2023

Surveillance, State Secrets, and the Future of Constitutional Rights

Laura K. Donohue
Georgetown University Law Center, lkdonohue@law.georgetown.edu

Sup. Ct. Rev. (forthcoming 2023)

SURVEILLANCE, STATE SECRETS, AND THE FUTURE OF CONSTITUTIONAL RIGHTS

Laura K. Donohue*

[Forthcoming in the *Supreme Court Review* (2023)]

I. INTRODUCTION

In 2006, the Federal Bureau of Investigation (FBI) hired Craig Monteilh to become an informant for Operation Flex.[1] The FBI directed him to attend the Islamic Center of Irvine (ICOI), to represent that he wanted to convert to Islam and to record his interactions using audio and video devices they provided.[2] His handlers repeatedly made it clear that they were solely interested in information about Muslims.[3] All "leaders in the Muslim community" constituted "potential threats".[4]

Posing as Farouk al-Aziz, Monteilh subsequently attended classes, collected information about community members, went to daily prayers, memorized verses from the Quran, and tried to obtain compromising information to pressure members to become informants.[5] The FBI directed him to pay particular attention to anyone who was particularly religious or who criticized U.S. foreign policy.[6] He recorded face-to-face meetings with devices secreted in the buttons of his shirt.[7] He left his key fob and mobile phone in prayer rooms, offices, restaurants, cafés, and other areas, allowing him to record conversations when he was not present.[8] Monteilh went through drawers.[9] When directed to date Muslim women, he asked about how he should handle intimacy and was told to "just have sex" with them to obtain more information—which he subsequently did.[10] In addition to going daily to ICOI, he

* Scott K. Ginsburg Professor of Law and National Security, Georgetown Law. Special thanks to Omar Haddad and Wilson Holzhaeuser for their help obtaining many of the materials addressed in this Article. It further benefited from discussions with Parker Rider-Longmaid and Brian Levy, with whom I worked on amicus briefs in *Federal Bureau of Investigation v. Fazaga* and *Wikimedia Foundation v. National Security Agency*, respectively. Geoffrey Stone, Kenneth Karas, Alex Abdo, and Ahilan Arulanantham provided additional, helpful comments on the text, which are much appreciated.

[1] Fazaga v. FBI, 965 F.3d 1015, 1026 (9th Cir. 2020). Monteilh appears to have originally been hired by the FBI in 2003 to become an informant for white supremacist investigations after he connected with the Aryan Brotherhood while serving time in prison; Teresa Watanabe & Scott Glover, *Man Says He Was FBI Informant*, L.A. TIMES, (Feb. 26, 2009), https://www.latimes.com/archives/la-xpm-2009-feb-26-me-informant26-story.html.

[2] *Fazaga*, 965 F.3d at 1026.

[3] *Id.*; Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, ¶¶ 16 (informant directed "to meet and get contact information for a certain number of Muslims per day"), 17 (noting instructions "to gather as much information on as many people in the Muslim community as possible); 18 (directing him to target "anyone who studied *fiqh*, who openly criticized U.S. foreign policy, including the U.S. military's presence in Muslim countries . . . who was an imam or sheikh; who went on *Hajj*; who played a leadership role" etc. and stating that instead of specific targets, his handlers has tasked him with immersing himself in the Muslim community to gather "as much information on as many people and institutions as possible."); 19 (reporting FBI Agent as stating, "We want to get as many files on this community as possible."), https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf.

[4] Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301 ¶ 51.

[5] *Fazaga*, 965 F.3d at 1026-27; Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, ¶ 1, https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf.

[6] Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301 at¶ 18.

[7] *Id*. ¶ 5.

[8] *Id*. ¶¶ 17, 65-67.

[9] *Id*. ¶ 29.

[10] *Id*. ¶ 52.

spent a significant amount of time weekly at nine other area mosques, attending up to four mosques a day.[11]

As a result of Monteilh's actions, the Bureau obtained "hundreds of phone numbers; thousands of email addresses; background information on hundreds of individuals; hundreds of hours of video recordings of the interiors of mosques, homes, businesses, and associations; and thousands of hours of audio recordings of conversations, public discussion groups, classes, and lectures."[12] Apparently, Monteilh was not the only collection source: the FBI informed him that all of the mosques he visited had extensive surveillance equipment already installed.[13] He further learned that the Orange County/Los Angeles Muslim community had been "saturated" by other informants, at a level commensurate with East Germany during the Cold War, and Cuba.[14] Similar operations were underway in New York and Dearborn, Michigan.[15]

This information is public. It derives from statements by FBI Agents in other cases, Monteilh's sworn declarations, Ninth Circuit adjudication, and media reports, and it raises significant concern about whether and how the FBI is using the Foreign Intelligence Surveillance Act (FISA). It indicates that the Bureau may have acted outside either the ordinary criminal Title III warrant procedure or the statutory limitations in FISA to place entire religious communities under electronic surveillance.[16] By the FBI handlers' admission, there was no pre-existing criminal warrant—according to Monteilh, they indicated that they "could get in a lot of trouble if people found out what surveillance they had in the mosques."[17] One handler suggested that national security investigations do not require any warrant: all its absence means is that the FBI cannot use the information in court. But they can still collect it.[18]

Taking the facts at face value, it would be hard to imagine a more troubling disregard for statutory provisions, as well as constitutional rights enshrined in the first and fourth amendments of the Constitution and secured by the fifth amendment due process clause. Yet the government's position in the case is that it cannot defend itself without recourse to state secrets and, in a radical departure from how the privilege has been understood for centuries, the Court should dismiss the case at the pleadings stage. Its argument turns what, since the Founding of the United States, has been a common law evidentiary rule into a justiciability standard.

Decided on alternate grounds and sent back to the Ninth Circuit for further consideration, the Supreme Court's 2022 decision in *Federal Bureau of Investigation v. Fazaga* heralds a worrying trend.[19] Over past 15 years, as more information about how the government wields its foreign intelligence collection authorities on U.S. soil has become available, it has become clear that the government has repeatedly acted outside its constitutional and statutory limits and at

---

[11] *Fazaga*, 965 F.3d. at 1026-27; Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, ¶ 26, https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf.

[12] *Fazaga*, 965 F.3d at 1027; *See also* Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, ¶ 71, https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf

[13] *Id.* ¶ 28.

[14] *Id.* ¶ 58.

[15] *Id.* ¶ 19.

[16] *See* discussion Part V (infra).

[17] Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, ¶¶ 17, 28, https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf

[18] *Id.* ¶ 67.

[19] *See* Federal Bureau of Investigation v. Fazaga, 142 S. Ct. 1051 (2022).

times in flagrant disregard for judicial orders.[20] As a result, dozens of cases challenging surveillance have been making their way through the courts.[21] Unlike in prior eras, in certain cases it has become easier in light of the information available and the programmatic nature of collection for litigants to establish an injury-in-fact. In response, the government has crafted a new state secrets analysis, raised the privilege early in litigation to have suits dismissed, broadened its assertion to encompass entire categories of information, and claimed what for centuries has been a common law rule as an Article II constitutional power.[22] Because of the government's shift, what is now at stake is the possibility of any litigant to ever challenge illegal and unconstitutional surveillance. *Fazaga* represents the tip of the iceberg in terms of the risks to individual rights that would follow, should the government ultimately prevail.

This Article begins by according three developments a central role in elevating the evidentiary base on which litigants can rely. First, following the release of classified materials by the media and the government, more information about how the government has been interpreting its legal authorities and what programs are underway is now available. It shows that the *way* in which the intelligence community collects communications has shifted, making it easier to demonstrate an injury-in-fact. Second, parallel efforts to obtain information via the Freedom of Information Act (FOIA) about domestic foreign intelligence collection has forced thousands of more documents into the public domain, providing a factual basis for suits to progress. Third, this information indicates that the government routinely exceeds its constitutional and statutory limits, prompting judicial challenge. With standing met, the government is falling back on a re-interpretation of state secrets to avoid Article III adjudication.

The Article next turns to *Fazaga*, detailing the question addressed by the Supreme Court: whether certain provisions in FISA displaced the state secrets privilege. Siding with the government, the Supreme Court determined that it did not

---

[20] *See, e.g.*, Memorandum Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00050 (FISA Ct. 2009) (Hogan, J.), at 11-13, https://www.dni.gov/files/documents/icotr/702/EFF%2016-CV-02041(HSG)%20Doc%2005%2006.13.17%20--%20REDACTED.PDF (NSA analysts improperly acquiring U.S. persons' communication; CIA exhibiting a "profound misunderstanding of minimization procedures" and inappropriately disseminating reports containing USP information to NSA, FBI, and DOJ; and FBI failing to report compliance incidents to the Court in violation of Rule 10(c) of the Foreign Intelligence Surveillance Court Rules of Procedure); Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00138 (FISA Ct.) (Hogan, J.), https://www.dni.gov/files/documents/icotr/08202018/0820218_Document-27.pdf (government conducted unauthorized surveillance); Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00254 (FISA Ct.) (Hogan, J.), https://assets.documentcloud.org/documents/4780432/EFF-Document-2.pdf (holding that NSA's acquisition of [Redacted] constitutes unauthorized electronic surveillance because it failed to comply with 50 U.S.C. §1804(a)(2) and (a)(3)(B)); Memorandum Opinion and Order, *[REDACTED]*, No. [REDACTED] (FISA Ct. Nov. 18, 2020) (Boasberg, J.), at 41, 43, 49-50, https://www.intel.gov/assets/documents/702%20Documents/declassified/20/2020_FISC%20Cert%20Opinion_10.19.2020.pdf, (stating that the Court it "continues to be concerned about FBI querying practices involving U.S.-person query terms, including (1) application of the substantive standard for conducting queries; (2) queries that are designed to retrieve evidence of crime that is not foreign-intelligence information; and (3) recordkeeping and documentation requirements." And noting that it would "continue to closely monitor the government's reporting in order to evaluate whether the querying procedures are being implemented in a manner consistent with the statute and the Fourth Amendment.")

[21] *See, e.g.*, Wikimedia Foundation v. National Security Agency/Central Security Service, 14 F.4th 276 (4th Cir. 2021); In re Terrorist Attacks on September 11, 2001, 523 F.Supp.3d 478 (S.D.N.Y. 2021); Page v. Comey, No. 20-CV-3460 (DLF), 2022 WL 3981135 (D.D.C. Sept. 1, 2022); Trump v. Clinton, No. 22-CV-14102, 2022 WL 4119433 (S.D. Fla. Sept. 8, 2022).

[22] For a detailed discussion of how state secrets evolved from 2001 to 2010, *see* Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77 (2010).

and remanded the case for determination of the state secrets assertion. In doing so, the Court sidestepped the most important question: whether the government can avoid accountability when it acts in apparent disregard of acts of Congress as well as Americans' first, fourth, and fifth amendment rights. This question will not go away: it already is up in a parallel case on a petition of certiorari.[23]

The Article highlights the novel theory of state secrets being advanced in *Fazaga* and dozens of parallel cases, noting that it departs in four critical ways from how, for centuries, state secrets has operated. First, the government has collapsed the *Reynolds* evidentiary rule and *Totten* contractual bar by re-casting the latter in terms of a "very subject matter" analysis.[24] This change discards the entire point of *Totten*: that parties entering into a secret contractual relationship with the government have *ex ante* notice that future disputes are unlikely to be addressed in open court. In other words, *the contract itself*, contains the understanding that confidentiality will be maintained. This rule does not apply to situations where the government acts unilaterally: neither have both parties agreed, nor has notice been served in regard to the unavailability of judicial redress should a pre-existing contract be breached. Second, the government is asserting the privilege early in suits to request dismissal, instead of employing it as part of discovery or at the merits stage to exclude evidence. Third, it has adopted an overbroad approach, asserting state secrets not over particular documents, but instead over broad categories of information. Such assertions sweep in a significant amount of information already in the public domain and often do not withstand judicial scrutiny. Fourth, the government is attempting to transform a common law rule into a constitutional power, increasingly claiming that it derives from the executive's Article II authorities.

The Article concludes by emphasizing the implications of the government's re-casting of state secrets. What is at stake in *Fazaga* extends well beyond the case to protecting the rights of the People against government malfeasance as well as the ability of the democratic structures to hold the executive branch to account.

II. PROGRAMMATIC SURVEILLANCE AND STANDING

Programmatic surveillance has long been a feature of U.S. intelligence collection.[25] The stakes are high: on the one hand, information gleaned may help to detect and mitigate national security threats. In an age of weapons of mass destruction, the costs of failing to do so may be catastrophic. On the other hand, directed against U.S.

---

[23] *See* Petition for Writ of Certiorari, Wikimedia Foundation v. National Security Agency/Central Security Service, et al., 14 F.4th 276 (No. 22-190).

[24] *See* United States v. Reynolds, 345 U.S. 1 (1953); Totten v. United States, 92 U.S. 105 (1875).

[25] *See, e.g.*, S. Select Comm. to Study Governmental Operations with Respect to Intel. Activities 1975-76, (Church Committee) Final Report, S. Rep. No. 94-755, at 21 (1976), Book II, Intelligence Activities and the Rights of Americans (recounting CIA, NSA, and FBI warrantless collection of domestic and international communications 1936-1976 and noting, "[s]ince the re-establishment of federal domestic intelligence programs in 1936, there has been a steady increase in the government's capability and willingness to pry into. . . the political activities and personal lives of the people. The last forty years have witnessed a relentless expansion of domestic intelligence activity." (p. 21)). *See also* Commission on CIA Activities within the United States, 1975 (Rockefeller Commission), pp. 101-115 (detailing numerous CIA mail intercept programs dating back to the 1950s), pp. 116-129 (discussing CIA collection of information on anti-war activists and dissidents in the 1960s and 1970s), pp. 130-150 (examining CIA and FBI participation in Operation CHAOS 1967-74); Interception of International Telecommunications by the National Security Agency, Report by the Committee on Government Operations, (Pike Committee), pp. 5-11 (discussing operation of the Black Chamber 1919-1929, which analyzed cables obtained from Western Union Telegraph Company and the Postal Telegraph Company); pp. 11-25 (detailing the collection of international telecommunications traffic 1945-1975 by the Army Signal Security Agency and later the National Security Agency); pp. 975-1018 (addressing the Drug Enforcement Administration's domestic and international intelligence programs); pp. 1019-1086 (highlighting the FBI Domestic Intelligence programs).

citizens, such programs may threaten foundational constitutional rights by chilling freedom of speech, religion and association, violating the right to privacy, and running roughshod over the right against self-incrimination—to say nothing of due process concerns. Accordingly, the revelation that the government is collecting information on citizens is often accompanied by efforts to hold the government to account.

Following disclosures by President Ford's Commission on CIA Activities Within the United States, for instance, twenty-one individuals and five anti-war organizations brought suit against officials in the CIA, FBI, Department of Defense, and Secret Service asserting violation of their first, fourth, fifth, and ninth amendment rights.[26] As soon as the *New York Times* revealed that in the aftermath of the Sept. 11, 2001 attacks President George W. Bush had authorized warrantless surveillance, lawsuits alleging a range of constitutional violations mounted.[27] Just over a month after the attack, the Center for Constitutional rights filed the first action.[28] By February, two more cases had been filed.[29] In May, another 27 cases were filed, with six more in June.[30] As the filings picked up steam, by August 2006, a multidistrict panel had ordered the consolidation of more than 50 cases and their transfer to the Northern District of California.[31] The release of the Snowden documents and the revelation that the government was conducting bulk collection under Section 215 of the USA PATRIOT Act proved no different.[32]

Historically, though, the case or controversy requirement often prevented suits from moving forward: it could be devilishly difficult to establish an injury-in-fact when the underlying documents were classified. Following the release of government documents by the media in June 2013, subsequent declassification, and successful FOIA litigation, however, the context changed. The documents revealed the breadth of surveillance underway as well as a government acting outside statutory and constitutional limits. With litigants increasingly able to demonstrate standing, the government turned to state secrets as a way to head off litigation.

A. The Shoals of Standing

In 1992 in *Lujan v. Defenders of Wildlife*, the Supreme Court articulated the three part-test for standing:

> First, the plaintiff must have suffered an "injury in fact" — an invasion of a legally protected interest which is (a) concrete and particularized, [] and (b) "actual or imminent, not 'conjectural' or 'hypothetical,'" [] Second, there must be a causal connection between the injury and the conduct complained of — the injury has to be "fairly . . . trace[able] to the challenged action of the defendant, and not . . . th[e] result [of] the independent action of some third

[26] Halkin v. Helms, 690 F.2d 977, 981 (D.C. Cir. 1982).
[27] *See* James Risen and Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, (Dec. 16, 2005), https://www.nytimes.com/2005/12/16/politics/bush-lets-us-spy-on-callers-without-courts.html (stating that Bush had signed a presidential order in 2002 giving NSA the authority to monitor international telephone calls and international email messages "of hundreds, perhaps thousands, of people inside the United States without warrants over the past three years in an effort to track possible 'dirty numbers' linked to Al Qaeda").
[28] Complaint at 1, Ctr. For Const. Rights v. Bush, No. 06-00313 (N.D. Cal. Jan. 17, 2006).
[29] *See* Hepting v. AT&T, 439 F.Supp.2d 974 (N.D. Cal. 2006); complaint, Al-Haramain Islamic Found., Inc. v. Bush, 451 F.Supp. 2d 1215 (D.Or. 2006) (No. 06-0274).
[30] *See generally* Donohue, *supra* note 22, at 148.
[31] *Id.* at 149.
[32] *See* 50 U.S.C. § 1861 and discussion, *infra*.

> party not before the court." [] Third, it must be "likely," as opposed to merely "speculative," that the injury will be "redressed by a favorable decision."[33]

To meet the first criteria, plaintiffs in surveillance cases have to be able to demonstrate that *their* communications in particular are being monitored and/or collected. The mere existence of a program, in the past, has generally proven insufficient. Lacking access to classified information, it could be extremely difficult to make the case for standing.

