REIMAGINING SURVEILLANCE LAW

*Emily Berman**

Controversy erupted in 2019 when news broke that the FBI had disregarded its own rules and regulations when it initiated surveillance of Donald Trump's campaign advisor, Carter Page, as a possible Russian agent. Less publicity has accompanied the fact that this incident was not an anomaly. In fact, revelations of unlawful foreign intelligence surveillance activities have come with alarming regularity over the past two decades. These regulatory, statutory, and constitutional violations have involved unauthorized collection of information, misusing information in the government's possession, and repeatedly misleading the Foreign Intelligence Surveillance Court regarding the nature and scope of surveillance programs. This Article argues that frequent violations are inevitable under the current regulatory model, that these violations impose unacceptable costs on Americans' privacy interests, and that they can only be prevented by reimagining surveillance regulation. The Article seeks to do so by drawing on the idea of "constitutional common law" and the related concept of underenforcement of constitutional norms—the idea that some doctrinal rules will systematically fail to fully vindicate constitutional rights. After detailing the government's extensive record of surveillance-rule violations, the Article explains why surveillance rules are predictably, systematically biased towards underenforcement. It then goes on to propose multiple specific reforms designed to combat this tendency, particularly in the contexts where violations have been most problematic.

TABLE OF CONTENTS

* Associate Professor and Royce R. Till Professor of Law, University of Houston Law Center. Thanks to participants in UHLC Summer Faculty Workshop and the ACS Constitutional Law Colloquium, as well as Bill Banks, Barry Friedman, Aziz Huq, James Nelson, and Jessica Roberts.

I. INTRODUCTION

The government regularly breaks its own rules when it comes to foreign intelligence surveillance. Sometimes, this results in high-profile controversies. In the summer of 2013, for example, a massive leak of classified information from former National Security Agency ("NSA") contractor, Edward Snowden, revealed secret programs collecting data about Americans' electronic communications.[1] More recently, revelations that the Federal Bureau of Investigation ("FBI") provided inaccurate and incomplete information to the Foreign Intelligence Surveillance Court ("FISC")[2] to justify surveillance of Donald Trump's

1. *See, e.g.*, John Cassidy, *Snowden's Legacy: A Public Debate About Online Privacy*, NEW YORKER (Aug. 20, 2013), https://www.newyorker.com/news/john-cassidy/snowdens-legacy-a-public-debate-about-online-privacy [https://perma.cc/SCZ6-KJNU]. At least some of the programs revealed by Snowden arguably exceeded the NSA's lawful authorities. *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE TELEPHONE RECORDS PROGRAM CONDUCTED UNDER SECTION 215 OF THE USA PATRIOT ACT 10 (2014).

2. The FISC was established in 1978 by the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1801–1885c, and is composed of eleven federal district court judges designated by the Chief Justice of the United States who serve staggered seven-year terms. *Id.* § 1803.

one-time foreign policy advisor, Carter Page, put surveillance in the hot seat once again.[3] The episodic nature of these notorious incidents might give the impression that surveillance-law violations are themselves sporadic. The reality, however, is that ongoing violations have been the norm, not the exception, in the exercise of the government's foreign intelligence surveillance authorities.[4]

This Article posits that two factors render violations inevitable. First, certain features inherent in the enterprise of surveillance render surveillance rules systematically biased towards underenforcement.[5] And second, the early aughts' focus on terrorism prevention prompted government surveillance and investigative authorities to—as then-Director of the National Security Agency ("NSA"), General Michael Hayden, liked to say—get "chalk dust on [our] cleats,"[6] to maximally exploit the government's surveillance authorities and push up against the statutory and constitutional boundaries of those authorities. The combination of these two dynamics had the predictable effect of producing a great deal of government activity that did not simply step up to the line, but repeatedly crossed it.[7] Compounding the problem, the FISC—the primary oversight body for contemporary surveillance programs—has proved reluctant to respond aggressively, repeatedly allowing problematic surveillance practices to continue while remedies for the violations are devised and implemented.[8]

The problem is one of constitutional dimensions. As the Supreme Court has recognized, surveillance of Americans poses not only a threat to Americans'

3. *See, e.g.*, Charlie Savage, *We Just Got a Rare Look at National Security Surveillance. It Was Ugly*., N.Y. TIMES (Sept. 20, 2021), https://www.nytimes.com/2019/12/11/us/politics/fisa-surveillance-fbi.html [https://perma.cc/7G4R-FJZ3].

