative of all people targeted or spied on under FISA.

One way notice recipients are likely not representative relates to intelligence tactics. Intelligence-gathering through surveillance of foreign officials is not intended to lead to prosecution, so that entire segment of FISA usage is unlikely to appear in the notice pool.[291] Relatedly, prosecution is not always the tool of choice for terrorism investigators, who may prefer to monitor, recruit an informant or double agent, or disrupt by some other means.[292] Surveillance of terrorist suspects may aim to gather intelligence about targets' movements or plans, an initiative unlikely to lead to prosecution if they are abroad.[293]

In addition, since the government only needs probable cause that a target is an agent of a "foreign power" to get a FISA warrant, rather than

---

[291] *See* S. REP. NO. 95-604, pt. I, at 39 (1978), *reprinted in* 1978 U.S.C.C.A.N. 3940–41. ("Although there may be cases in which information acquired from a foreign intelligence surveillance will be used as evidence of a crime, these cases are expected to be relatively few in number, unlike Title III interceptions the very purpose of which is to obtain evidence of criminal activity.").

[292] *The USA Patriot Act in Practice: Shedding Light on the FISA Process: Hearing Before the S. Comm. on the Judiciary*, 107th Cong. (2002) (statement of David Kris, Assoc. Deputy Att'y Gen., Dep't of Just.).

[293] *See* conversation with former DOJ NSD employee, *supra* note 65.

probable cause of participation in criminal activity,[294] many people surveilled will likely not actually be agents of a foreign power or committing a criminal act. While it is possible that the surveillance reveals evidence of another crime and leads to prosecution, most of these false positives that do not lead to actionable intelligence will not receive notice. In both cases, we cannot know whether the group of people surveilled has different characteristics from those prosecuted.

Finally, surveillance targets may not always receive FISA notice even when they are prosecuted. This omission can legitimately occur when there is sufficient independent non-FISA evidence to convict without having to disclose the FISA evidence. More concerningly, this situation can also arise through the use of "parallel construction" and narrow interpretations of the statutory term "derived" to hide FISA use.[295] Federal prosecutors have spoken openly of the "bedrock concept"[296] of parallel construction, a method through which investigators re-obtain evidence using a parallel path of inquiry to obscure the true source of evidence and avoid giving notice. As an example, in 2013, journalists revealed a far-reaching program that distributed NSA surveillance tips to DEA investigators.[297] Agents were trained to "use 'normal investigative techniques to recreate the information provided,'" [298] and taught that the program could not be revealed to prosecutors to avoid "disclosure of these sensitive sources of information in our open, public trial system."[299] This program suggests the broad use of parallel construction to hide surveillance sources. Those defendants are invisible in the notice pool, despite qualifying for notice under the statute. Parallel construction is most likely to skew the dataset by reducing the number of Section 702 notices, and thus

---

[294] *See* 50 U.S.C. § 1805(a)(2)(A); *see also supra* Part III.A for more detail on the "foreign power" requirement.

[295] *See* discussion *supra* Part IV.B.1; Natasha Babazadeh, *Concealing Evidence: "Parallel Construction," Federal Investigations, and the Constitution*, 22 VA. J.L. & TECH. 1, 8 (2018); Amanda Claire Grayson, *Parallel Construction: Constructing the NSA Out of Prosecutorial Records*, 9 HARV. L. & POL'Y REV. S25, S33 (2015).

[296] *See* John Shiffman & Kristina Cooke, *Exclusive: U.S. Directs Agents to Cover Up Program Used to Investigate Americans*, REUTERS (Aug. 5, 2013), www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R20130805 [https://perma.cc/CRB3-DBCN] (quoting a senior DEA official).

[297] *Id*.

[298] *Id*.

[299] Shawn Musgrave, *DEA Teaches Agents to Recreate Evidence Chains to Hide Methods*, MUCKROCK (Feb. 3, 2014), www.muckrock.com/news/archives/2014/feb/03/dea-parallel-construction-guides/ [https://perma.cc/ZZ6J-Z3PC].

the number of incidentally overheard or non-targeted individuals who receive notice, since the government is most interested in hiding newer and more invasive surveillance tools like bulk collection.