In the 1982 case *Halkin v. Helms*, for example, the D.C. Circuit noted that just because individuals found themselves on a watch list (in this case, Operation MINARET), it did not necessarily mean that their communications had been collected.[34] Without being able to demonstrate actual interception, the program's constitutionality could not be challenged.[35] Similarly, following revelation of STELLARWIND, residential telephone customers brought a class action against government agencies and officers, raising first and fourth amendment claims, and asserting, *inter alia*, violation of separation of powers.[36] Chief Judge Vaughn R. Walker of the Northern District of California dismissed the suit on the grounds that neither the plaintiffs nor their purported class representatives had alleged a sufficiently particular injury.[37] Generalized harm would not suffice. In a parallel case, plaintiffs in regular communication with individuals overseas filed a suit in Michigan, asserting a first and fourth amendment challenge, as well as violation of separation of powers. The Sixth Circuit dismissed the suit on grounds that the plaintiffs lacked standing.[38]

Even where statutory language has been introduced to govern programmatic collection, the standing bar has proven high. In 2008, Congress added FISA Section 702.[39] The provision empowered the Attorney General in conjunction with the Director of National Intelligence (DNI) to place non-U.S. persons reasonably believed to be outside the United States under surveillance.[40] Human rights, labor, legal, and media organizations in contact with individuals they believed to be likely targets brought suit on fourth amendment grounds.

Justice Alito, writing for the Supreme Court in 2013 in *Clapper v. Amnesty International*, dismissed the case for lack of standing: "[R]espondents' theory of *future* injury is too speculative to satisfy the well-established requirement that the threatened injury must be 'certainly impending.'"[41] Even if such certainty could be established, it could not be demonstrated that such injury was "fairly traceable" to the statutory authority.[42] Nor could respondents avail themselves of the argument that they had already had to adopt "costly and burdensome measures to protect the confidentiality of their international communications.[43] The respondents could not

---

[33] Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-561 (1992) (internal citations omitted).
[34] Halkin v. Helms, 690 F.2d 977, 998 (D.C. Cir. 1982).
[35] *Id.*
[36] Complaint, Jewel v. NSA, MDL Docket No. C 06-1791 VRW, Jan. 21, 2010, 2010 WL 235075.
[37] *Id*., at *1. *Cf.* Shubert et al v. Obama et al, C 07-0693 Doc. #38 (MDL Doc. #680). *But see* Jewel v. National Security Agency, 673 F.3d 902 (9th Cir. 2011) (finding standing and remanding for consideration of state secrets assertion).
[38] ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007). *Cf.* In re Telecommunications Records Litig., 522 Fed.Appx.383 (9th Cir. 2013) (applying *Clapper* to dismiss plaintiff's claims on the grounds that they lacked actual knowledge of the Government's targeting practices). *See also* Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190 (1205) (9th Cir. 2007) (suit dismissed on grounds that standing not met).
[39] FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.
[40] *See* 50 U.S.C. §1881a.
[41] Clapper v. Amnesty Int'l, 568 U.S. 398, 401 (2013) (Alito, J.) (emphasis in original).
[42] 568 U.S. at 402 (Alito, J.).
[43] *Id.*

"manufacture standing by choosing to make expenditures based on hypothetical future harm that is not certainly impending."[44] Should the government elect to use FISA-derived information in a criminal trial, it would have to provide advance notice, giving the affected person the opportunity to challenge the lawfulness of the acquisition.[45]

In making this last assertion, the Court relied on statutory provisions (which require the government to notify anyone against whom any information obtained from electronic surveillance has been used), as well as repeated representations to the Court by the U.S. Solicitor General that the Department of Justice (DOJ) would so notify individuals.[46] This representation turned out to be false.[47] Not only was it not the practice of the DOJ to inform defendants that FISA had played a role in their case, but law enforcement agencies had been trained to use "parallel construction" to shape evidentiary chains to ensure that neither the prosecution nor the defense would know that the information leading to a criminal case derived from FISA-related surveillance.[48] With such policies in place, standing, and the ability of citizens to pursue their constitutional claims, proved elusive.

B. Primary Solidification of the Injury-in-fact Requirement

Less than four months after *Clapper*, *The Guardian* and other newspapers began publishing information obtained by Edward Snowden, a former National Security Agency (NSA) contractor.[49] Drawing further on investigative reporting,

---

[44] *Id.*

[45] *Id.* at 421. ("[I]f the Government intends to use or disclose information obtained or derived from a §1881a acquisition in judicial or administrative proceedings, it must provide advance notice of its intent, and the affected person may challenge the lawfulness of the acquisition.").

[46] *See* 50 U.S.C. § 1806(c). During oral argument, Justice Sotomayor asked, "General, is there anybody who has standing?" She continued, "As I read your brief, standing would only arise at the moment the government decided to use the information against someone in a pending case. To me, that [] would seem to say that the Act. . . if there was a constitutional violation in the interception, that no one could ever stop it until they were charged with a crime, essentially." Transcript at 3-4, Clapper v. Amnesty Int'l, 568 U.S. 398 (No. 11-1025), https://www.supremecourt.gov/oral_arguments/argument_transcripts/2012/11-1025.pdf. Don Verelli, the Solicitor General, replied with a "clear example" of a situation in which litigants would have standing: namely, where "an aggrieved person, someone who is a party to a communication, gets notice that the government intends to introduce information in a proceeding against them. They have standing. That standing could include a facial challenge like the one here." *Id.* at 4. Similarly, in his brief to the court, the Solicitor General argued in response to Amnesty International's argument that failure to find standing would result in immunizing section 702 from constitutional challenge: "That contention is misplaced. Others may be able to establish standing even if respondents cannot. As respondents recognize, the government must provide advance notice of its intent to use information obtained or derived from" 702 "against a person in judicial or administrative proceedings and that person may challenge the underlying surveillance." 568 U.S. 398 at 401.

[47] *See* Adam Liptak, *A Secret Surveillance Program Proves Challengeable in Theory Only*, N. Y. TIMES (July 15, 2013). At the time the Solicitor General made his representation, no criminal defendant had ever received notice of Section 702 surveillance. After the New York Times article was published, the government issued five notices Oct. 2013 to April 2014—including for cases in which individuals had already been tried and convicted. After that, however, the notices stopped for nearly two years. *See* Patrick Toomey, *Why Aren't Criminal Defendants Getting Notice of Section 702 Surveillance – Again?*, JUST SECURITY, (Dec. 11, 2015).

[48] *See generally* Responsive Documents, Drug Enforcement Admin., MUCKROCK, http://www.documentcloud.org/documents/1011382-responsivedocuments.html#document/p9.

[49] *See*, e.g., Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN, (June 6, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order; Charlie Savage, *NSA Said to Search Contents of Messages To and From America*, N.Y. TIMES, (Aug. 8, 2013), https://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html#:~:text=WASHINGTON%20%E2%80%94%20The%20National%20Security%20Agency,surveillance%2C%20according%20to%20intelligence%20officials.; Barton Gellman & Ashkan

these articles revealed the surprising scope of surveillance then underway.[50] The public outcry that followed stemmed from deep concern about the impact of the programs on Americans' constitutional rights. The Privacy and Civil Liberties Oversight Board (PCLOB), previously floundering, suddenly took form, held hearings, and issued a scathing report on the government's use of FISA.[51] Congress held dozens more hearings, calling government officials to testify to ensure that legislators had full information about the extent of the programs that had been secretly operating for years, collecting American's telephony and internet metadata and content without their knowledge. From three bills on FISA the prior year (when three of the statute's provisions had been due to sunset), over the twelve months following Snowden's disclosures, Congress considered forty-two different bills, with proposed amendments to foreign intelligence collection ranging from radical restructuring of the Foreign Intelligence Surveillance Court (FISC) to defunding and withdrawing surveillance authority.[52]

Such was the tenor of the public outrage that the government immediately had to respond. The administration first tried to correct the record by issuing statements and documents to offset the information being leaked and the accompanying news articles.[53] President Barak Obama next directed DNI James Clapper to declassify and

---

Soltani, *NSA Collects Millions of Email Address Books Globally*, WASH. POST, (Oct. 14, 2013), https://www.washingtonpost.com/world/national-security/nsa-collects-millions-of-e-mail-address-books-globally/2013/10/14/8e58b5be-34f9-11e3-80c6-7e6dd8d22d8f_story.html.

[50] *See, e.g.*, Barton Gellman & Ashkan Soltani, *NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say*, WASH. POST, (Oct. 30, 2013), https://www.washingtonpost.com/world/national-security/nsa-infiltrates-links-to-yahoo-google-data-centers-worldwide-snowden-documents-say/2013/10/30/e51d661e-4166-11e3-8b74-d89d714ca4dd_story.html; Barton Gellman & Ashkan Soltani, *NSA Tracking Cellphone Location Worldwide, Snowden Documents Show*, WASH. POST, (Dec. 4, 2013), https://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html; Nicole Perlroth, Jeff Larson, & Scott Shane, *NSA Able to Foil Basic Safeguards of Privacy on the Web*, N.Y. TIMES, (Sept. 5, 2013) https://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html; Glenn Greenwald & Ryan Grim, *Top-Secret Document Reveals NSA Spied on Porn Habits As Part of Plan to Discredit "Radicalizers",* HuffPost, (Nov. 26, 2013), https://www.huffpost.com/entry/nsa-porn-muslims_n_4346128; Siobhan Gorman, *NSA Officers Spy on Love Interests*, WALL ST. J., (Aug. 23, 2013), https://www.wsj.com/articles/BL-WB-40005.

[51] *See* Privacy and Civil Liberties Oversight Board, Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign. Intelligence Surveillance Court, (Jan. 23, 2014), https://documents.pclob.gov/prod/Documents/OversightReport/ec542143-1079-424a-84b3-acc354698560/215-Report_on_the_Telephone_Records_Program.pdf.

[52] *See, e.g.*, 159 Cong. Rec., 12237 (2013) (debating whether to prohibit certain kinds of collection under FISA and to defund section 215 collection).

[53] *See, e.g.*, Press Release, Joint Statement: NSA and Office of the Director of National Intelligence (Aug. 22, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/917-joint-statement-nsa-and-office-of-the-director-of-national-intelligence (stating that an article published in the *Wall Street Journal* mischaracterized the NSA's Section 702 collection activities); Press Release, DNI Statement on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Jun 8, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/872-dni-statement-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act (criticizing the *Guardian* and the *Washington Post* for not providing the "full context" of the programs underway resulting in "significant misimpressions" and "inaccuracies"); Press Release, DNI Statement on Activities Authorized Under Section 702 of FISA (June 6, 2013) (stating that the *Guardian* and *Washington Post* articles "contain numerous inaccuracies"); Press Release, DNI Statement on Recent Unauthorized Disclosures of Classified Information (Jun 6, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/868-dni-statement-on-recent-unauthorized-disclosures-of-classified-information (the *Guardian* "article omits key information regarding how a classified intelligence collection program is used to prevent terrorist attacks and the numerous safeguards that protect privacy and civil liberties.") *See also* Press Release,

make certain information about FISA surveillance programs public—which he did.[54] Obama then constituted a Review Board to examine foreign intelligence collection and to consider the best course of action to respond to the concerns raised.[55]

The cumulative result of these actions was the infusion of a tremendous amount of previously classified material into the public discourse, providing details about the breadth of the surveillance programs underway.[56] Lawsuits, representing a range of political views, demographics, and professional interests, quickly followed. Less than a week after the first Snowden release and the Obama Administration's response, for instance, the ACLU filed suit in the Southern District of New York.[57] The following day, Anna Smith, a nurse and mother of two children, filed suit in Idaho,[58] as did conservative former DOJ prosecutor Larry Klayman in the D.C. District Court.[59] Within a month, the Electronic Privacy Information Center had filed

---

Facts on the Collection of Intelligence Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (Jun 8, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/871-facts-on-the-collection-of-intelligence-pursuant-to-section-702-of-the-foreign-intelligence-surveillance-act; Administration White Paper: Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act (Aug. 9, 2013), https://irp.fas.org/nsa/bulk-215.pdf.

[54] *See, e.g.*, Press Release, DNI Announces the Declassification of the Existence of Collection Activities Authorized by President George W. Bush Shortly After the Attacks of September 11, 2001, (Dec. 21, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/991-dni-announces-the-declassification-of-the-existence-of-collection-activities-authorized-by-president-george-w-bush-shortly-after-the-attacks-of-september-11-2001; Press Release, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Nov. 18, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/964-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act; Press Release, DNI Clapper Declassifies Additional Intelligence Community Documents Regarding Collection Under Section 501 of the Foreign Intelligence Surveillance Act (Oct. 28, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/954-dni-clapper-declassifies-additional-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act; Press Release, DNI Clapper Declassifies Intelligence Community Documents Regarding Collection Under Section 5 of the Foreign Intelligence Surveillance Act (FISA) (Sept. 10, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/927-dni-clapper-declassifies-intelligence-community-documents-regarding-collection-under-section-501-of-the-foreign-intelligence-surveillance-act-fisa; Press Release, DNI Clapper Directs Annual Release of Information Related to Orders Issued Under National Security Authorities (Aug. 30, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/922-dni-clapper-directs-annual-release-of-information-related-to-orders-issued-under-national-security-authorities; Press Release, DNI Clapper Declassifies and Releases Telephone Metadata Collection Documents (July 31, 2013), https://www.dni.gov/index.php/newsroom/press-releases/press-releases-2013/item/908-dni-clapper-declassifies-and-releases-telephone-metadata-collection-documents. Starting in 2014, the DNI began annually issuing a Statistical Transparency Report Regarding the government's use of national security authorities. *See* Statistical Transparency Report Regarding Use of National Security Authorities: Annual Statistics for Calendar Year 2013 (2014).

[55] *See* Liberty and Security in a Changing World: Report and Recommendations of The President's Review Group on Intelligence and Communications Technologies, (Dec. 12, 2013), https://www.justsecurity.org/wp-content/uploads/2013/12/2013-12-12_rg_final_report.pdf.

[56] For a compilation of the NSA documents released in 2013 alone, *see* American Civil Liberties Union, NSA Documents Released to the Public Since June 2013, https://www.aclu.org/nsa-documents-released-public-june-2013.

[57] Complaint, American Civil Liberties Union v. Clapper, Docket No. 1:13-cv-03994 (S.D.N.Y. Jun 11, 2013).

[58] Complaint, Smith v. Obama et al, Docket No. 2:13-cv-00257 (D. Idaho Jun 12, 2013).

[59] Complaint, Klayman et al v. Obama et al, Docket No. 1:13-cv-00881 (D.D.C. Jun 11, 2013). *See also* Jerry Markon, *Northern Idaho Mom Sues President Over Government Surveillance Program*, WASH. POST, (July 25, 2013), https://www.washingtonpost.com/politics/northern-idaho-mom-sues-president-over-government-surveillance-program/2013/07/25/4994d1d4-f092-11e2-bed3-b9b6fe264871_story.html.

a writ of mandamus before the Supreme Court, seeking an end to bulk collection.[60] Churches, telephone service providers, and even members of Congress stepped up, seeking to stop what they alleged was a gross violation of their constitutional rights.[61]

In contrast to prior eras, standing no longer proved insurmountable. What had changed was not the mere existence of programmatic (or bulk) collection, but the information available. What it revealed about the processes mattered. In an era of global communications, the *way* in which surveillance was being given effect—such as sitting on the backbone of the internet and scanning all traffic as it crossed certain points (Upstream), or by collecting information in bulk about internet service providers customers (PRISM), made it easier to demonstrate that it was highly likely that plaintiffs' communications were being monitored by the government. In case after case, the courts began to find that plaintiffs had standing.[62]

C. Secondary Stream: Freedom of Information Act Litigation

While the release of documents directly linked to the media coverage that started in June 2013 provided the primary grounds for the shift in standing, parallel developments in the FOIA realm provided a second, powerful force and demonstrated a judiciary increasingly reluctant to give the executive branch a free pass. The government was far from cooperative. It initially ignored formal requests for more details about these programs. When brought into court, the government fought vigorously, asserting FOIA Exemptions 1(A), (3), (5), (6), and 7(A), (C), (D), and (E).[63] The government even went so far as to argue to the FISC that it should not allow a suit to proceed because the litigants could use FOIA to seek access to FISC opinions in a district court, only to then show up in a district court to argue that FOIA could *not* be used to obtain FISC opinions.[64] But non-specialized Article III courts

[60] Petition for a Writ of Mandamus and/or Prohibition, In Re Electronic Privacy Information Center, No. 13-58, July 8, 2013.

[61] *See, e.g.*, First Unitarian Church of Los Angeles et al v. National Security Agency et al, Docket No. 4:13-cv-03287 (N.D. Cal. Jul 16, 2013); In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things, Op. and Order, Docket No. BR 14-01, FISC, (Mar. 20, 2014); Ellen Nakashima, *Surveillance Court Rejected Verizon Challenge to NSA Calls Program*, WASH. POST, (Apr. 25, 2014), https://www.washingtonpost.com/world/national-security/surveillance-court-rejected-verizon-challenge-to-nsa-calls-program/2014/04/25/78d430c2-ccc2-11e3-93eb-6c0037dde2ad_story.html; Complaint, Paul et al v. Obama et al, Docket No. 1:14-cv-00262 (D.D.C. Feb 18, 2014).

[62] *See, e.g.*, Klayman v. Obama, 957 F.Supp.2d 1 (D.D.C. 2013) (finding standing), vacated by Obama v. Klayman, 800 F.3d 559 (D.C. Cir. 2015); Smith v. Obama, 24 F.Supp.3d 1005 (D. Id. 2014) (finding standing); Smith v. Obama, 816 F.3d 1239 (9th Cir. 2016) (finding standing); ACLU v. Clapper, 959 F.Supp.2d 724 (S.D.N.Y. 2013) (finding standing); ACLU v. Clapper, 785 F.3d 787 (2d Cir. 2015) (finding standing); Schuchardt v. President of the United States, 839 F.3d 336 (3d Cir. 2016) (finding standing); Wikimedia v. NSA/CSS, 14 F.4th 276 (4th Cir. 2021) (finding standing)..

[63] The most common FOIA exemptions asserted in the national security context include 5 U.S.C. § 552(b)(1) (materials authorized by Executive Order to be kept secret in the interest of national defense or foreign policy and properly classified under such order); 5 U.S.C. § 552(b)(3) (exempting material specified by statute, including, in the national security context, material specified un- der the National Security Act of 1947 as amended); 5 U.S.C. § 552(b)(5) (inter-agency or intra-agency memoranda or letters); 5 U.S.C. § 552(b)(6) (personnel files); 5 U.S.C. § 552(b)(7) (records or information compiled for law enforcement purposes).