4. *See, e.g.*, Ellen Nakashima, *Federal Court Approved FBI's Continued Use of Warrantless Surveillance Power Despite Repeated Violations of Privacy Rules***,** WASH. POST (Apr. 26, 2021, 5:22 PM), https://www.washingtonpost.com/national-security/fbi-surveillance-privacy-violations/2021/04/26/608f342a-a696-11eb-8d25-7b30e74923ea_story.html [https://perma.cc/Q774-PHRX]; Ellen Nakashima, *FBI and NSA Violated Surveillance Law or Privacy Rules, a Federal Judge Found*, WASH. POST (Sept. 4, 2020, 6:44 PM), https://www.washingtonpost.com/national-security/fbi-and-nsa-violated-surveillance-law-or-privacy-rules-a-federal-judge-found/2020/09/04/b215cf88-eec3-11ea-b4bc-3a2098fc73d4_story.html [https://perma.cc/S4YD-T8WT]; Charlie Savage, *N.S.A. Purges Hundreds of Millions of Call and Text Records*, N.Y. TIMES (June 29, 2018), https://www.nytimes.com/2018/06/29/us/politics/nsa-call-records-purged.html [https://perma.cc/3NEB-5X7U]; Charlie Savage, *N.S.A. Often Broke Rules on Privacy, Audit Shows*, N.Y. TIMES (Aug. 16, 2013), https://www.nytimes.com/2013/08/16/us/nsa-often-broke-rules-on-privacy-audit-shows.html [https://perma.cc/8HWJ-RARS]; DEMAND PROGRESS, SECTION 215: A BRIEF HISTORY OF VIOLATIONS (2019); DEMAND PROGRESS, INSTITUTIONAL LACK OF CANDOR 2–8 (2017) (detailing Section 702 violations).

5. *See infra* Section III.B.

6. *See, e.g.*, SHANE HARRIS, THE WATCHERS: THE RISE OF AMERICA'S SURVEILLANCE STATE 159 (2010).

7. Sometimes these violations—labeled "compliance incidents" in bureaucracy-speak—have gone undetected for years at a time. *See* Barton Gellman, *NSA Broke Privacy Rules Thousands of Times Per Year, Audit Finds*, WASH. POST (Aug. 15, 2013), https://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_story.html [https://perma.cc/8P74-K229]. Most of the violations have been inadvertent. *See id.* On one hand, that is a good thing—there has been no indication of widespread, coordinated, intentional efforts by the government to overstep its authorities. On the other hand, no system in which participants acting in good faith nevertheless overstep on a regular basis can be viewed as an effective regulatory regime.

8. *See, e.g.*, Jennifer Stisa Granick & Ashley Gorski, *How to Address Newly Revealed Abuses of Section 702 Surveillance*, JUST SEC. (Oct. 18, 2019), https://www.justsecurity.org/66622/how-to-address-newly-revealed-abuses-of-section-702-surveillance/ [https://perma.cc/L9A4-AH8F].

privacy guaranteed by the Fourth Amendment,[9] but also to free speech and association rights embodied in the First Amendment.[10] Surveillance statutes and regulations have been explicitly crafted to reflect constitutional limits and safeguard individual rights.[11] Each time the intelligence community exceeds its surveillance authorities, therefore, it risks infringing on the constitutional rights of Americans.[12]