[64] *Compare* Gov's Opp. Br. at 5, In re Motion for Release of Court Records, No. Misc. 07-01 (FISC) ("The ACLU can use FOIA [] to seek access to FISC orders and Government briefs in the Executive's possession. The FOIA process . . . is the proper means for the ACLU to seek records of [the FISC's] proceedings form the Executive Branch. Moreover, FOIA's judicial remedies must be sought only in district court, not in [the FISC].") *and* Declaration of Mark A. Bradley ¶ 7, *Elec. Frontier Found. v. DOJ*, 57 F. Supp. 3d 54 (D.D.C. Apr. 1, 2013) (No. 12-1441-ABJ), ECF No. 11-3; Department of Justice's Statement of Material Facts Not in Genuine Dispute at 3, *Elec. Frontier Found. v. DOJ*, 57 F. Supp. 3d 54 (D.D.C. Apr. 1, 2013) (No. 12-1441-ABJ), ECF No. 11-2 (arguing that FISC opinions were not available via FOIA because FISC had not ordered their publication). The

became less and less enamored of the government's overbroad assertions. As a result, significantly more documents ended up being released.

In 2011, for instance, when the ACLU submitted a FOIA request for records concerning the government's interpretation or use of Section 215, the government produced just three documents in response.[65] Once the ACLU filed suit, the government produced some more documents.[66] Following the *Guardian's* publication of the FISC Order directing Verizon to provide telephony metadata on a daily basis, a federal district court ordered the government to see if there was anything else that could be released.[67] This time, the government released *over 1,000 pages* of material.[68] In 2014, the ACLU narrowed its request to any fully withheld FISC opinions related to bulk collection. The government responded by providing a Vaughn index with eight more entries, and an unspecified number of documents.[69]

The federal district court was irate: "[B]y advancing incorrect and inconsistent arguments, the Government acted without the candor this Court expects from it."[70] It noted, "The Government's argument that it believed until June 2013 that FISC orders could not be produced in response to FOIA requests strains credulity."[71] The government's "assertion on the initial summary judgment motion . . . was incorrect. And it then failed to produce or list on the Vaughn index three documents which the Government had disclosed elsewhere."[72] The court continued,

> These inconsistencies shake this Court's confidence in the Government's submissions. The deference the Government ordinarily receives in FOIA cases is rooted largely in the courts' trust that the Government will comply with its statutory obligations. That compliance is not apparent here.[73]

Following the Snowden leaks, the government continued to stonewall. In January 2015, for example, the *New York Times* submitted a FOIA request to the NSA to obtain information about the agency's collection activities under FISA Amendments Act Section 702 and its predecessor, the Protect America Act; bulk phone records collection activities under Section 215 of the USA PATRIOT Act, and bulk Internet metadata collected under the FISA pen register/trap and trace provisions. The NSA did not respond. On March 31, 2015, the newspaper filed suit.

---

government's position is that because the FISC's rulings contain classified information, only the government can decide when to make them public. *See*, e.g., U.S. Reply Brief, In re Certification of Questions of Law to the FISCR, 18-01 (FISA Ct. Rev. Mar. 5, 2018, pp. 6-7) ("Movants would place in the FISC the power to make independent national security judgments and to order the release of information that the Executive Branch has properly classified pursuant to its constitutional power. …[T]his claim of unilateral FISC power to override the Executive's classification decisions is completely devoid of merit."); *id.* at 21 ("[T]he powers 'to classify and control access to information bearing on national security' are constitutionally committed to the Executive Branch, necessarily granting the Executive 'broad discretion to determine who may have access' to national security information."). The government's argument relies on a mis-characterization of *Dep't of Navy v. Egan*, a case in which the Court held that a particular statute did not give the Merit Systems Protection Board (an Article II tribunal) control over security clearance determinations. *See Dep't of the Navy v. Egan*, 484 U.S. 518, 530-32 (1988).

[65] ACLU v. FBI, 59 F.Supp.3d 584, 586 (S.D.N.Y. 2014).

[66] *Id.* at 587.

[67] *Id*.

[68] *Id.* at 588.

[69] *Id.* at 588.

[70] *Id.* at 591.

[71] *Id*.

[72] *Id.* at 591-2.

[73] *Id.* at 592.

Over the course of litigation, despite repeated invocation of national security exceptions, the government was ultimately forced to make hundreds of pages of information public, including, *inter alia*, reports on overcollection, purging of files, and assessing how effectively management controlled collection under the programs.[74] Similar efforts by the Electronic Frontier Foundation (EFF) eventually led to the declassification and public release of *more than 1,000 pages* responsive to the plaintiff's FOIA request—but only after the court stood up to the government's overbroad assertions.[75]

Many documents over which the government asserted national security exceptions related to routine matters of law. In one case, the government had withheld Westlaw printouts, summaries of FISC legal opinions, descriptions of the scope of the FISC's jurisdiction, and discussions of FISA process improvements.[76] The federal district court noted that DOJ had failed to address why such materials could not be released and required further declarations tailored to the withholdings in question. The government, accordingly, narrowed its claims—a pattern repeated throughout the case as challenges to withheld material arose.[77]

In addition to releasing more documents, FOIA suits also resulted in narrowing redactions. In 2012, for example, EFF submitted a FOIA request to DOJ's National Security Division (NSD).[78] EFF requested any written opinion or order where the FISC had held that collection was unreasonable under the fourth amendment or implementation had circumvented the spirit of the law, and any briefing to the Senate Select Committee on Intelligence (SSCI) and the House Permanent Select Committee on Intelligence. The government identified five responsive documents, withholding two in full and redacting the remaining three.[79] Following the 2013 public outcry, the government declassified and redacted all of them.[80] The federal district court, conducting *in camera* review, challenged a dozen redactions, questioning whether they were justified on national security grounds.[81] The Government subsequently decided to lift many of them—apparently without any risk to national security.[82]

Fazaga itself arose in part because of FOIA litigation.[83] In early 2006, organizations and individuals in the Southern California Muslim community made a FOIA request to the FBI, seeking information related to the surveillance operation. Almost a year later, the FBI notified some of the plaintiffs that it did not have any responsive documents and provided to others a total of four heavily redacted pages.[84] Plaintiffs responded by filing suit in the district court to challenge the adequacy of the search. The government subsequently produced *over one hundred* pages of heavily redacted documents.[85] It followed this with a motion for summary judgment, attesting that its invocation of the national security exemptions was both necessary

---

[74] New York Times v. NSA, 205 F.Supp.3d 374 (S.D.N.Y. 2016).
[75] Elec. Frontier Found. v. DOJ, No.: 4:11-cv-05221-YGR, 2014 WL 3945646 (N.D. Cal. Aug. 11, 2014). Numerous cases follow suit. *See, e.g.,* American Civil Liberties Union v. U.S. Department of Justice, 210 F. Supp. 3d 467, 471 (S.D.N.Y. 2016) (After the DOJ conducted a new FOIA search following court orders in 90 F. Supp. 3d 201, approximately 80 responsive documents were located.)
[76] *See* Elec. Privacy Information Center v. Dep't. of Justice, 296 F.Supp.3d 109, 115 (D.D.C. Nov. 7, 2017).
[77] Elec. Privacy Information Center, 296 F.Supp.3d at 116.
[78] Elec. Frontier Found. v. Dep't. of Justice, 57 F.Supp.3d 54, 56 (D.D.C. 2014).
[79] *Id.* at 57.
[80] *Id.* at 57-8.
[81] *Id.* at 58.
[82] *Id.* at 59.
[83] *See* Islamic Shura Council of Southern California v. Federal Bureau of Investigation, 635 F.3d 1160 (9th Cir. 2011).
[84] *Id.* at 1162.
[85] *Id.* at 1163.

and proper. Plaintiffs objected and requested that the district court examine the redacted documents. Upon receiving an order from the court directing it to provide any documents redacted or withheld, the FBI acknowledged to the court that there were *additional* responsive documents, which it has not disclosed either to the court or to the plaintiffs.[86] The district court, and the Ninth Circuit on appeal, expressed significant concern that the government had misled both the plaintiffs and the court.[87] The complaint in *Fazaga* went on to cite to some of the materials obtained over the course of the FOIA litigation.

D. Rule of Law Considerations

The material that entered the public domain from each of these streams produced important information about the scope of the surveillance programs underway and how the law was being interpreted.[88] It also revealed that the government had repeatedly acted beyond its statutory authority and in contravention to judicial direction, raising concerns about the impact on citizens' constitutional rights.[89]

From the beginning of the bulk telephony program under the FISA's business records provision (Section 215), for example, FISC opinions showed that the NSA routinely ran queries on U.S. persons (USPs) using terms that did not meet the judicially-required standard of reasonable, articulable suspicion.[90] The FISC in 2009 concluded that it had been "so frequently and systematically violated that it can fairly be said that this critical element of the overall . . . regime has never functioned effectively."[91] That same year, the FISC discovered that the government had been picking and choosing which of its misdoings it reported, omitting, for example, failures to de-task accounts even after the NSA knew that the targets were on U.S. soil (thereby continuing to collect their communications in violation of the statute).[92]

In another case, the FISC called attention to the government's "chronic tendency to mis-describe the actual scope of NSA [Title I] acquisitions in its submissions to this Court," noting,

> These inaccuracies have previously contributed to unauthorized electronic surveillance and other forms of statutory and constitutional deficiency. It is evident that the government needs every incentive to

[86] *Id.* at 1164.
[87] *Id*. The district court sanctioned the government under Rule 11(c) for deceiving the court. *See* Islamic Shura Council of S. Cal. v. Fed. Bureau of Investigation, 278 F.R.D. 538, 539 (C.D. Cal. 2011). The Ninth Circuit subsequently reversed the ruling on technical grounds. *See* Islamic Shura Council of S. Cal. v. Fed. Bureau of Investigation, No. 12-55305, 2013 WL 3992123 (9th Cir. 2013) (per curiam).
[88] *See, e.g*., Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00004 (FISA Ct.) (Baker, J.), GID.C.00004, https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-2.pdf. [Local] (evaluating Fourth Amendment implications; holding that the FBI marking procedures violated the statutory minimization requirements);
[89] *See, e.g*., Opinion and Order Regarding Fruits of Unauthorized Electronic Surveillance, *[REDACTED]*, Nos. [REDACTED], GID.C.00059 (FISA Ct. Dec. 10, 2010) (Scullin, Jr., J.), GID.C.00059 https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-11.pdf. [Local]; Opinion and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance, *[REDACTED]*, Nos. [REDACTED], GID.C.00067 (FISA Ct. May 13, 2011) (Scullin Jr., J.), GID.C.00067 https://www.dni.gov/files/documents/icotr/EFF-FOIA-Jan-31-Doc-10.pdf. [Local]
[90] Prod. of Tangible Things from [REDACTED], GID.C.00036 at 11; 2009 WL 9150913, at *5.
[91] *Id.*
[92] *Id.*

> provide accurate and complete information to the Court about NSA operations, whenever such information is material to the case.[93]

The executive branch made similar, inaccurate representations about the post-tasking review process.[94]

In 2011, the FISC discovered that the NSA had misled it about Section 702 Upstream collection, acquiring (in violation of the statute) tens of thousands of domestic USP communications.[95] In response, the court forbade the NSA from using USP identifiers to query upstream data. Six years later, the FISC discovered that, nevertheless, "NSA analysts had been conducting such queries in violation of that prohibition [and] with much greater frequency than had previously been disclosed."[96] The court underscored its concern about the government's failure to disclose noncompliance.[97] The institutional "lack of candor" presented "a very serious Fourth Amendment issue."[98]

In December 2019, the FISC similarly noted widespread violations of the FBI's querying standards, including agents undertaking queries of unminimized Section 702 information to vet sources and candidates; investigate college students participating in a "Collegiate Academy"; conduct background checks on individuals who had visited an FBI office; and dig up information on nearly 16,000 persons, of which NSD later assessed only seven persons satisfied the querying standard.[99] The FBI, moreover, had *never* applied for an order under FISA Section 702(f)(2), which is *required* before querying unminimized contents using a USP query term unrelated to national security or the effort to find and extract foreign intelligence.[100] Numerous other problems came to light.[101]

---

[93] *See* Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00254, at 10-11, 13014 (FISA Ct. [REDACTED]) (Hogan, J.) (NSA's acquisition of [REDACTED] constituted unauthorized electronic surveillance because it failed to comply with 50 U.S.C.A. § 1804(a)(2), (a)(3)(B) (West)). (citations have been redacted).

[94] *See* Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00062, at 20–21 (FISA Ct. 2010) (McLaughlin, J.), https://repository.library.georgetown.edu/handle/10822/1052735.

[95] *See* Memorandum Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00073, 2011 WL 10945618 (FISA Ct. Oct. 3, 2011) (Bates, J.), https://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and Order-20140716.pdf. *See also* Memorandum Opinion, *[REDACTED]*, No. PR/TT [REDACTED], GID.C.00092 (FISA Ct.) (Bates, J.), https://www.dni.gov/files/documents/1118/CLEANEDPRTT 2.pdf (stating, "NSA exceeded the scope of authorized acquisition continuously during the more than [REDACTED] years of acquisition under these orders.");

[96] Memorandum Opinion and Order, [REDACTED], No. [REDACTED], GID.C.00130, at 19 (FISA Ct. Apr. 26, 2017) (Collyer, J.), https://repository.library.georgetown.edu/bitstream/handle/10822/1052702/gid_c_00130.pdf?sequence=1&isAllowed=y. *See also* Exhibit A: Procedures Used by the National Security Agency for Targeting Non-United States Persons Reasonably Believed to be Located Outside the United States to Acquire Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended at 2, [REDACTED] (FISA Ct. Mar. 30, 2017) (No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1053027 [https://perma.cc/P7G9-28S2]; Exhibit B: Minimization Procedures Used by the National Security Agency in Connection with Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended, § 3(b)(4)b, at 4, [REDACTED] (FISA Ct. Mar 30, 2017) (No. No. [REDACTED]), *available at* https://repository.library.georgetown.edu/handle/10822/1053259 [https://perma.cc/D5LM-G5U7].

[97] *[REDACTED]*, GID.C.00130, at 4.

[98] *Id.* at 19 (quotations omitted).

[99] Memorandum Opinion and Order, *[REDACTED]*, No. [REDACTED], GID.C.00282 (FISA Ct. Dec. 6, 2019) (Boasberg, J.), at 65-67 https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2019_702_Cert_FISC_Opinion_06Dec19_OCR.pdf.

[100] *Id.* at 69-71.

[101] The NSA Office of the Inspector General, for instance, has repeatedly noted that the NSA is unable to ensure that data is queried in compliance with Section 702 targeting and minimization

The government's failure to follow the letter of the law extended well beyond those portions added by the 2008 FISA Amendments Act. Applications under Titles I and III (germane to *Fazaga*) also have been called into question. The DOJ Inspector General's (IG) investigation of Crossfire Hurricane, an operation initiated in 2016 to ascertain whether individuals involved with Donald Trump's presidential campaign coordinated with Russian efforts to interfere in the election, proves illustrative.[102] Following a 12-month inquiry, IG Michael Horowitz issued an exhaustive, nearly 500-page report based on upwards of 170 interviews with more than 100 witnesses, as well as more than one million documents held by the DOJ and FBI. He found significant discrepancies between law, policy, and FBI practice.[103] FISA applications for electronic surveillance left out information that cut against the FBI or was inconsistent with what they were telling the court—information directly relevant to the probable cause determination.[104] They contained information that had not been corroborated, misstatements, inaccurate data, and other errors, and they omitted important information.[105] Horowitz expressed his deep concern,

> That so many basic and fundamental errors were made by three separate, hand-picked teams on one of the most sensitive FBI investigations that was briefed to the highest levels within the FBI, and that FBI officials expected would eventually be subjected to close scrutiny, raised significant questions regarding the FBI chain of command's management and supervision of the FISA process.[106]

The IG further discovered that an FBI lawyer had falsified an email to tip the scales in favor of the FISC granting the application.[107]

Horowitz was sufficiently disquieted that he launched a second audit focused on FBI compliance with the Woods procedures—guidelines the FBI provided to the FISC and indicated that it would follow to ensure that FISA applications contain reliable information.[108] He randomly selected 29 applications

---

procedures. The NSA was supposed to address the concern by December 2017. As of March 2022, however, it still had not been done. *See* NAT'L SEC. AGENCY, OFF. INSPECTOR GEN., SEMIANNUAL REPORT TO CONGRESS, 1 OCTOBER 2021 – 31 MARCH 2022 34 (2022) (available at https://oig.nsa.gov/Portals/71/Images/NSAOIGMAR2022.pdf?ver=jbq2rCrJ00HJ9qDXGHqHLw%3d%3d&timestamp=1657810395907).

[102] OFF. OF THE INSPECTOR GEN., DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION i (revised Dec. 20, 2019) [hereinafter CROSSFIRE HURRICANE REPORT], https://repository.library.georgetown.edu/handle/10822/1058716. During the campaign, a foreign government informed the Obama Administration that Russia had reached out to the Trump team to offer to release information that would be damaging to the Democratic Party candidate. *Id.* at ii.

[103] *See id.* at i, ii–xviii.

[104] *Id.*

[105] *Id.* at viii–ix, xi–xii.

[106] *Id.* at xiv.

[107] *Id.* at ix. *See also* Matt Zapotosky, *Ex-FBI Lawyer Avoids Prison After Admitting He Doctored Email in Investigation of Trump's 2016 Campaign*, WASH. POST (Jan. 21, 2021), https://www.washingtonpost.com/national-security/kevin-clinesmith-fbi-john-durham/2021/01/28/b06e061c-618e-11eb-afbe-9a11a127d146_story.html [https://perma.cc/GFS2-XLNC].

[108] In March 2000, the FISC discovered that in four or five separate cases, DOJ had been disseminating FISA information to the FBI and U.S. Attorney's Office without the required authorizations of the Court. *In re* All Matters Submitted to Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611, 620, GID.C.00002, at 620 (FISA Ct. 2002) (Lamberth, J.), *rev'd by In re* Sealed Case, 310 F.3d 717, GID.CA.00001 (FISA Ct. Rev. 2002) (per curiam). A few months later, the government confessed to errors in 75 separate FISA applications relating to major terrorist attacks, including:

targeting U.S. persons from 2014 to 2019.[109] He discovered that *every application* contained errors.[110] Although DOJ had indicated to the FISC that it was following the Woods procedures, it was not in fact doing so. In many cases, there were no files at all.[111] In cases where there were files, facts lacked support or corroboration, or were inconsistent with claims being made to the FISC. On average, each application had approximately 20 errors, with up to 65 in just one.[112] Horowitz continued his examination, in September 2021 issuing the final results in which he identified 400 instances of non-compliance in the 29 applications, as well as an additional 179 applications for which the original Woods File was missing, destroyed, or incomplete.[113]

This is the context within which *Fazaga* arose: information in the public domain indicates that the government has repeatedly acted outside its constitutional and statutory limits—including in regard to the authorities at issue in the case. Despite repeated efforts by the FISC to hold the government to account, it has proven difficult to do so. With standing met, litigants like Fazaga are coming forward to assert their constitutional rights.

III. THE *FAZAGA* CLAIMS

In 2011, Yassir Fazaga, an imam at the Orange County Islamic Foundation (OCIF), and two ICOI community members, Ali Malik, and Yasser Abdelrahim, brought a class action suit against the FBI, asserting eleven causes of action related to unconstitutional searches as well as unlawful discrimination on the basis of, or burdens on, or abridgement of the right to religion—implicating the first amendment, the equal protection guarantee of the due process clause of the fifth amendment, the privacy act, the Religious Freedom Restoration Act, FISA, and the Federal Tort Claims Act.[114] Their concerns centered on Operation Flex, the surveillance program apparently launched in 2006 to collect information about the Orange County Muslim

---

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

Id. at 620. These actions prompted the adoption of the Woods procedures, to ensure that the Court could rely on the information in future applications.

[109] Management Advisory Memorandum from Michael E. Horowitz, Inspector Gen., to Christopher Wray, Dir., FBI, regarding the Audit of the Federal Bureau of Investigation's Execution of its Woods Procedures for Application Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons at 2 (Mar. 30, 2020), https://repository.library.georgetown.edu/handle/10822/1058475 [https://perma.cc/V9N9-2DHH].

[110] *See id.* at 7–8.

[111] *Id.* at 7.

[112] *Id.*

[113] U.S. DEP'T. OF JUSTICE OFFICE OF THE INSPECTOR GENERAL, AUDIT OF THE FEDERAL BUREAU OF INVESTIGATION'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS, Sept. 2021 7 (2021) (available at https://oig.justice.gov/sites/default/files/reports/21-129.pdf). *See also* A MESSAGE FROM THE INSPECTOR GENERAL: AUDIT OF THE FBI'S EXECUTION OF ITS WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS, Sept. 2021 (available at https://oig.justice.gov/sites/default/files/2021-09/09-30-2021.pdf).

[114] First Amended Complaint, Fazaga v. FBI, 8:11-cv-00301-CJC-VBK (Sep. 1, 2011) (available at https://www.aclu.org/legal-document/fazaga-v-fbi-first-amended-complaint).

community. As aforementioned, the FBI had hired Monteilh as an informant. It later directed him to begin asking pointed questions in the Islamic community about jihad.[115] He represented to members of ICOI that he felt it his duty as a Muslim to take violent action.[116] Several members became alarmed and reported him to the mosque's leadership. One called the FBI directly and told others to call the Irvine Police Department, which they did, obtaining a restraining order against Monteilh.[117] In 2009, the government brought a criminal prosecution for naturalization fraud against one of the members who had called the police for the restraining order.[118] An FBI Special Agent's testimony during the bail hearing revealed an informant at ICOI, whom the plaintiffs identified as Monteilh.

As soon as the suit commenced, the Government asserted state secrets privilege in regard to three categories of information and moved to dismiss the discrimination claims on state secrets grounds.[119] The district court dismissed all but one of the plaintiffs' claims—including their fourth amendment assertion—based on state secrets.[120] On appeal, the Ninth Circuit reversed on the grounds that "the district court should have reviewed any state secrets evidence necessary for a determination of whether the alleged surveillance was unlawful following the secrecy-protective procedure set forth in FISA."[121] For the court, FISA had supplanted state secrets.

The statute creates a private right of action for an individual subject to electronic surveillance in violation of FISA's procedures. For civil liability,

> An aggrieved person, other than a foreign power or agent of a foreign power . . . who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation.[122]

In the FISA world, "foreign power" (FP) and "agent of a foreign power" (AFP) are terms of art: the statute defines them to ensure that targets of surveillance are affiliated with foreign governments or are members of international terrorist organizations.[123] The government must demonstrate probable cause that the target is an FP/AFP *and* that the target is using the facilities to be placed under surveillance.[124] The aim is to ensure that individuals who do not meet the probable cause standard—for instance, the entire Orange County Islamic community—are not put under surveillance. The statute *prohibits* electronic surveillance outside of FISA or the ordinary Title III warrant procedure.[125]

---

[115] Declaration of Craig F. Monteilh, Fazaga v. FBI, SA-cv-11-00301, at ¶ 73. Monteilh claims that the FBI provided him with a letter granting him immunity to allow him to engage in jihadist rhetoric and criminal activity. *Id.* at ¶ 72. *See also* 965 F.3d at 1027.
[116] *Id.* at ¶ 73. *See also Fazaga*, 965 F.3d at 1027.
[117] *Id.* at ¶ 73. *See also Fazaga*, 965 F.3d at 1028.
[118] Niazi, who had lived in the United States since 1998 and obtained citizenship five years previously, was related by marriage to Amin al-Haq, a member of a designated terrorist organization. He failed to disclose the relationship during his application, giving rise to charges of perjury, naturalization fraud, misuse of a passport obtained by fraud, and making false statements to a federal agency. Teresa Watanabe & Scott Glover, *Man Says He Was FBI Informant*, L.A. TIMES, (Feb. 26, 2009), https://www.latimes.com/archives/la-xpm-2009-feb-26-me-informant26-story.html.
[119] Fazaga v. FBI, 965 F.3d 1015, 1024-25 (9th Cir. 2020).
[120] *Id.* at 1025.
[121] *Id.*
[122] 50 U.S.C. § 1810.
[123] *See* § 1801(a), (b).
[124] § 1805(2)(A), (B).
[125] § 1809. The Ninth Circuit held that the plaintiffs constituted aggrieved persons within the meaning of the statute. *Fazaga*, 965 F.3d at 1053.

Monteilh's recording of conversations to which he was not party fell within FISA's fourth definition of electronic surveillance.[126] The plaintiffs, though, had both an objective and subjective reasonable expectation of privacy in the inner sanctums of the mosque. The Ninth Circuit explained,

> [T]he prayer hall "is [a] sacred space where particular rules and expectations apply. Shoes are prohibited, one must be in a state of ablution, discussing worldly matters is discouraged, and the moral standards and codes of conduct are at their strongest." Notably, "[g]ossiping, eavesdropping, or talebearing (*namima*—revealing anything where disclosure is resented) is forbidden." And ICOI, which Malik and AbdelRahim attended, specifically prohibited audio and video recording in the mosque without permission.[127]

Fazaga's office and AbdelRahim's apartment and car similarly raised free-stating fourth amendment concerns. The case therefore fell within FISA's remit.

The Ninth Circuit looked to two district courts which had previously held that the statute had displaced common law rules like state secrets on matters within FISA's purview.[128] Under FISA Section 1806(f),

> *Whenever* a court or other authority is notified [that the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance] . . . or *whenever* any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States . . . before any court . . . to discover or obtain applications or orders or other materials relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this Act, the United States district court . . . *shall, notwithstanding any other law*. . . , review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted.[129]

The language ("notwithstanding any other law", several uses of "whenever", and the command that courts "shall" use the procedures), confirmed "Congress's intent to make the *in camera* and *ex parte* procedure the exclusive procedure for evaluating evidence that threatens national security in the context of electronic surveillance."[130] Those clauses overrode "on the one hand, the usual procedural rules precluding such

---

[126] *See* § 1801(f) (defining electronic surveillance as "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy *and* a warrant would be required for law enforcement purposes")
[127] *Fazaga*, 965 F.3d at 1034.
[128] *See also* Jewel v. NSA, 965 F. Supp.2d 1090, 1105-06 (N.D. Cal. 2013); In re NSA Telecomms Recs. Litig., 564 F. Supp. 2d 1109, 1117-24 (N.D. Cal. 2008).
[129] § 1806(f) (emphasis added).
[130] *Fazaga*, 965 F.3d at 1045.

severe compromises of the adversary process and, on the other, the state secrets evidentiary dismissal option."[131]

The government disagreed. Nothing in the text of FISA expressly mentions "state secrets".[132] Nor does anything in FISA's legislative history.[133] To overturn such a settled practice, the government argued, Congress needed to give a clear statement.[134] Beyond this, it suggested, § 1806(f) procedures only apply where the *government* initiates the legal action—not in the case of affirmative challenge to the legality of electronic surveillance.[135]

The Ninth Circuit saw it rather differently, zeroing in on two circumstances in which FISA contemplates *in camera, ex parte* procedures: (1) when the government gives notice of its intent to "use or disclose. . . any information obtained or derived from an electronic surveillance"; and (2) where "any motion or request is made by an aggrieved person. . . to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance."[136] In regard to the former, the complaint alleged that information was being collected pursuant to FISA Titles I/ III. Although the government refused to confirm or deny it, the fact that the Attorney General asserted state secrets in relation to "any information obtained during the course of" Operation Flex, the "results of the investigation" and "any results derived from" the "sources and methods" used in Operation Flex, conveyed notice. The government objected, arguing, "By the panel's reasoning, a litigant who asserts the attorney-client privilege signals her intent to use or disclose private communications with counsel. . . But, of course, [he does] nothing of the sort."[137] Seeking dismissal did not amount to "a declaration of the govenrment's 'inten[t] to enter into evidence or otherwise use or disclose' any privilaged information 'in any trial, hearing, or other proceeding.'"[138] In regard to the latter, the court reasoned that the plaintiffs' effort to "obtain" information gathered or derived from electronic surveillance so that it could be either destroyed or returned, amounted to a "motion or request" to obtain it.[139]

---

[131] *Id*. The court further cited to legislative history, noting "It is to be emphasized that, although a number of different procedures might be used to attack the legality of the surveillance, it is the procedures set out in subsections (f) and (g) 'notwithstanding any other law' that must be used to resolve the question." *Id.*at 1045-46 (quoting H.R. REP. NO. 95-1283, pt. 1, at 91 (1978)). The court made a parallel argument from practice, noting that the same concerns underlay both the FISA procedures and the state secrets privilege—as recognized by multiple district courts in support of the proposition that FISA supplanted state secrets as to ELSUR. *Id.* (citing Jewel v. NSA, 965 F. Supp. 2d 1090., 1106 (N.D. Cal. 2013) and quoting In re NSA Telecomms. Recs. Litig., 564 F. Supp. 2d 1109, 1119 (N.D. Cal. 2008)). It also advanced two historical arguments: first, that Congress intended FISA to serve as a comprehensive approach to regulating domestic foreign intelligence collection, by establishing a balancing role for all three branches, repleted with oversight mechanisms, rules, a special court, and a civil enforcement mechanism. Second, the Court suggested that the legislative history confirmed "Congress's intent to displace the remedy of dismissal for the common law state secrets privilege." *Id.* at 1046-47. FISA embodied Congress's response to the revelations of the Church Committee, which had called for "fundamental reform" to "[m]ake clear to the Executive branch that [Congress] will not condone, and does not accept, any theory of inherent or implied authority to violate the Constitution." *Id.* at 1047. FISA was Congress's primary instrument for doing so.

[132] *See* Brief for the Petitioners, Fed. Bureau of Investigation v. Fazaga, No. 20-828, p. 19.

[133] *Id.*

[134] *Id.* at 20.

[135] See *id.* at 18 ("The government invokes the state-secrets privilege for the same reason that any party asserts any evidentiary privilege: to prevent the introduction or disclosure of the privileged information, not to facilitate its use. Excluding evidence—not using that evidence—is how a litigant claiming any privilege vindicates the interest protected by that privilege.")

[136] 50 U.S.C. § 1806(c), (f).

[137] Brief for the Petitioners, Fed. Bureau of Investigation v. Fazaga, No. 20-828, p. 25.

[138] *Id.* at 26.

[139] According to the government, as aforementioned, a substantive request for relief on the merits was not the kind of procedural motion that would trigger FISA's procedures. It drew a distinction between a prayer for relief and a "motion", "[a]nd although it might be colloquially described as a 'request,' it

The Supreme Court, unconvinced by the Ninth Circuit's approach, held that in civil litigation, § 1806(f) does not displace the state secrets privilege.[140] Writing for a unanimous Court, Justice Alito stated that the provision governs circumstances in which the *government* seeks to employ information obtained from electronic surveillance.[141] In reaching this conclusion, the Court relied on two arguments. First, the statute does not refer to "state secrets privilege", which suggests that Congress did not seek to cabin the privilege.[142] Such a limitation, regardless of whether state secrets represented a common law privilege or a constitutional power assigned to the executive branch, could only follow from clear statutory language.[143] While the Court was right that the statute nowhere explicitly replaced "state secrets," the argument sidestepped the fact that at the time of FISA's passage, the term was neither the only nor the most common one employed to describe the evidentiary rule.[144]

Second, the Court determined that the language of §1806(f) is not incompatible with the state secrets privilege.[145] They operate in different ways and apply to different circumstances. Justice Alito explained:

> Section 1806(f) is most likely to come into play when the Government seeks to use FISA evidence in a judicial or administrative proceeding, and the Government will obviously not invoke the state secrets privilege to block disclosure of information that it wishes to use. Section 1806(f) is much more likely to be invoked in cases of this sort than in cases in which an aggrieved person takes the lead and seeks to obtain or disclose FISA information for a simple reason: individuals affected by FISA surveillance are very often unaware of the surveillance unless it is revealed by the Government.[146]

Thus, even where an aggrieved party brings suit, the statute and the privilege entail different inquiries, provide for different forms of relief, and adopt different procedures.[147]

The Court did not weigh in on the substantive state secrets claims advanced by the government, remanding the case for further adjudication. The questions presented are critical and have already returned to the Court in the latest state secrets

---

is nothing like a motion to suppress or comparable procedural motion at which § 1806(f) is aimed." *Id.* at 18. Instead, the statutory language should be read in conjunction with provisions related to the government giving notice of the intent to use or disclose material, or when the aggrieved person attempted to suppress such material—nor could any litigant try to use a new statute to avoid the statutory language. *Id.* at 29-31. Fazaga responded to this argument by noting that there is nothing in the text that expressly limits motions or requests to "procedural motions" – nor is it limited to adjudication on the merits. *See* Brief for the Respondents, Federal Bureau of Investigation v. Fazaga, No. 20-828, p. 22.

[140] Fazaga, 142 S. Ct. 1051.

[141] *Id*., at 1060.

[142] *Id.* at 1060-61

[143] *Id.*

[144] *See e.g.*, United States v. Nixon, 418 U.S. 683, 701, 711 (1974) (making no reference to "state secrets", instead describing *Reynolds* as protecting "national security secrets" and "military matters which, in the interest of national security, should not be divulged.")

[145] Fazaga, 142 S. Ct. 1061.

[146] *Id*.

[147] *Id*. Under FISA, the question is whether the information was lawfully obtained—an inquiry irrelevant under state secrets, which instead focuses on whether, if made public, the information will damage national security. For FISA, if the court determines that the information was lawfully obtained, it does not have the ability to award relief. In contrast, under state secrets, if a court determines disclosure would not affect national security, it can be disclosed. For 1806(f), the court has to award relief if collection violated the law. For state secrets, lawfulness has nothing to do with the relief. Finally, under *Totten*, a case can be dismissed under state secrets—which is not an option under § 1806(f). *Id.* at 1061-62.

petition for certiorari—the ninth such petition in the past 18 months.[148] The problem is not going to go away for the simple reason that the manner in which the government has been wielding the privilege in *Fazaga*, and dozens of parallel suits, marks a sharp departure from how it has historically operated and raises serious questions about the future of certain constitutional rights.

IV. REINVENTING STATE SECRETS

The government's current interpretation of the state secrets privilege, which is rooted in the early 21st century torture and rendition cases, departs in four important respects from how the privilege, for centuries, has operated. First, it collapses the distinction between *Reynolds* and *Totten* to transform an evidentiary rule into a justiciability standard. In *Fazaga* and numerous other cases, the government has adopted a "very subject matter" analysis, sidelining the *ex ante* contractual argument undergirding the *Totten* bar. Second, the government now asserts the privilege early in suits (at the pleadings stage) to request dismissal, instead of employing it to ensure that particular evidence is excluded during discovery or trial. Third, it adopts a topical approach, asserting state secrets over broad categories which include information that poses no risk to U.S. national security as well as information already in the public domain. Fourth, the government is beginning to claim as a constitutional power a privilege that has always been a common law rule. All four elements, at issue in *Fazaga*, mark a host of similarly-situated cases making their way through the courts.

---

[148] In *Wikimedia Foundation v. National Security Agency*, the operator of one of the busiest websites (more than one trillion international Internet communications annually), is challenging the constitutionality of the government's use of Section 702. Petition for a Writ of Certiorari, No. 22-190, p. 8. Like *Fazaga*, the suit is based on information in the public domain, much of which the government itself has provided. The DNI reported in April 2022 that the government targeted 232,432 individuals and groups outside the United States over the previous year. Office of Dir. Of Nat'l Intel, *Annual Statistical Transparency Report* 17 (Apr. 2022). ODNI, PCLOB, the FISC/R, government officials, and FOIA lawsuits have provided details about how Upstream collection occurs on these targets. The NSA routinely scans international Internet communications as it traverses high-speed circuits operated by major communication service providers. *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 36 (2014). Unable to ascertain in advance which communications are unique to the targets, the NSA scans and copies all packets crossing certain international sites, subsequently reassembling them so that they can be examined to determine if they contain certain selectors. Data subsequently can be retained, queried, and disseminated. Because "Wikimedia's trillions of communications cross every international Internet link carrying public Internet traffic into and out of the United States," and "NSA conducts Upstream surveillance on at least one 'international Internet link,'" at least some of Wikimedia's communications are likely being monitored. Petition for a Writ of Certiorari, No. 22-190, pp. 11-12. Although the district court initially dismissed the case on the grounds that Wikimedia's allegations were too speculative to establish Article III standing, the court of appeals concluded that the facts put forward were "sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications." Wikimedia Foundation v. NSA, 857 F.3d 193, 211 (4th Cir. 2017). *See also* Wikimedia Foundation v. NSA, 14 F.4th 276, 279 and 292-94 (4th Cir. 2021) (again finding standing). On remand, the government indicated that it would continue to challenge Wikimedia's standing and argued that discovery should be bifurcated to allow the standing question first to be resolved. The court, however, directed the parties to undertake a limited five-month period of jurisdictional discovery prior to ruling on the merits. Order, Wikimedia Found. v. Nat'l Sec. Agency, 1:15-cv-662 (D. Md. Oct. 3, 2017). The government responded to several requests from the plaintiffs by arguing state secrets privilege. Wikimedia Found. V. National Sec. Agency, 335 F.Supp.3d 772 (2018). As in *Fazaga*, the government is requesting that the suit be dismissed altogether on the grounds that the surveillance programs in question are classified and that releasing information covering a range of topics would undermine U.S. national security.