This risk to civil liberties is particularly acute in the context addressed in this Article: surveillance conducted inside the United States in order to collect foreign intelligence information.[13] In all contexts, surveillance rules are necessary to ensure that the government only collects information it is authorized to collect and that the information is not used improperly. But intelligence-surveillance law is in many ways both more permissive and less transparent than traditional criminal surveillance. The standards the government must meet to engage in surveillance for intelligence purposes are less stringent than those required when the target is a criminal suspect,[14] while the scope of the surveillance itself

9. *See* United States v. U. S. Dist. Ct. (Keith), 407 U.S. 297, 320 (1972); *In re* Sealed Case No. 02-001, 310 F.3d 717, 746 (FISA Ct. Rev. 2002); *In re* Directives to Yahoo! Inc. Pursuant to Section 105b of Foreign Intel. Surveillance Act, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

10. *See Keith*, 407 U.S. at 313–14.

11. One senator argued that, without surveillance regulation, "we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government." *See id.* at 314 (quoting Sen. Philip A. Hart).

12. The nature of the harms that flow from government surveillance are a subject of debate. For some, any threat to First and Fourth Amendment protection is problematic because "[p]rivacy is an inherent human right, and a requirement for maintaining the human condition with dignity and respect." Bruce Schneier, *The Eternal Value of Privacy*, WIRED (May 18, 2006, 2:00 AM), https://www.wired.com/2006/05/the-eternal-value-of-privacy/ [https://perma.cc/9HCJ-ZV76]. Others, however, insist that "[i]f you aren't doing anything wrong, what do you have to hide?" *Id.* But this argument fails to acknowledge that humans engage in many lawful—even necessary—activities that we nonetheless desire to keep private (from the government and from others), that individuals engaged in innocuous activities may nevertheless be victims of errors or abuses by those in power, *Keith*, 407 U.S. at 317 ("The historical judgment, which the Fourth Amendment accepts, is that unreviewed executive discretion may yield too readily to pressures to obtain incriminating evidence and overlook potential invasions of privacy and protected speech."), and that there are broad societal harms imposed by excessive surveillance. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) ("[M]odern enterprise and invention have, through invasions upon [a person's] privacy, subjected him to mental pain and distress, far greater than could be inflicted by mere bodily injury."); Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131, 1133–34 (2011); Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 765 (2007) [hereinafter Solove, *I've Got Nothing to Hide*] (explaining that surveillance, even of legal activities, "can create chilling effects on free speech, free association, and other First Amendment rights essential for democracy. Even surveillance of legal activities can inhibit people from engaging in them"); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 495 (2006) (pointing to the chilling effect when "people are generally aware of the *possibility* of surveillance"); Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373, 1426 (2000) ("Pervasive monitoring of every first move or false start will, at the margin, incline choices toward the bland and the mainstream."); Peter P. Swire, *Financial Privacy and the Theory of High-Tech Government Surveillance*, 77 WASH. U. L. Q. 461, 473 (1999) ("If I know that I am under surveillance, I might . . . restrict my activities, so that nothing embarrassing or otherwise harmful could be detected.").

13. *See* 50 U.S.C. § 1801(e) (defining foreign intelligence information as information relating to the ability of the U.S. to protect against threats emanating from foreign powers as well as information relating to the national defense or the conduct of U.S. foreign affairs).

14. *Compare, e.g.*, 18 U.S.C. § 3122, *with* 50 U.S.C. § 1804.

is frequently broader.[15] Moreover, unlike criminal defendants, most subjects of foreign intelligence surveillance will never know that they have been targeted, so the government's activity will never face challenges to its lawfulness in open court. In addition, it is often difficult to determine both what data is being collected under surveillance authorities and how it is being used.[16] Indeed, because most FISC decisions remain secret, even identifying what rules the government should be following can be difficult.[17] What we do know is that the volume of collection is enormous.[18] And the greater the volume of data in the government's possession, the greater the risk of misuse, and the greater the potential for harm.