A. Creation of the "Very Subject Matter" Analysis

State secrets did not, in 1953, spring fully-armed from Zeus's forehead. From the Founding, British and American common law recognized the privilege as a common law evidentiary rule.[149] Where exclusion of evidence prevented a plaintiff from making a prima facie case, the court could order dismissal. The sole exception, established in *Totten*, related to secret contractual relationships between the government and private actors, where both parties had ex ante notice that litigation in open court likely would not be available should a dispute arise.

Post-9/11, with standing met in regard to the Terrorism Surveillance Program (TSP), the government immediately fell back on state secrets to avoid litigation, collapsing the *Reynolds* and *Totten* distinction by re-casting classified contract cases in terms of a "very subject matter" approach. The Ninth Circuit, in a case dealing with the TSP, balked at the assertion—not least because the government itself had already admitted to conducting warrantless surveillance outside of FISA. Undeterred, the government raised the same argument in the context of torture, coercive interrogation, and rendition. As in the surveillance cases, there was enough information in the public domain for standing to be met, prompting the government to re-cast state secrets as a justiciability standard. In *El-Masri* and then in *Jeppesen*, the argument gained purchase. Precedent set, the re-crafted understanding of state secrets worked its way back into surveillance cases like *Fazaga*, heralding potentially devastating effects for the future of citizens' first, fourth, and fifth amendment rights and the ability of the People to hold the government to account.

1. State Secrets as an Evidentiary Rule

English law has long treated state secrets as a common law evidentiary rule.[150] On this side of the Atlantic, starting with Aaron Burr's trial in 1807 and continuing

---

[149] *See, e.g.*, Gen. Dynamics Corp. v. United States, 563 U.S. 478, 485 (2011) ("Reynolds . . . decided a purely evidentiary dispute by applying evidentiary rules."). *El-Masri*, 479 F.3d at 303-04 (considering SSP an evidentiary rule "bas[ed] in the common law of evidence").

[150] In *Rex v. Watson*, the court considered whether the criminal defendant could elicit testimony as to the accuracy of a map of the Tower of London. Rex v. Watson, 2 Stark. 116, 148-49 (1817). In the wrong hands, such information could prove problematic. The judge, consistent with the privilege, did not halt the proceedings. Instead, he directed that testimony be limited to establishing whether the plan reflected the interior of the Tower and whether similar documents could be purchased. *Id.* In *Wyatt v. Gore*, the court excluded certain communications between the Lieutenant Governor of Upper Canada and attorney-general, as such communications should be treated as "confidential: no office of this kind could be executed with safety . . . were suffered to be disclosed." Wyatt v. Gore Holt 299 (N.P. 1816). The case, nevertheless, proceeded, with the plaintiff prevailing. The following year, in *Cooke v. Maxwell*, the court excluded on similar grounds instructions from the governor of Sierra Leone to a military officer. Cooke v. Maxwell, 2 Stark. 183, 183, 185-86 (1817). While the plaintiff could not provide the contents of the communications, he could demonstrate "that what was done was done by the order of the defendant." *Id.* at 186. He prevailed. *Id.* at 187. Similarly, in *Home v. Bentink*, the court withheld minutes taken at a military court of enquiry on the grounds that such "matters, secret in their natures, and involving delicate enquiry and the names of persons, stand protected." Home v. Bentinck, 2 Brod. & B. 130 (1820). Numerous cases from that time through the mid-20th century followed suit—each one treating the privilege as a common law evidentiary rule. *See, e.g.*, Regina v. Russell, 7 Dowl Pr. 693 (1839) (excluding the papers of the former Secretary of State); H.M.S. Bellerophon, 44 L.J. Adm. 5, 6-7 (1875) (excluding the log books of a navy ship that collided with another ship as well as government communications about the incident); Mercer v. Denne [1904] 2 Ch. 535, 544 (maps of seashore boundaries prepared for the war office excluded on grounds that it would be too dangerous to admit them); Mercer v. Denne, [1905] 2 Ch. 538, 561 (C.A. 1905) (affirming Mercer v. Denne on appeal); Duncan v. Cammell, Laird & Co., [1941] 1 K.B. 640 644 (C.A.) (excluding documents relating to the design of a submarine which sank in 1939 on the grounds based on the Lord of the Admiralty's claim in an affidavit that it "would be injurious to the public interest"), *aff'd* in Duncan v. Cammell, Laird & Co., [1942] A.C. 624 (H.L.).

through *Reynolds*, courts routinely approached it in a similar manner.[151] Thus, in the 1912 case *Firth Sterling Steel Co. v. Bethlehem Steel Co.*, the federal district court directed that drawings related to the manufacture of armor-piercing projectiles be removed from the record.[152] In *Pollen v. Ford Instrument Co.*, the court ordered that documents detailing sighting mechanics for guns be expunged on the grounds "that any disclosure of the structures used by the Navy or others authorized by it would be detrimental to the national defense and the public interests."[153]

Courts tempered government assertions of the privilege. In *United States v. Haugen*, for instance, the federal district court excluded a government contract but sanctioned proof of a portion of it to be submitted.[154] In *Cresmer v. United States*, the plaintiff sought the report of the Navy Board of Investigation into an airplane that crashed, killing the plaintiff's intestate.[155] Although the document initially had been withheld, the judge requested a copy of it to ensure "that the report in question contained no military or service secrets which would be detrimental to the interests of the armed forces of the United States or to National security."[156] Seeing "nothing in it which would in any way reveal a military secret or subject the United States and its armed forces to any peril by reason of complete revelation," he ordered that it be produced.[157] He explained, "In the absence of a showing of a war secret, or secret in respect to munitions of war, or any secret appliance used by the armed forces, or any threat to the National security, it would appear to be unseemly for the Government to thwart the efforts of a plaintiff in a case such as this to learn as much as possible concerning the cause of the disaster."[158]

The determination of whether to allow the evidence to enter into proceedings resided with the judge.[159] Accordingly, in *O'Neill v. United States*, the court took judicial notice of "the general policy of the common law, prohibiting disclosure of state secrets the publication of which might seriously embarrass or harm the government in its diplomatic relations, military operations, or measures for national

---

[151] In *United States v. Burr*, the court made reference to the evidentiary rule, but did not actually invoke it, explaining its limits in capital cases: "That there may be matter, the production of which the court would not require, is certain; but, in a capital case, that the accused ought, in some form, to have the benefit of it, if it were really essential to his defence, is a position which the court would very reluctantly deny. It ought not to be believed that the department which superintends prosecutions in criminal cases, would be inclined to withhold it." *United States v. Burr*, 25 F.Cas. 30, 37 (Cir. Court, D. Va. 1807). The Court continued, "What ought to be done under such circumstances present a delicate question, the discussion of which, it is hoped, will never be rendered necessary in this country. At present it need only be said that the question does not occur at this time. There is certainly nothing before the court which shows that the letter in question contains any matter the disclosure of which would endanger the public safety. If it does contain such matter, the fact may appear before the disclosure is made. If it does contain any matter which it would be imprudent to disclose, which it is not the wish of the executive to disclose, such matter, if it be not immediately and essentially applicable to the point, will, of course, be suppressed." *Id.* Chief Justice Marshall, riding circuit, allowed the defense to subpoena President Jefferson to obtain a letter which an alleged co-conspirator, General James Wilkinson, had sent to him. *See* Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 Geo. Wash. L. Rev. 1249, 1272 (2007).

[152] Firth Sterling Steel Co. v. Bethlehem Steel Co., 199 F. 353 353-56 (E.D. Pa. 1912).

[153] Pollen v. Ford Instrument Co., 26 F. Supp. 583, 584 (E.D.N.Y. 1939).

[154] United States v. Haugen, 58 F. Supp. 436 (E.D. Wash. 1944).

[155] Cresmer v. United States, 9 F.R.D. 203 (E.D.N.Y. 1949).

[156] *Id.* at 204.

[157] *Id.*

[158] *Id.*

[159] Efforts by the government to assert this privilege in realm of criminal prosecution often failed—precisely because such documents could be material to the defense. *See, e.g.*, King v. United States, 112 Fed. 988, 996 (5th Cir. 1902); Schneiderman v. United States, 320 U.S. 118 (1943); United States v. Coplon, 185 F.2d 629 (2d Cir. 1950); Zimmeman v. Poindexter, 74 F.Supp. 933 (D. Haw. 1947); Haugen v. United States, 153 F.2d 850 (9th Cir. 1946); United States v. Clegg, 846 F.2d 1221 (9th Cir. 1988).

security."[160] It was for the court to ascertain if and when state secrets applied. As the Second Circuit Court of Appeals noted in the 1947 case *Bank Line v. United States*, "no general principle of refusing discovery on a general statement of prejudice to its best interests can or should be applied to any branch of the government, including the armed forces."[161]

Like the English, American treatises considered state secrets to be a common law evidentiary rule.[162] Simon Greenleaf, author of the first American treatise on evidence that served as the undisputed authority for nearly half a century, underscored the "class of cases, in which evidence is excluded from motives of public policy, namely, secrets of state, or things, the disclosure of which would be prejudicial to the public interest."[163] In the interests of public safety, "the rule of exclusion is applied no further than the attainment of that object."[164] Greenleaf provided as examples "communications between a provincial governor and his attorney-general on the state of the colony, or the conduct of its officers; or between such governor and a military officer under his authority; the report of a military commission of inquiry, made to the commander-in-chief; and the correspondence between an agent of the government and a Secretary of State."[165] All related to military and foreign affairs.

In 1940, John H. Wigmore similarly identified "secrets of state" as one of three types of evidentiary privileges relating to official information.[166] The testimonial privilege was limited to international relations, military affairs, and public security.[167] Other scholarly works followed course. In 1949, the *Yale Law Journal* explained that "originally the common law privilege [to withhold government information] protected only the identity of informers and secrets affecting the national security."[168] In the *Vanderbilt Law Review*, William Sanford similarly analyzed the contemporary "State of the Law as to Executive Privileges", considering as the very first "Privilege[] *Established by the Courts*", "Data Affecting National Security (Military and Diplomatic Secrets)".[169] In each case, it was for the

---

[160] O'Neill v. United States, 79 F.Supp. 827, 829 (E.D. Pa. 1948).

[161] Bank Line v. United States, 163 F. 2d 133, 139 (2d Cir. 1947) (Clark, J. concurring). He did not believe that the information being sought would "aid and comfort some unknown potential enemy if the Navy" stated precisely why "concealment of specific information is material to national defense." *Id*.

[162] *See, e.g.*, 1 Thomas Starkie, *A Practical Treatise on The Law of Evidence* § 80, at 106 (1826) (drawing attention to the exclusion of documents which, "on grounds of state policy" could be excluded because they were "prejudicial to the community."); JOHN PITT TAYLOR, GEORGE PITT-LEWIS, CHARLES FREDERIC CHAMBERLAYNE, A TREATISE ON THE LAW OF EVIDENCE AS ADMINISTERED IN ENGLAND AND IRELAND, Vol. 1 (1895), § 909, 589.

[163] 1 SIMON GREENLEAF, A TREATISE ON THE LAW OF EVIDENCE § 250, at 323-324 (6th ed. 1852).

[164] *Id.*

[165] *Id.* at § 251.

[166] 8 WIGMORE, EVIDENCE § 2378 (3d ed. 1940), at 792.

[167] *Id*. at 794.

[168] *Government Privilege Against Disclosure of Official Documents*, 58(6) YALE L. J. 993, 993 (1949). *See also Evidence-Privileged Communications-State Secrets*, 47 W. Va. L. Rev. 338, 340 (1941) (noting that where state secrets are asserted, where it is in the public interest, "the judge may order that the records be opened to the petitioner").

[169] William V. Sanford, *Evidentiary Privileges against the Production of Data Within the Control of Executive Departments*, 3(1) VANDERBILT L. REV. 73, 74 (1949) (emphasis added). Sanford wrote, "In the contemporary state of international affairs, where there is always a real danger of a serious international dispute, the security of the state requires efficient armed forces and diplomatic services." *Id*. at 75. While it was virtually impossible to draw a hard line, documents protected by the privilege related to U.S. military and foreign affairs. *Id*. *See als*o Kessler v. Best, 121 Fed. 439 (C.C.S.D.N.Y. 1903) (excluding documents in the archives of a foreign consulate); Crosby v. Pacific S. S. Lines, 133 F. 2d 470, 475 (9th Cir. 1943), cert denied, 319 U.S. 752 (1943) ("The special treatment of consuls is caused probably in part by treaty, in part by the fact that they are under the jurisdiction of the diplomatic department of government, and in party by the character of their business and permanent of existence and locality." And noting that in such circumstances (in relation to foreign governments),

court to ascertain whether certain evidence would be allowed as part of the judicial record.

2. *Reynolds* and Its Progeny

By the time of *Reynolds*, the sole exception to this unbroken practice of treating state secrets as an evidentiary rule was the contractual bar established in *Totten*.[170] A Court of Claims action seeking recovery for an espionage contract forged during the Revolutionary War, *Totten* provided for dismissal of the suit on two grounds: first, the contract itself stipulated "a secret service"—"[b]oth employer and agent must have understood that the lips of the other were to be for ever sealed respecting the relation of either to the matter."[171] The central concern was not just the "publicity produced" by such an act, but that requiring such information "would itself be a breach of a contract".[172] Second, the Court articulated "a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to the disclosure of matter which the law itself regards as confidential."[173]

As the Supreme Court later recognized in *General Dynamics v. United States*, *Totten* stands for an extremely narrow line of precedent resting on the judiciary's "common-law authority to fashion contractual remedies in Government-contracting disputes."[174] The decision captured "what the *ex ante* expectations of the parties were or reasonably ought to have been"—i.e., "that state secrets would prevent courts from resolving many possible disputes under the . . . agreement."[175]

Accordingly, in *Tucker v. United States*, a contractor brought a claim for expenses and compensation for secret services he allegedly performed for the Psychological Warfare Branch, Military Intelligence Department, and other agencies of the federal government.[176] The federal district court held in 1954 that secrecy regarding such services was necessary and that publicity would be a breach of contract, thus precluding recovery on the claim.[177] Similarly, in 1988, in *Guong v. United States*, a Vietnamese citizen alleged that he was recruited by the CIA to conduct covert military operations in North Vietnam.[178] The plaintiff claimed that the CIA agreed to pay him and, if captured, rescue him. In the event that the rescue failed, the plaintiff's wife was to receive his pay. After he was captured by the North Vietnamese in 1964, though, he was not rescued and the U.S. government stopped paying his wife. He escaped from prison and in 1986 filed an action to recover damages for the breach of contract. As in *Totten*, the federal court dismissed the

"the rule to be applied is the one we would apply to a similar department of government here."); Viereck v. United States, 130 F. 2d 945, 961 (D.C. Cir. 1942) (excluding testimony of an employee of the British Censor's Office in Bermuda).

[170] Totten v. United States, 92 U.S. 105, 107 (1875). ("It may be stated as a general principle, that public policy forbids the maintenance of any suit in a court of justice, the trial of which would inevitably lead to disclosure of matters which the law itself regards as confidential, and respecting which it will not allow the confidence to be violated.").

[171] *Id.* at 106.

[172] *Id.* at 107.

[173] *Id.*

[174] General Dynamics Corp. v. United States, 563 U.S. 478, 485 (2011); *see also* Tenet v. Doe, 544 U.S. 1, 3 (2005) (noting "the longstanding rule, announced more than a century ago in Totten, prohibiting suits against the Government based on covert espionage agreements").

[175] *General Dynamics*, 563 U.S. at 490 (citing *Totten*, 92 U.S. at 106).

[176] Tucker v. United States, 118 F. Supp. 371 (Ct. Cl. 1954).

[177] *Id*.

[178] Guong v. United States, 860 F.2d 1063 (Fed. Cir. 1998).

claim on the grounds that the contract was secret at the time of its creation, giving Guong *ex ante* notice.[179]

The mere fact of a government contract was not sufficient; it had to be part of a secret agreement—this is what ensured *ex ante* notice. In other words, *embedded in the contract itself* was the understanding that confidentiality would be maintained, making public access to it a breach.

Outside of this context, the evidentiary rule, formalized in *Reynolds* but previously employed in cases on both sides of the Atlantic, applied.[180] In *Reynolds*, the Air Force refused to release documents related to electronic equipment on board a B-29 bomber, which had crashed and killed three civilian passengers. According to the government, the plane had been on "a highly secret mission", and disclosure of the specific documents in question would "seriously hamper[] national security, flying safety, and the development of highly technical and secret military equipment."[181] Looking to Burr's trial as well as Greenleaf and Wigmore's *Treatise on the Law of Evidence*, the Court noted that state secrets privilege was "well established in the law of evidence."[182]

Over the ensuing decades, outside of the contractual context, *Reynolds* controlled. Thus, in *Greene v. McElroy*, the D.C. Circuit upheld state secrets as an evidentiary rule in regard to a security clearance application.[183] In *Pan Am. v. Aetna*, an insurance dispute arising out of the 1970 hijacking and subsequent destruction of Pan Am Flight 083 by the Popular Front for the Liberation of Palestine, the Second Circuit upheld the CIA's state secrets claim over certain files, even as the case continued.[184]

Courts did not always acquiesce to government claims. In *Halpern v. United States*, for example, the court rejected the Secretary of the Navy's claim of state secrets over the plaintiff's patent application, and all documents, statements, and testimony related to their technical subject.[185] Remanding the case, the court noted that the district court could adopt procedures to ensure that there would be no danger of public disclosure.[186] In *Heine v. Raus*, a slander action, the Fourth Circuit in 1968 tempered the CIA's invocation of state secrets by issuing rulings on each question

---

[179] Vu Duc Guong v. United States, No. 21-86C, slip op. at 3 (Ct. Cl. Sept. 30, 1987), *quoted in* Guong v. United States, 860 F.2d at 1064-65 (affirming lower court decisions).

[180] *See, e.g.*, Bernstein v. United States, 256 F.2d 697 (10th Cir. 1958) (In an action for fraud brought by the government against private parties, the court ruled that if a report made by witness for government during course of his investigation of sale of war surplus property was relevant and not privileged for security reasons or as an attorney's mental impression, conclusions, opinions or legal theories, it was proper subject for production and inspection).

[181] *Reynolds*, 345 U.S. 4-5.

[182] 345 U.S. at 6-7. *See also* 1 SIMON GREENLEAF A TREATISE ON THE LAW OF EVIDENCE, § 251 n. 5 (John Henry Wigmore ed., 16th ed. 1899); United States v. Burr, 25 F. Cas. 30, 37 (Marshall, Circuit Justice, C.C.D. Va. 1807).

[183] Greene v. McElroy, 254 F.2d 944 (D.C. Cir. 1958). On appeal, the Supreme Court reflected, "Certain principles have remained relatively immutable in our jurisprudence. One of these is that, where governmental action seriously injures an individual . . . the evidence used to prove the Government's case must be disclosed to the individual so that he has an opportunity to show that it is untrue." Greene v. McElroy, 360 U.S. 474, 496 (1959). Embodied in the sixth amendment, cross examination, as recognized by Wigmore in his treatise on evidence, had become a cornerstone of American jurisprudence. *Id.* at 497. In this case, neither the President nor Congress had "delegated to the Department of Defense the authority to bypass these traditional and well recognized safeguards." *Id.* at 500.

[184] Pan American World Airways v. Aetna Casualty & Surety Co., 368 F. Suppl. 1098, 1140 (S.D.N.Y. 1973). *See also* United States v. Bass, 472 F.2d 207 (8th Cir. 1973) (Court of Appeals confirming that the trial judge used due care to ensure that the defendants in a military contractor fraud/conspiracy case, were afforded maximum but reasonable discovery, and that the government provided enough information to the judge during the *in camera* review.)

[185] Halpern v. United States, 258 F.2d 36, 44 (2d Cir. 1958).

[186] *Id*. at 43-44.

calling for information, requiring a witness "to answer those which the Court thought would not impair the privilege while foreclosing answers to those questions which apparently would."[187] In *Committee for Nuclear Responsibility v. Seaborg*, the D.C. Circuit in 1971 considered an environmental challenge to the government's proposed underground nuclear test (Cannikin), to be carried out in Alaska.[188] The court isolated and removed military and diplomatic secrets from documents addressing potential environmental hazards, allowing the case to proceed. While the government's interest in the former was "plain", plaintiffs—in a manner similar to *Fazaga*—stated that they did not seek any secrets.[189]

Cases involving surveillance proceeded in similar fashion. Thus, in *Jabara v. Kelly*, a U.S. citizen sued the FBI director for alleged illegal surveillance, harassment and intimidation. The government asserted state secrets in response to several interrogatories, which the federal district court in 1973 largely upheld even as it required the release of some information (such as the name of the agency intercepting the calls) to the plaintiff.[190] Similarly in *Spock v. United States*, an action was brought against the United States, the Director of the NSA, and several unknown agents for alleged unlawful interception of plaintiff's oral, wire, telephone and telegraph communications. The federal district court found in 1978 that the state secrets privilege was validly established by a public and a sealed affidavit by the Secretary of Defense, but that it did not prevent the plaintiff from accessing the courts or require dismissal of the complaint.[191] In *Ellsberg v. Mitchell*, plaintiffs sought compensation for warrantless electronic surveillance.[192] The D.C. Court of Appeals ruled in 1983 that the state secrets privilege had been drawn too broadly: the government had failed to disclose the identities of the Attorneys General who had authorized the wiretaps, despite the government conceding, during oral argument, that there was no reason such information would undermine national security.[193]

Under the *Reynolds* standard, if a plaintiff could not make out a prima facie case or carry the burden of persuasion without the privileged information, then the court dismissed the case. Discharging the suit thus acted as a logical consequence of the evidentiary rule. In *Zuckerbraun v. General Dynamics Corp.*, for instance, the Second Circuit in 1991 determined that because information relating to the weapons system's "design, manufacture, performance, functional characteristics, and testing" could not be made public, the appellant could not establish a prima facie case.[194] The following year, *Bareford v. General Dynamics Corp*. was resolved on similar grounds. There, the plaintiffs alleged that a Navy frigate's defense system had failed to counter Iraqi missiles.[195] The Fifth Circuit observed in 1992 that while the plaintiffs had accumulated "considerable evidence," it fell short of establishing that the Phalanx system had failed its basic function.[196]

---

[187] Heine v. Raus, 399 F.2d 785, 788 (4th Cir. 1968).
[188] Comm. For Nuclear Responsibility v. Seaborg, 463 F.2d 788 (D.C. Cir. 1971).
[189] *Id*.
[190] Jabara v. Kelly, 476 F. Supp. 561 (E.D. Mich. 1973).
[191] Spock v. United States, 464 F.Supp. 510 (D.C.N.Y. 1978)
[192] Ellsberg v. Mitchell, 709 F.2d 51 (D.C. Cir. 1983).
[193] *Id*. at 52.
[194] Zuckerbraun v. General Dynamics Corp., 935 F.2d 544, 547-48 (2d Cir. 1991). *See also* Nejad v. United States, 724 F. Supp. 753, 754, 756 (D.C. Cal. 1989) (noting that absent "disclosure of the AEGIS system technology [and rules of engagement], the case could not be tried).
[195] Bareford v. General Dynamics Corp. 973 F.2d 1138, 1140 (5th Cir. 1992).
[196] *Id*. at 1142. *See also* Black v. United States, 62 F.3d 1115, 1118 (8th Cir. 1995) (dismissing the suit on the grounds that absent the prohibited information the plaintiff could not "establish[] a prima facie Bivens claim"); Frost v. Perry, 919 F. Supp. 1459, 1468 (D. Nev. 1996) ("Plaintiffs cannot provide the essential evidence to establish its [sic] *prima facie* case for any of its eleven claims due to the Defendants' assertion of the military and state secrets privilege."); Bentzlin v. Hughes Aircraft Co.,

On the other side of a suit, in the event that a defendant claimed an inability to properly mount a defense without the documents subject to state secrets, following *in camera* review of the information in question and its subsequent exclusion, courts post-*Reynolds*, on occasion, ordered dismissal. As the Fourth Circuit sitting en banc explained in 1980 in *Farnsworth Cannon, Inc. v. Grimes*, a case that dealt with allegedly tortious interference with future contract rights between Farnsworth Cannon and the U.S. Navy,

> The unavailability of the evidence is a neutral consideration, and, whenever it falls upon a party, that party must accept the unhappy consequences. If the assertion of the privilege leaves plaintiff without sufficient evidence to satisfy a burden of persuasion, plaintiff will lose. If plaintiff's case might be established without the privileged information, dismissal is not appropriate. The same standards apply to defendants.[197]

In either case, the action was a logical outcome of the evidentiary rule.

One of the leading cases on the defense side is *Molerio v. FBI*, where then-Judge Antonin Scalia, writing for the D.C. Circuit, dismissed an FBI applicant's first amendment claim.[198] Only after determining that the privilege had been properly asserted did the court turn to "the difficult issue of the effect" of the privilege. While Molerio could still make out a *prima facie* "circumstantial case permitting the inference that his father's [first amendment-protected] political activities" contributed to the FBI's refusal to hire him," the court, having looked at the underlying evidence, determined that the decision had been based on entirely different information.[199]

Under the *Molerio* line of cases, where the district court "determine[s] that the defendant will be deprived of a valid defense based on the privileged materials, it may properly dismiss the complaint."[200] Courts understand a "valid defense" to mean a defense which "is meritorious and not merely plausible and *would require judgment for the defendant*."[201] Such a situation would entail a miscarriage of justice. A critical first step is judicial scrutiny of the evidence in question. Without that, the D.C. Circuit warned, "virtually every case in which the United States successfully invokes the state secrets privilege would need to be dismissed," replacing "the practice of deciding cases on the basis of evidence" with "a system of conjecture."[202]

From the time of *Reynolds* until the early 21st century, *Totten* was cabined to cases involving a secret agreement on the grounds that a classified contract conveyed an *ex ante* understanding that should a dispute arise, litigation in open court would not be available as an option.[203] There was a world of difference between that context and one in which litigants who had never contracted with the government sought relief for violations of their rights. Accordingly, in 1979, in *Clift v. United States*, the Second Circuit reversed the district court's dismissal of a

---

833 F. Supp. 1486, 1496 (C.D. Cal. 1993) (plaintiff could not make out a prima facie case without the information excluded due to state secrets).

[197] Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268, 270-72 (4th Cir. June 12, 1980) (en banc) (per curiam) (citation omitted) (citing various cases).

[198] Molerio v. FBI, 749 F.2d 815 (D.C. Cir. 1984).

[199] 749 F.2d 825.

[200] *In re* Sealed Case, 494 F.3d 139, 149 (D.C. Cir. 2007).

[201] *Id*. (citing Kasza v. Browner, 133 F.3d 1159, 1166 (9th Cir. 1998) and Tenenbaum v. Simonini, 372 F.3d 776, 777-78 (6th Cir. 2004) as adopting the "valid defense" standard).

[202] *In re Sealed Case*, 494 F.3d at 150.

[203] *See, e.g.*, Clift v. United States, 597 F.2d 826 (1979); Tenet v. Doe, 544 U.S. 1 (2005); General Dynamics Corp. v. United States, 563 U.S. 478 (2011).

complaint when state secrets prevented government documents relating to a patent application from being produced. According to the court of appeals, *Totten* "afford[ed] no support" as the inventor had not entered into any contract. To the contrary, it was *the government's action* (i.e., placing a secrecy order on his patent application) that was at issue.[204] As Justice Gorsuch later explained, "the general rule" in state secrets cases is that "the privilege protects only against the production of certain evidence—not the inconvenience of lawsuits. If a way exists for a court to discharge its statutory duty to entertain a case without the government's privileged proof, that way must be found."[205]

3. Creation of the "Very Subject Matter" Analysis

Post-9/11, as more information about the warrantless electronic surveillance conducted as part of TSP became available and with standing met, the government fell back on state secrets to try to get the suits dismissed. Lacking precedent, it re-crafted the *Totten* bar to read as a "very subject matter" analysis. Initially, the courts rejected this approach: it was hard to uphold a claim that the subject matter was a state secret when the President was giving press conferences about it. The government, nevertheless, persisted. In the torture and rendition cases, with standing met, the government once more collapsed the *Reynolds* evidentiary rule and the *Totten* bar. Those cases now serve as precedent for arguments again being made in the surveillance realm. *Fazaga* serves as an example *par excellence*.

The first time the government appears to have made the "very subject matter" argument—in relation to surveillance—the courts did not go along with it. In *Al-Haramain Islamic Foundation v. Bush*, the FBI accidentally provided a Top Secret document containing sensitive compartmented information (TS/SCI) to an individual who had been determined to be a Specially Designated Global Terrorist.[206] Based on the information provided, Al-Haramain and two U.S. citizens who interacted with the organization brought suit for warrantless electronic surveillance conducted outside of FISA.[207] With standing met, the government turned to state secrets and an broad reading of *Reynolds* to argue for dismissal:

> Here, the "very subject matter" of this lawsuit is a state secret. Plaintiffs allege that they have been the subjects of warrantless surveillance under a classified foreign intelligence program. National security matters are not peripheral to this case; the very goal of this lawsuit is to obtain a determination as to whether NSA has undertaken any warrantless surveillance of Plaintiffs and, if so, whether that action was lawful—including whether the President had authority to establish the program and whether its alleged application to Plaintiffs violated their Constitutional rights.[208]

In light of the fact that virtually all foreign intelligence collection programs are classified, the implication of the government's argument was that *no suit* could ever

---

[204] *Clift*, 597 F.2d 830 (citing and quoting *Totten*, 92 U.S. at 106).
[205] United States v. Zubaydah, 142 S. Ct. 959, 996 (Gorsuch, J., dissenting).
[206] Memorandum in Opposition to Plaintiffs' Opposition to Defendants' Lodging of Material Ex Parte and In Camera, at 2, 7, Al-Haramain Islamic Foundation, Inc. et al v. Bush et al, 451 F.Supp.2d 1215 (D. Or. 2006) , (3:06-cv-00274-KI), ECF No. 32. It took two months for the FBI to request its return. *Id*. at 12. *See also* Al-Haramain Islamic Found. V. Bush, 507 F.3d 1190, 1193 (9th Cir. 2007).
[207] Memorandum in Support of the United States' Assertion of the Military and State Secrets Privilege and Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment, at 3, *Al-Haramain*, 451 F.Supp.2d 1215, (3:06-cv-00274), ECF No. 59.
[208] *Id*. at 5 (quoting *Reynolds*)

be brought challenging surveillance. This is a remarkable proposition, not least because FISA itself both establishes civil liability and contains criminal penalties to address violations.[209] In 2007, the Ninth Circuit rejected the government's assertion on different grounds, noting that the President had already admitted to having undertaken TSP outside FISA's strictures, and remanded the case to the district court to determine whether FISA preempted the state secrets privilege.[210]

As allegations of torture emerged, with standing apparently met, the government once again turned to state secrets and a re-crafting of the traditional test to try to halt litigation. In *El-Masri v. United States*, a German citizen brought suit against the former director of the Central Intelligence Agency and others, alleging that he was captured in Macedonia in December 2003 and subsequently handed over to the CIA, which rendered him to a black site in Afghanistan and proceeded to beat, drug, bind, blindfold, and interrogate him.[211] The complaint asserted three causes of action: a Bivens claim regarding El-Masri's fifth amendment right to due process and two violations of the Alien Tort Statute (contravention of the international legal norms against arbitrary detention and cruel, inhuman, or degrading treatment).[212]

In its brief to the Fourth Circuit, the government collapsed *Reynolds* and *Totten*, arguing that state secrets were so central to the suit that it could not proceed without disclosing them. In support of this proposition, it cited to the Fourth Circuit's 1985 decision in *Fitzgerald v. Penthouse Int'l*, stating that it stood for the general proposition that where "the unavailability of the information protected by the privilege precludes either the plaintiff or defendant from establishing their respective legal positions on the issues in the case, then the case must be dismissed."[213]

In *Fitzgerald*, however, the central question turned on a contractual claim: whether a scientist could testify about whether he was undertaking marine animal research under a classified contract with the CIA.[214] Similarly, in *Sterling v. Tenet*, a covert agent in the CIA brought a Title VII racial discrimination claim against his employer.[215] The Fourth Circuit in *Sterling* concluded that a trial "would require disclosure of highly classified information concerning the identity, location, and assignments of CIA operatives."[216] Both cases, like *Totten*, turned on voluntary entrance into a (secret) contractual relationship with the government. In such circumstances, both parties had *ex ante* knowledge that a future suit could risk sensitive national security concerns, making legal action unavailable. In *Totten*, Justice Stephen Field had explained,

> The service stipulated by the contract was a secret service; the information sought was to be obtained clandestinely, and was to be communicated privately; the employment and the service wee to be equally concealed. Both employer and agent must have understood that the lips of the other were to be for ever sealed respecting the

[209] 50 U.S.C. §1809 (imposing a fine of not more than $10,000 or imprisonment of up to five years for either engaging in electronic surveillance outside of either FISA or Title III or disclosing or using such information—both of which appear to be at issue in the case of Al-Haramain).
[210] Al-Haramain Islamic Found. V. Bush, 507 F.3d at 1193.
[211] *El-Masri*, 479 F.3d 296, 300 (4th Cir. 2007).
[212] Complaint, El-Masri v. Tenet et al, Docket No. 1:05-cv-01417 (E.D. Va. Dec. 6, 2005). *See also El-Masri*, 479 F.3d 300-301.
[213] *Id.* at *35.
[214] *See* Fitzgerald v. Penthouse Intern., Ltd., 776 F.2d 1236 (4th Cir. Nov. 7, 1985). The government also made brief reference to *Farnsworth Cannon, Inc. v. Grimes*. *See* Farnsworth Cannon, Inc. v. Grimes, 635 F.2d 268 (4th Cir. June 12, 1980).
[215] Sterling v. Tenet, 416 F.3d 338 (4th Cir. Aug. 3, 2005).
[216] *Id.* at 341.

> relation of either to the matter. This condition of the engagement was implied from the nature of the employment.[217]

The complaint in *El-Masri* was about something entirely different: whether *the government's unilateral actions* had violated El-Masri's rights by subjecting him to extraordinary rendition. Under *Reynolds*, the appropriate response would have been to exclude whichever documents met the standard, and then to proceed. If the litigant could not make out a *prima facie* case, the suit should be dismissed.[218] Alternatively, if the government could not present a meritorious defense without certain information, then the court, after reviewing the material, could dismiss the suit as a logical outcome of applying the evidentiary rule. In *El-Masri*, the Fourth Circuit in 2007 did neither, instead accepting the government's newly-minted "very subject matter" approach.

In a similar action the following year, *Mohamed v. Jeppesen*, five foreign nationals brought a civil suit against a defense contractor, alleging its role in their forced disappearance, torture, and inhumane treatment as part of the CIA's extraordinary rendition program.[219] Once again, the United States intervened and sought dismissal. As in *El-Masri*, the government argued that "the very subject matter of plaintiffs' claims is a state secret."[220] Embedded in this assertion, however, was one that had more purchase: the plaintiff's argument turned on a contractual relationship between *Jeppesen* and the CIA. Had the suit been a matter of dispute between Jeppesen and the agency, then *Totten* would at least be available. But it was not. To the contrary, it was a civil action against a private company, making the *Reynolds* evidentiary rule more appropriate. Assumedly, Jeppesen would have sought information about the contractual relationship to mount a defense—which may (or may not) have led to the same conclusion (dismissal of the suit), but this would have been a logical outcome of the evidentiary rule. Instead, the government asserted the much broader claim.

The problem with the "very subject matter" approach is that it puts the government in a position of insulating itself from accountability. *As long as a program is classified,* then *any* constitutional challenge to it can be defeated. This is precisely what has happened as similar arguments have begun to infuse the surveillance realm.