This Article argues that ensuring that the government's efforts to collect and use foreign intelligence information abides by constitutionally required limits requires a fundamental shift—a reimagining—in our approach to surveillance regulation and the bureaucratic culture surrounding its implementation. More specifically, I contend that frequent constitutional violations are an inevitable and predictable product of structural features inherent in surveillance activities, that these violations impose unacceptable costs on civil liberties, and that only by approaching the problem from a different perspective can we prevent them. The Article offers such a perspective, drawing on constitutional theories identifying the phenomenon of systemic underenforcement of constitutional norms[19] to generate concrete recommendations for surveillance reform. The key insight from the theory of underenforcement is that there is a distinction between constitutional *meaning*—what the words of the Constitution actually protect or proscribe—and constitutional *doctrine*—the rules judges use to decide constitutional questions. This means that constitutional doctrine can, at times, yield rules that are not coextensive with the meaning of the Constitution itself. In other

15. *See, e.g.*, *Keith*, 407 U.S. at 320 ("Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent.").

16. *See* Solove, *I've Got Nothing to Hide*, *supra* note 12, at 766 ("[W]ithout greater transparency in data mining, it is hard to claim that programs like the NSA data mining program will not reveal information people might want to hide, as we do not know precisely what is revealed.").

17. *See* David D. Cole, Jameel Jaffer & Theodore B. Olsen, *What Is America's Spy Court Hiding from the Public?*, N.Y. TIMES (June 2, 2021), https://www.nytimes.com/2021/06/02/opinion/Supreme-Court-FISA-secrecy.html [https://perma.cc/SQ9W-GM44] (arguing that maintaining secrecy of FISC opinions impoverishes public debates about surveillance and undermines trust in the government).

18. *See, e.g.*, Charlie Savage, *N.S.A. Triples Collection of Data from U.S. Phone Companies*, N.Y. TIMES (May 4, 2018), https://www.nytimes.com/2018/05/04/us/politics/nsa-surveillance-2017-annual-report.html [https://perma.cc/NF5Q-X465].

19. *See, e.g.*, Henry P. Monaghan, *Foreword: Constitutional Common Law*, 89 HARV. L. REV. 1, 1 (1975); Lawrence Gene Sager, *Fair Measure: The Legal Status of Underenforced Constitutional Norms*, 91 HARV. L. REV. 1212, 1212 (1978); Joseph D. Grano, *Prophylactic Rules in Criminal Procedure: A Question of Article III Legitimacy*, 80 NW. U. L. REV. 1, 1 (1985); David A. Strauss, *The Ubiquity of Prophylactic Rules*, 55 U. CHI. L. REV. 190, 190 (1988); Richard H. Fallon Jr., *Implementing the Constitution*, 111 HARV. L. REV. 54, 56 (1997); Bryan K. Landsberg, *Safeguarding Constitutional Rights: The Uses and Limits of Prophylactic Rules*, 66 TENN. L. REV. 925, 925 (1999); Daryl J. Levinson, *Rights Essentialism and Remedial Equilibration*, 99 COLUM. L. REV. 857, 857 (1999); Susan R. Klein, *Identifying and (Re)formulating Prophylactic Rules, Safe Harbors, and Incidental Rights in Constitutional Criminal Procedure*, 99 MICH. L. REV. 1030, 1030–31 (2001); Evan H. Caminker, Miranda *and Some Puzzles of Prophylactic Rules*, 70 U. CIN. L. REV. 1, 1 (2001); Mitchell N. Berman, *Constitutional Decision Rules*, 90 VA. L. REV. 2, 3 (2004).

words, doctrine might either over- or underenforce constitutional norms. In contexts such as surveillance, where the likelihood of underenforcement is high, courts can guard against that underenforcement by opting for rules that intentionally create a buffer zone between what the Constitution demands and what government action the rules actually permit.[20] In short, they can demand that we do the opposite of getting chalk on our cleats—that we stay far enough behind that line that a stray step will not take us into forbidden territory. This Article advocates for the adoption of such rules to regulate government surveillance activities.