In its brief in *Fazaga*, the government cited the federal district court's 2008 decision in *Jeppesen thirteen times* to support its "very subject matter" claim.[221] Because the issue involved a classified matter, "[l]itigating the case to a judgment on the merits would present an unacceptable risk of disclosing state secrets."[222] The government, quoting a case quoting *Totten*, explained, "Where, as here, the privileged evidence goes to the heart of a claim, that claim cannot be litigated, and dismissal is compelled."[223] But this is not at all what *Totten* held. *Totten* held that individuals entering into a classified contract with the government had *ex ante* notification that future disputes were unlikely to reach the light of day in a courtroom. That was part of the deal. It was a different context than situations challenging

---

[217] Totten v. United States, 92 U.S. 105, 106 (1875).
[218] This was why it mattered that there was already information in the public domain, such as the Council of Europe's 2006 draft report on rendition and detention, and the government's own release of information about the CIA program. *See El-Masri*, 479 F. 3d at 302.
[219] Mohamed v. Jeppesen Dataplan, Inc., 539 F. Supp. 2d 1128 (N.D. Cal. 2008).
[220] Redacted, Unclassified Brief for Intervenor-Appellee the United States, Mohamed v. Jeppesen Dataplan, Inc., 539 F. Supp. 2d 1128 (N.D. Cal. 2008) (No. 08-15693) 2008 WL 4973859.
[221] Brief for the Federal Appellees, *Fazaga v. FBI* (12-56874) BL-43 pp. 2, 11, 23, 41, 42, 47, 51, 52, 53, 61, 63.
[222] *Id*. at 2 (internal quotations and citations omitted). *See also id.* at 47, 51, 52.
[223] *Id*. at 53.

unilateral government actions that allegedly violate statutory law and the constitution.[224]

In tandem with the "very subject matter" analysis is a second argument advanced by the government to support dismissal: namely, "when litigation would risk or require the disclosure of information protected by the state secrets privilege."[225] This assertion appeared in abbreviated form in conjunction with the first re-crafting of state secrets in 2006 in *Al-Haramain*.[226] It rests on the *hypothetical* possibility that privileged information might, in the future, be released which may then impact U.S. national security. This argument evokes the spectre of Justice Scalia's concern in *Molerio*, when he warned against entering the realm of conjecture as grounds on which to deny rights.[227]

The government also argues in conjunction with its "very subject matter" claim that once privileged information is removed, "there is no basis for a court to evaluate that privileged evidence to determine whether a party's contentions are correct or whether a party's claims or defenses would prevail if the state secrets had not been excluded. Indeed, it would be improper for a court to seek to assess the merits of the parties' claims or defenses if doing so would require consideration of privileged evidence."[228] Yet this is precisely how, for centuries, the privilege worked, particularly in light of the potential miscarriage of justice should the defense be deprived of critical evidence.

B. Dismissal at the Pleadings Stage

A second novel move made in the post-9/11 environment is the assertion of state secrets early in suits to argue for dismissal. This approach departs from the traditional use of state secrets during the discovery process. Courts historically have jealously guarded this line.

In the 1957 case of *Halpern v. United States*, for instance, the government moved to dismiss without prejudice an action brought by the plaintiff under the Inventive Secrecy Act of 1951 seeking compensation for damage caused by a secrecy order entered by the government against the plaintiff's patent.[229] The federal district court noted that the state secrets privilege provides an exemption from the

---

[224] In *Wikimedia*, the Fourth Circuit, buying into the government's argument erred. It determined that state secrets could be invoked under three conditions:

> (1) 'the plaintiff cannot prove the prima facie elements of his or her claim without privileged evidence'; (2) 'even if the plaintiff can prove a prima facie case without resort to privileged information, . . . the defendants could not properly defend themselves without using privileged evidence'; and (3) further litigation would present an unjustifiable risk of disclosure.'

Wikimedia Found. v. Nat'l Sec. Agency/Cent. Sec. Serv., 14 F.4th 276, 303 (4th Cir. 2021) (quoting Abilt v. CIA, 848 F.3d 305, 313-14 (4th Cir. 2017) (footnote omitted)). The first two conditions are entirely consistent with how state secrets have consistently operated. The last condition, however, applies only to the *Totten* line of cases—indeed, the court cited to *Abilt v. CIA* in support of its proposition, a case in which a covert CIA employee sued the agency for discriminating against him for having narcolepsy and taking periodic naps while working. *Abilt*, 848 F.3d at 309.

[225] Brief for Intervenor-Appellee United States, Sakab Saudi Holding Co. v. Aljabri, 578 F. Supp. 3d 140 (D. Mass. 2021); 2022 WL 2275195 * *see* Government Brief, Docket No. 22-0152, Doc. BL-50.

[226] Al-Haramain Islamic Foundation, Inc. v. Bush, 451 F.Supp.2d 1215, 1225 ("Litigating this matter will necessarily require, and risk, the disclosure of state secrets.")

[227] *See, e.g., id.* at *3 ("When full litigation of claims and defenses would require a court to evaluate privileged evidence on which a party relies, thereby risking or requiring the disclosure of privileged information that is excluded from the suit, the court should dismiss the suit.")

[228] *Id.*

[229] Halpern v. United States, 151 F.Supp 183 (S.D.N.Y. 1957).

testimonial duty; as a result, with no testimonial duty present the privilege assertion was premature.[230] Two years later, in *United States v. 62.50 Acres of Land More or Less Situated in Lake County Ohio*, the government sought to condemn a parcel of land and to use it as a ballistic missile launcher site.[231] The government objected to the admission of interrogatories related to an explosion at the Middletown, New Jersey Nike site and moved that they be stricken.[232] Citing *Reynolds* and *Halpern*, the court ruled that the claim of privilege was premature.[233]

Prior to 9/11, courts took a similar view of efforts to assert state secrets early in suits alleging unconstitutional surveillance. In *In re United States of America*, for instance, the plaintiff brought a claim under the Federal Tort Claims Act, alleging that injuries to her and her deceased husband from COINTELPRO, conducted by the FBI 1950 to 1964.[234] The district court rejected the government's assertion and directed the FBI to answer the complaint.

Post-9/11, the government changed course. In *El-Masri*, it intervened at the pleading stage and asserted state secrets.[235] It argued, "there is no categorical rule that the state secrets privilege can be asserted only in response to discrete discovery requests."[236] It then cited three cases, none of which applied. The first, *Sterling v. Tenet*, dealt with an employment contract at the CIA—a case clearly in the *Totten*, not the *Reynolds*, line of cases. The second, *Salisbury v. United States*, was a FOIA case involving a national security exception—not a state secrets case.[237] The third, *DTM Research, L.L.C. v. AT&T Corp*, dealt with trade secrets—not state secrets.[238] The reason there was no rule against it was because state secrets always had operated during discovery or in the course of the trial as an evidentiary rule. The government made a similar move in *Jeppesen*: after the plaintiffs filed the First Amended Complaint, but prior to the defendant's response or any undertaking of discovery, the United States intervened, asserted state secrets, and requested dismissal of the suit.[239]

The government's recourse to state secrets early in litigation carried over to other suits—which then cited to the rendition cases in support. Thus, in *Husayn v. Mitchell*, the government relied heavily on *Jeppesen*. The same occurred in *Sakab Saudi Holding Co. v. Aljbri* and *Kareem v. Haspel*.[240] In *Fazaga*, the government again cited *Jeppesen* in support of asserting the claim at the pleadings stage.[241] According to the government, plaintiffs' claims as to religious discrimination in *Fazaga* could not even move into the discovery stage without jeopardizing national security.[242]

C. From Particularity to Generality

---

[230] *Id.*
[231] US v 62.50 Acres of Land More or Less Situated in Lake County Ohio, 23 F.R.D. 287, 288 (N.D. Ohio 1959).
[232] *Id.*
[233] *Id*.
[234] In re United States, 872 F.2d 472 (D.C. Cir. 1989).
[235] Brief of the Appellee, 2006 WL 2726281, at *12.
[236] Brief of the Appellee, 2006 WL 2726281, *12; See Sterling v. Tenet, 416 F.3d 338, 341-42 (4th Cir. 2005).
[237] *See* Salisbury v. United States, 690 F.2d 966 (D.C. Cir.1982).
[238] *See* DTM Rsch. LLC. V. AT&T Corp., 235 F.3d 327, 334 (4th Cir. 2001).
[239] Redacted, Unclassified Brief for Intervenor-Appellee the United States, 2008 WL 4973859, No. 08-cv-15693 (9th Cir. Aug. 27, 2008).
[240] *See* Sakab Saudi Holding Co. v. Aljabri, 578 F.Supp. 3d 140 (D. Mass. 2021)
[241] Brief for the Federal Appellees, Fazaga v. FBI, 13-cv-55017 at 3 (Mar. 17, 2015).
[242] *Id*.

For centuries, the state secrets privilege applied to *particular* documents or testimonial information that could not enter litigation.[243] In 1910, in *In Re Grove*, for instance, the Secretary of the Navy initially asserted it over "the plans, drawings, specifications, and other illustrative and descriptive papers . . . relating to the construction and operation of the steam turbines" embedded in torpedo boat destroyers.[244] He later capitulated, allowing the documents to be used in litigation. In *The Wright and the Papoose*, a case in admiralty, the plaintiff sought discovery of the records of the Naval Court of Inquiry on May 31, 1931 regarding the collision.[245] Since no secrecy had been preserved during the hearing, the court considered the argument as to the danger of granting the motion to withhold the information "not very impressive."[246]

Courts repeatedly have focused on which documents, in particular, should be excluded. In *Republic of China v. National Union Fire Insurance*, the federal judge in 1956 excluded an order in council from the British government, two letters from the Secretary of state and replies by Britain, and one statement by the British Foreign Office.[247] In *Zuckerbraun v. Gen. Dynamics Corp*., the Secretary of the Navy in 1990 exercised the privilege over the rules of engagement authorized for, and military orders applicable to, the USS Stark at the time of the incident being litigated, as well as information regarding the design, performance, and functional characteristics of the combatant ships and the weapons and defense systems installed on them.[248] Case after case followed course.[249]

Over the past 15 years, however, the government has increasingly begun to assert state secrets over entire categories of information.[250] The trend began as early as 2006, with *Al-Haramain*, in which the government asserted the privilege over "(i) information regarding the al Qaeda threat; (ii) information regarding the Terrorist Surveillance Program; and (iii) information that would confirm or deny whether

---

[243] *See supra* note 150 and Duncan v. Cammell, Laird & Co., (1942) A.C. 624.
[244] In re Grove, 180 F. 62, 65-66 (3d Cir. 1910).
[245] The Wright, 2 F.Supp. 43(E.D.N.Y. 1932); *see also* Anglo-Saxon Petroleum Co. v. United States, 78 F.Supp. 62 (D. Mass. 1948) (seeking an order directing the United States to produce the transcript from a particular Naval Board of Inquiry).
[246] *The Wright*, 2 F.Supp.43.
[247] Republic of China v. National Union Fire Insurance, 142 F. Supp. 551 (D. Md. 1956).
[248] Zuckerbraun v. General Dynamics Corp., 755 F. Supp. 1134, 1139 (D. Conn. 1990).
[249] *See, e.g.*, Pollen v. Ford Instrument Co., 26 F. Supp. 583, 583-84 (E.D.N.Y. 1939) (noting where the U.S. Navy exerted the privilege over "drawings showing the construction of range keepers or other apparatus for determining sighting data for guns."); Firth Sterling Steel Co. v. Bethlehem Steel Co., 199 F. 353 353-56 (E.D. Pa. 1912). (excluding and expunging certain drawings relating to armor-piercing projectiles); United States v. Haugen, 58 F. Supp. 436 (E.D. Wash. 1944) (detailing a contract relating to construction of a nuclear power plant).
[250] *See, e.g.*, In re Terrorist Attacks on September 11, 2001, 523 F.Supp.3d 478, 499 (S.D.N.Y. 2021) (government asserting state secrets privilege over subject information, reasons for investigation and results, sources and methods, and foreign government information and information sharing with foreign partners); Defs.' Req. That the Ct. Discharge the Order to Show Cause and Deny Pl.'s Req. for Access to the Classified Steinbach Declaration, or, in the Alternative, Mot. to Dismiss in Light of the Att'y General's Assertion of the State Secrets Privilege at 10, Twitter v. Barr, , No. 4:14-cv-04480-YGR (N.D. Cal. Mar. 15, 2019) (government asserting the state secrets privilege over four categories, including "Information Regarding How Adversaries May Seek to Exploit Information Reflecting the Government's Use of National Security Legal Process"); Mitchell v. United States, No. 16-MC-0036-JLQ (E.D. Wash. May 31, 2017), ECF No. 91 (government asserting privilege over seven categories, ranging from "information identifying individuals involved with the" CIA interrogation program to "information concerning the CIA's internal structure and administration"); Ibrahim v. Dep't of Homeland Sec., No. 06-00545 (WHA), 2013 WL 4549941, at *4-5 (N.D. Cal. Aug. 23, 2013) (government asserting state secrets privilege over information related to subject identification, the reasons for investigations and their results, and sources and methods employed in counterterrorism operations).

Plaintiffs have been targeted for surveillance under the TSP or any other program."[251] Although there was information in the public domain about the first two categories—including from the President himself—the government cast the net widely to prevent further information from becoming public.

The torture and rendition cases again proved instrumental. In *Mohamed v. Jeppesen*, General Michael Hayden, the Director of the CIA, submitted a classified declaration detailing "the scope of information" subject to state secrets and harms that might follow, should such matters be publicly released.[252] Hayden identified "several categories of information implicated by" the case: any information that would tend to confirm or deny whether any private entity or foreign government assisted the CIA on clandestine intelligence activities; any information about the scope or operation of the CIA's detention and interrogation program—including site locations, methods of interrogation, and identity of prisoners; and any additional information regarding CIA activities, sources, or methods.[253]

This approach continues to mark cases relating to the interrogation and rendition programs. In 2019, for instance, responding to a request from the Polish government that two former CIA contractors testify about the detention and transfer of prisoners for coercive interrogation, the government intervened and asserted state secrets over seven topics:

> (1) information that could identify individuals involved in the CIA detention and interrogation program; (2) information regarding foreign government cooperation with the CIA; (3) information pertaining to the operation or location of any clandestine overseas CIA station, base, or detention facility; (4) information regarding the capture and/or transfer of detainees; (5) intelligence information about detainees and terrorist organizations, including intelligence obtained or discussed in debriefing or interrogation sessions; (6) information concerning CIA intelligence sources and methods, as well as specific intelligence operations; and, (7) information concerning the CIA's internal structure and administration.[254]

These categories encompassed a report issued by the SSCI on the CIA's use of enhanced interrogation techniques; a ruling issued by the European Court of Human Rights regarding treatment of a prisoner held in Guantánamo Bay; testimony provided in court by former CIA contractors who designed and carried out the post-9/11 interrogation program; and a memoir published by one of the contractors.[255] That such information was public did serve as formal acknowledgement of the location of the black sites, but the CIA's rationale for withholding *all* such information, on the grounds that something contained in these categories might mention "Poland" or Polish officials (particularly in light of the fact that it was polish officials requesting the information), stretches credulity. Under the government's

---

[251] Mem. of Points and Authorities in Support of the United States' Assertion of the Military and State Secrets Privilege and Defendants' Mot. to Dismiss or, in the Alternative, for Summary Judgment at 4, Al-Haramain Islamic Found., Inc. v Bush, 451 F.3d 1190 (9th Cir. 2007) (No. 3:06-cv-00274).
[252] Redacted, Unclassified Brief for Intervenor-Appellee the United States, 2008 WL 4973859. *See generally* Mohamed v. Jeppesen Dataplan, Inc., 539 F. Supp. 2d 1128 (N.D. Cal. 2008).
[253] Redacted, Unclassified Brief for Intervenor-Appellee the United States, 2008 WL 4973859.
[254] Husayn v. Mitchell, 938 F.3d 1123, 1132 (9th Cir. 2019).
[255] *See* Report of the Senate Select Committee on Intelligence, Committee Study of the Central Intelligence Agency's Detention and Interrogation Program, S. Rep. 113-288, (Dec. 9, 2014), https://www.intelligence.senate.gov/sites/default/files/publications/CRPT-113srpt288.pdf; Case of Abu Zubaydah v. Lithuania, Judgment, Strasbourg, Eur. Ct. H.R., May 31, 2018; J. MITCHELL & B. HARLOW, ENHANCED INTERROGATION: INSIDE THE MINDS AND MOTIVES OF THE ISLAMIC TERRORISTS TRYING TO DESTROY AMERICA (2016); United States v. Zubaydah, 142 S.Ct. 959 (2022).

approach, even the CIA's copy of SSCI's Report would fall subject to state secrets. These categories, moreover, incorporate a significant amount of utterly unrelated material. The seventh category, for instance, ("information concerning the CIA's internal structure and administration"), appears to include everything from the name of the current Director of the CIA to the Agency's (unclassified) organization chart—currently available on Wikimedia.[256]

The categorical approach has spread to other kinds of national security-related suits, in some cases verging on the absurd. In *Twitter v. Barr*, for instance, the executive in 2019 asserted state privilege over four categories, including, inter alia, "Information Regarding How Adversaries May Seek to Exploit Information Reflecting the Government's Use of National Security Legal Process." [257] Assumedly, this would include every official report required by FISA, as well as a significant amount of scholarship.

In *Wikimedia*, a case challenging programmatic collection under Section 702, the government in 2021 asserted the privilege over seven topic areas:

> (1) "Entities subject to Upstream surveillance activities";
> (2) "Operational details of the Upstream collection process";
> (3) "Location(s) on the Internet backbone at which Upstream surveillance is conducted";
> (4) "Categories of Internet-based communications subject to Upstream surveillance activities";
> (5) "the scope and scale on which Upstream surveillance is or has been conducted";
> (6) "NSA decryption capabilities"; and
> (7) "Additional categories of classified information contained in opinions and orders issued by, and in submissions made to, the FISC."[258]

These categories included information not just in the public domain but which *the government itself* had already released. The Fourth Circuit did not seem at all bothered by this, reading the lower court's decision as merely limiting "*additional* information related to those categories."[259]

That approach, however, made two false assumptions: first, that all material not yet released threatens national security; and second, that all material *in these categories* threatens national security. The first is demonstrably false: all sorts of information not previously released by the government does not rise to the level of potentially causing grave harm if released. Such documents are constantly being sought across the government through FOIA requests and, when ignored or blocked, litigation. Simply because information hasn't been released has no bearing on its national security qualities. As for the later claim, the fact that information in each of these categories is already public—at apparent no risk to national security—defies the assumption.

---

[256] See CIA Org Chart May 14, 2009, available at https://commons.wikimedia.org/wiki/File:Cia_org_chart_2009_may_14.jpg.

[257] Defs.' Req. That the Ct. Discharge the Order to Show Cause and Deny Pl.'s Req. for Access to the Classified Steinbach Declaration, or, in the Alternative, Mot. to Dismiss in Light of the Att'y General's Assertion of the State Secrets Privilege at 10, Twitter v. BarrNo. 4:14-cv-04480-YGR (N.D. Cal. Mar. 15, 2019).

[258] Defs.' Mem. at 7–8, No. 1:15-cv-00662-TSE (D. Md. Apr. 28, 2018), ECF No. 138.

[259] Wikimedia Foundation v. National Security Agency/Central Security Service, 14 F.4th 276, 302 (4th Cir. 2021); *see also* Wikimedia Foundation v. National Security Agency, 427 F.Supp. 3d 582, 611 (D. Md. 2019).

In *Fazaga*, the government again adopted a categorical approach. The Attorney General asserted state secrets over three general areas:

> (1) *Subject Identification*: Information that could tend to confirm or deny whether a particular individual was or was not the subject of an FBI counterterrorism investigation, including in Operation Flex.
>
> (2) *Reasons for Counterterrorism Investigations and Results*: Information that could tend to reveal the initial reasons (i.e. predicate) for an FBI counterterrorism investigation of a particular person (including in Operation Flex), any information obtained during the course of such an investigation, and the status and results of the investigation. This category includes information obtained from the U.S. Intelligence Community related to the reasons for an investigation.
>
> (3) *Sources and Methods*: Information that could tend to reveal whether particular sources and methods were used in a counterterrorism investigation of a particular subject, including in Operation Flex. This category includes previously undisclosed information related to whether court-ordered searches or surveillance, confidential human sources, and other investigative sources and methods, were used in a counterterrorism investigation of a particular person, the reasons such methods were used, the status of the use of such sources and methods, and any results derived from such methods.[260]

The FBI added a catch-all: "This description of the broad categories of information subject to the Attorney General's claim of privilege is not meant to foreclose the possibility that other information related to FBI counterterrorism investigations including Operation Flex may be identified in later proceedings as subject to privilege."[261]

Once again, these categories incorporate information already in the public domain—much of it put there by the government. They envelop law enforcement data that the public has a right to know and which is necessary to ensure that the FBI acts within its lawful limits. Within these categories, moreover, the possibility that the government may overclaim the national security risks is significant, not least because it has a long history of doing precisely that.

In 2018, District Court Judge Anthony Trenga published an article in the *Harvard National Security Journal* analyzing how state secrets privilege plays out in the courts.[262] Addressing the increased frequency and scope of government assertions, he underscored the importance of the judicial role in challenging "overstated or, in fact, baseless" government claims.[263] Interviewing 31 of his colleagues on the federal bench, Judge Trenga noted "[t]he willingness of more experienced judges to probe deeper," speculating that it related in part "to their commonly held belief that, with effort, most issues of disclosure can be resolved in a way that allows the litigation to proceed."[264] Several of the judges he interviewed,

---

[260] Public Declaration of Mark F. Giuliano, Federal Bureau of Investigation, Case No. SACV11-00301 CJC, Fazaga v. FBI, (Aug. 1, 2011), at 52-53, https://www.supremecourt.gov/DocketPDF/20/20-828/185460/20210730194627462_20-828ja.pdf.
[261] *Id*.
[262] Anthony John Trenga, *What Judges Say and Do in Deciding National Security Cases: The Example of the State Secrets Privilege*, 9 HARV. NAT'L SEC. J. 1 (2018).
[263] *Id*. at 2, 49-51.
[264] *Id*. at 49.

"talked about how the scope of a privilege claim narrows substantially once a judge 'pushes back.'"[265] One put the number as high as fifty percent of the time.[266] Judges could often find a way to allow the suit to move forward "by working through the parties' specific needs of particular pieces of information".[267] It was a matter of being willing to get into the details of a case. Trenga wrote,

> Several other judges, particularly those with substantial state secrets experience . . . , some with a background in law enforcement, saw . . . the initial assertion of privilege claims broader than the government can ultimately defend and attributed this conduct, in various articulations, to an attempt, for the most part, to avoid "the hard analysis' and the sometimes tedious and difficult task of separating protected information from non-protected information until a judge reacts adversely.[268]

Some of the judges further highlighted "concern[] about a 'bureaucratic habit' to assert the privilege in 'too rote a fashion.'"[269]

Judge Trenga's findings align with numerous cases in which the government has over-stated the national security risks at stake in releasing information publicly. The No Fly List cases provide a good example. In the 2014 case *Ibrahim v. Dep't of Homeland Sec.*, a visa holder argued that her inclusion on the federal No Fly List violated her constitutional rights.[270] The government initially invoked an evidentiary state secrets privilege but subsequently reversed its position, arguing for summary judgment on state secrets grounds.[271] When the case when to trial, however, the government conceded that the plaintiff had never actually presented a threat to the United States. An FBI agent had merely misunderstood the form that he had filled out which resulted in her being placed on the list.[272] The following year, in *Mohamed v. Holder*, the government once more moved for summary judgment on state secrets grounds.[273] Following *in camera* review, the federal district court "conclude[d] that there is no information protected from disclosure under the state secrets privilege that is necessary" for the litigation to proceed.[274]

Overbroad claims mark government representations in parallel national security realms. The FOIA context has already been addressed.[275] The same could be said of representations to specialized Article III courts about what materials can be made public. In 2013, for example, the ACLU, along with numerous media organizations and legislators from both sides of the aisle, filed a motion requesting that the court release its opinions interpreting Section 215.[276] The government identified one opinion and, without any explanation, stated that it would be withheld in full. The FISC expressed its concern that the government had not provided any rationale as to why the information could not be released.[277] The government shifted

---

[265] *Id*.
[266] *Id*.
[267] *Id*. at 50.
[268] *Id*. at 51.
[269] *Id*. (internal citation omitted).
[270] Ibrahim v. Dep't of Homeland Sec., 62 F. Supp. 3d 909 (N.D. Cal. 2014).
[271] *Id.* at 914.
[272] *Id.* at 915-916.
[273] Mohamed v. Holder, 2015 U.S. Dist. LEXIS 92997, at *4-5 (E.D. Va. July 16, 2015).
[274] *Id*.
[275] S*ee* discussion, *infra*.
[276] Opinion and Order, *In re Orders of this Court Interpreting Section 215 of the Patriot Act*, No. Misc. 13-02, GID.C.00085, 2013 WL 5460064 (FISA Ct. Sept. 13, 2013) (Saylor IV, J.).
[277] *Id.* at 9.

course and agreed to publish parts of the opinion.[278] After more pressure from the court and its staff, the government agreed that "certain additional information" could be released—apparently with no risk to national security.[279] These cases underscore the dangers inherent in the categorical approach increasingly adopted by the government: it sweeps in significant amounts of information already in the public domain while preventing other, important information, which does not present any sort of risk to national security, from reaching light of day.

D. Judicial Authority versus Executive Branch Constitutional Power

In yet another departure from how the state secrets privilege has historically been treated, the government has begun to argue that it is a constitutionally-derived Article II authority.[280] In its brief to the Supreme Court in *Fazaga*, the government stated, "[a]ny ambiguity in Section 1806(f) must be resolved in favor of retaining the *constitutionally based* state secrets privilege."[281] For the government, the President's commander-in-chief powers as well as his "authority to 'make Treaties,' to 'appoint Ambassadors,' and to otherwise conduct the Nation's foreign affairs," accords the executive the primary responsibility for the conduct of foreign relations.[282]

Conspicuously missing from the brief was any reference to the foreign affairs and military powers provided to Congress in Article I(8).[283] Absent, too, was any reference to the advice and consent clause and the role of the Senate in making treaties or appointing ambassadors or other public ministers and consuls.[284]

The government also failed to acknowledge the myriad ways in which Congress gives effect to its foreign affairs and war powers *by regulating sensitive national security information*. The legislature has gone to great length in FISA to ensure that information obtained from electronic surveillance, physical search, pen registers and trap and trace equipment, and access to business records remains secret.[285] The Atomic Energy Act of 1954 requires protection against unauthorized disclosure of any restricted data, as defined in the statute.[286] The Classified Information Procedures Act provides, in turn, for the admission of classified information at trial, establishing rules for, inter alia, pretrial conference, protective orders, discovery, notice, and the sealing of records in in camera hearings.[287] Four different statutes encapsulating five different requirements regulate national security

[278] *Id.*
[279] *Id.*
[280] Brief for the Petitioners, Fed. Bureau of Investigation v. Fazaga, No. 20-828, at 42 ("The state-secrets privilege is firmly rooted in the Constitution as well as the common law."). *See also id.* at 43 (stating, "The privilege . . . is . . firmly rooted in the Constitution.")
[281] *Id.* at 42 (emphasis added).
[282] *Id.* at 42-43.
[283] *See, e.g.,* U.S. CONST., Art. I § 8 cl. 10 ("To define and punish Piracies and Felonies committed on the high Seas, and Offences against the Law of Nations"); *Id.* cl. 10 ("To declare War, grant Letters of Marque and Reprisal, and make Rules concerning Captures on Land and Water"); Art. I(8)(12) ("To raise and support Armies"); *Id.* cl. 13 ("To provide and maintain a Navy"); *Id.* cl. 14 ("To make Rules for the Government and Regulation of the land and naval Forces"); I(8)(15) ("To provide for calling forth the Militia to execute the Laws of the Union, suppress Insurrections and repel Invasions"); *Id.* cl. 16 ("To provide for organizing, arming, and disciplining, the Militia"); and I cl. 18 ("To make all Laws which shall be necessary and proper for carrying into Execution the Foregoing Powers, and all other Powers vested by this Constitution in the Government of the United States, or in any Department or Officer thereof.").
[284] *Id.* Art. II cl. 2.
[285] *See* 50 USC §§1801 ff.
[286] *See* 42 U.S.C. §2014(y).
[287] *See* Classified Information Procedures Act, Pub. L. 96-456; 94 Stat. 2025 (Oct. 15, 1980), as amended through Pub. L. 111-16 (May 7, 2009).

letters.[288] Congress has insisted on gag orders, provided for delayed-notice search warrants, and taken numerous other steps to regulate access to national security information.[289]

In its brief to the Court, however, the government sidelined all of this, instead underscoring the Executive's "enormous power in the two related areas of national defense and international relations", suggesting that because state secrets privilege "relate[s] to the effective discharge" of that power, it is a constitutional power.[290]

In addition to overlooking Congress's substantial foreign affairs and war powers and numerous legislative acts regulating sensitive national security information, the government failed to consider several flaws in its argument. First, and most obviously, as an historical matter it is simply false that state secrets has always operated as an Article II constitutional power. As the earlier discussion demonstrates, state secrets has *always* been a common law rule. For the *Reynolds* and *Totten* lines of cases, the privilege derives from the exercise of Article III power, not from an authority assigned to Article II.

Like the collapse of the *Reynolds* evidentiary rule and *Totten* bar, the slippage appears to stem from the post-9/11 torture and interrogation cases and application to the surveillance realm. In its brief in *El-Masri*, the government opined on "The Nature of the State Secrets Privilege", suggesting that it is not merely a privilege, but rather, "the means by which the Executive Branch exercises its critical constitutional responsibility to protect secrets of state in the national interest."[291] Citing *dicta* in *United States v. Nixon* (which focused on executive privilege in relation to Presidential recordings), the government rather generously attributed to the Supreme Court the position "that state secrets privilege is rooted in, and is an aspect of, the powers granted to the President by Article II of the Constitution."[292]

In actual fact, all that the Court did in *Nixon* was to mention in passing the president's "article II duties" in regard to "military or diplomatic secrets".[293] The

---

[288] *See* Right to Financial Privacy Act of 1978, 12 U.S.C. §§3401-22; Electronic Communication Privacy Act of 1986, 18 U.S.C. § 2709; Fair Credit Reporting Act of 1970, 15 U.S.C. §§ 1681u, 1681v; National Security Act of 1947, 50 U.S.C. §3162.

[289] *See, e.g.,* USA PATRIOT Act, § 213 (authorizing sneak and peek search warrants); § 505 (forbidding recipients of NSLs from sharing the information with anyone else). In 2008, the Second Circuit found that the gag orders and lack of judicial review constituted a violation of the First Amendment.

[290] *Id.* at 44-45 (internal citations and quotations omitted); *see also* Fazaga government brief to the Ninth Circuit, at 54 (citing *El-Masri* in support of its reference to "the Executive Branch's constitutional authority to exercise control over information whose disclosure would jeopardize national security") In its brief to the Fourth Circuit in *Wikimedia*, the government argued against interpreting Section 1806(f) as "Congress's intent. . . to displace the longstanding *and constitutionally grounded* privilege." *See* Appellee's Br. At 11 in Wikimedia Foundation v. NSA/CSS, 14 F.4th 276 (4th Cir. 2021) (emphasis added). "This longstanding feature of our legal system enables the Executive Branch to fulfill its constitutional duties. As the Supreme Court has made clear, "[t]he authority to protect [national-security] information falls on the President as head of the Executive Branch and as Commander in Chief." [] And executive privileges that "relate[] to the effective discharge of a President's powers" are "constitutionally based." [] This Court has thus correctly recognized that the state- secrets privilege has "a firm foundation in the Constitution" and "performs a function of constitutional significance" because "it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities." *Id.* at 32 (internal citations omitted).

[291] Brief of the Appellee, 2006 WL 2726281, at *8.

[292] *Id.*

[293] *Nixon*, 418 U.S. at 710 (*Pari passu*, the case cited within *Nixon* (*Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp*.) focused on transportation routes between the United States and foreign countries. State secrets was nowhere to be found. Instead, the Court asserted that on such matters of foreign affairs, it should be deferential to the executive branch. Chicago & Southern Air Lines v. Waterman S.S. Corp, 333 U.S. 103, 111 (1948) ("Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative. They are delicate, complex, and involve large elements of prophecy.").

government's brief in *El-Masri* went on to cite to *United States v. Curtiss-Wright Export Corp*, again referencing the President as "the sole organ of the federal government in the field of international relations", to conclude in a non-sequitur that the state secrets privilege has "a substantial constitutional basis."[294]

According to the government, "The privilege is not merely a manifestation of a decision to classify national security information. Rather, it is a separate, carefully delineated exercise of Executive authority pursuant to the Constitution's allocation of responsibility to protect the Nation's Security."[295] The Fourth Circuit in *El-Masri* gave a nod to the government's claim, stating "Although the state secrets privilege was developed at common law, it performs a function of constitutional significance, because it allows the executive branch to protect information whose secrecy is necessary to its military and foreign-affairs responsibilities."[296] The court stopped short of grounding it in an Article II power, merely stating that state secrets operates in effect as judicial acknowledgment of the role of the executive.[297]

Second, relatedly, there is a distinction to be drawn between an evidentiary rule that takes notice of constitutional responsibilities and one that *derives* from constitutional power afforded the executive. There is a logical disconnect between the courts acting on their inherent power and, from this, the executive deriving an independent constitutional authority to prevent information from being presented in a judicial context. State secrets is a common law, judicially-created rule. Indeed, it could be argued that efforts by the executive branch to usurp the privilege by asserting it as an Article I power amounts to an unconstitutional exercise of Article III authorities. Allowing or excluding evidence goes directly to the case or controversy clauses and the judiciary's obligation to ensure that justice ensues. This is why courts at times dismiss suits based on state secrets either because a plaintiff cannot make out a *prima facie* case without the evidence, or because defendants would not be able to respond sufficiently to prevent juries from being misled in a manner that results in a miscarriage of justice.

Third, the suggestion that the executive branch gets to determine the extent of state secrets evokes the legal principle *nemo iudex in causa sua*. The point of separating and offsetting functional powers is to ensure that each branch not set the bounds of *its own authority*. This reading would contravene the constitutional design, undermining the structural checks and balances. As with the government's other novel interpretations of state secrets, the constitutional claim falls woefully short as a matter of history, logic, and constitutional analysis.

V. Concluding Remarks

In 2009, as Congress became increasingly concerned about the government's use of the state secrets privilege and began drafting legislation to restrict it, the Obama Administration issued guidance, stating it would "invoke the privilege in court only when genuine and significant harm to national defense or foreign relations is at stake and only to the extent necessary to safeguard those interests."[298] The government's move took the political winds from the sails of legislative reform, but it failed to stem the tide driving an ever more expansive interpretation of the common law evidentiary rule. Hearkening back to the torture and rendition cases in the early 21st

[294] Brief of the Appellee, 2006 WL 2726281, at *8.
[295] Brief of the Appellee, 2006 WL 2726281, at *45.
[296] *El-Masri*, 479 F.3d at 303.
[297] The court picked up on dicta in *Reynolds*, namely that the judiciary did not have to demand that the executive reveal certain information. 345 U.S. at 6.
[298] Memorandum for Heads of Executive Departments and Agencies, (Sept. 23, 2009), at 1, https://www.justice.gov/archive/opa/documents/state-secret-privileges.pdf [https://perma.cc/3WKL-XL67].

century, the government has in the interim re-crafted the common law rule in four critical ways: (1) collapsing the *Reynolds* evidentiary rule and the *Totten* contractual bar by discarding the *ex ante* argument and adopting a "very subject matter" analysis; (2) asserting state secrets at the pleadings stage to demand dismissal; (3) applying it to broad categories, instead of to specific information; and (4) claiming it as an Article II constitutional power.

On September 30, 2022, in the midst of the Supreme Court sending *Fazaga* back to the Ninth Circuit, the Attorney General re-issued the 2009 memorandum, again assuring the public that DOJ "is committed to ensuring that the United States invokes the state secrets privilege only when genuine and significant harm to national defense or foreign relations is at stake and only to the extent necessary to safeguard those interests."[299] Based on the cases making their way through the courts, however, that does not appear to be accurate. In the most recent filings in *Fazaga*, now back on remand to the district court, the government casually asserted (without any formal legal declaration) that someone in DOJ had looked at the case and determined that the state secrets assertion remains valid—a remarkable claim seventeen years after the actions in question and despite the considerable amount of information already in the public domain about Operation Flex and Monteilh's actions. It is possible, of course, that the program did not end in 2007 or that a similar initiative continues in a different guise. If so, however, then particularly in light of the significant statutory and constitutional questions at issue there is all the more reason to allow the case to proceed, excluding whatever specific information that may create a genuine risk to U.S. national security as part of the discovery process.

The issues presented in *Fazaga* are not going to go away. In case after case, the privilege is being used in new and more expansive ways. Employed in the context of suits challenging the warrantless collection of information on U.S. citizens, question exists as to whether *any* claim will be able to survive—even where, as in *Fazaga*, a significant amount of information in the public domain suggests that the government is acting outside statutory and constitutional constraints. Whether the government will be held to account remains to be seen. At stake is the future of foundational First, Fourth, and Fifth Amendment constitutional rights.

[299] Memorandum for Heads of Executive Departments and Agencies, Heads of Department Components, Supplement to Policies and Procedures Governing Invocation of the State Secrets Privilege, (Sept. 30, 2022), at 1, https://www.justice.gov/d9/pages/attachments/2022/09/30/supplement_to_policies_and_procedures_governing_invocation_of_the_state_secrets_privilege.pdf [https://perma.cc/8PN3-UKK7].