There are at least three, sometimes overlapping, circumstances that render the underenforcement of constitutional rights more likely—circumstances where rules creating a constitutional buffer zone are particularly appropriate. The first arises when there are systemic factors likely to produce rules violations.[21] The second is when violations are difficult to detect or to prove.[22] Finally, there are instances in which a clear, simple rule is required in order to guide government actors or deter violations.[23] As this Article will demonstrate, surveillance rules frequently exhibit one or more of these characteristics, thereby justifying use of rules that recognize the risk of underenforcement and consciously correct for that tendency.

This Article makes two important contributions to the existing literature on government surveillance. First, it compiles in one place a comprehensive picture of the nature and scope of the most problematic forms of surveillance-law violations that have emerged over the past twenty-plus years. It synthesizes revelations contained in dozens of disparate documents—leaked or declassified FISC opinions, inspector general investigations, and required periodic government-issued reports—to identify and categorize recurring problems that cut across different programs and different types of surveillance. This transprogrammatic perspective allows the Article to offer a holistic assessment of surveillance-law violations—an assessment that reveals a picture of chronic underenforcement.[24] This picture is comprised of at least three types of transgressions: providing false, misleading, or incomplete information to the FISC; collecting data whose collection is not authorized; and violating rules regulating the post-collection use of information.[25] The Article's second contribution is to recognize that this chronic underenforcement is the inevitable result of systemic forces and that preventing it will require a reimagining of surveillance rules. It, therefore, proposes reforms

20. The quintessential example of such a rule is the requirement that law enforcement officers issue *Miranda* warnings prior to custodial interrogation. *See infra* notes 252–56 and accompanying text. While *Miranda* is the most well-known such rule, as numerous commentators have pointed out, it is far from the only one. *See* sources cited *supra* note 19.

21. *See infra* Subsection III.B.1.

22. *See infra* Subsection III.B.2.

23. *See infra* Subsection III.B.3.

24. Professor Laura Donohue compiles her own account of the government's many compliance incidents in her paper examining the evolution of the FISC's jurisprudence. *See* Laura K. Donohue, *The Evolution and Jurisprudence of the Foreign Intelligence Surveillance Court and Foreign Intelligence Surveillance Court of Review*, 12 HARV. NAT'L SEC. J. 198, 255–70 (2021).

25. *See infra* Section II.B.

strategically designed to combat surveillance law's natural propensity toward underenforcement.[26]

The argument proceeds in three parts. Part II focuses on the recurring violations committed by surveillance agencies in the past two decades. It first describes the surveillance programs involved before presenting, in some detail, the violations themselves. Part III turns to the idea of underenforcement, fleshing out the concept and detailing why it is inevitable in the surveillance context. Finally, Part IV proposes multiple specific reforms designed to combat this underenforcement in the areas where violations have been most problematic.

II. VIOLATIONS OF SURVEILLANCE RULES

It is impossible to assess the need for reform or the shape that reform should take without first understanding, in some level of detail, both the programs being employed and the violations whose recurrence reform is meant to prevent. This Part therefore lays the foundation for the discussion that follows by first, in Section II.A, offering a brief description of the various surveillance programs involved, before turning in Section II.B to a granular discussion of the government's history of noncompliance, particularly since 9/11.

A. Surveillance Programs: A Primer

This Section will very briefly sketch the contours of the three forms of surveillance in which recurring violations appear. Some of these programs collect the contents of electronic communications—the substance of targets' telephone or e-mail exchanges—while others collect metadata—noncontent information, such as the phone numbers or e-mail addresses with which the target is in contact.[27] Collection, however, is only one element of electronic surveillance. Once the government collects the data from a particular target, it stores it in vast databases.[28] Members of the intelligence community then query the contents of those databases as part of their investigations, incorporate the data into intelligence analyses, and disseminate it to other government agencies and U.S. allies.[29] Each step in this process—targeting decisions, collection, retention, querying, and use of resulting information—is subject to various rules and regulations, most of which the courts and Congress have determined are necessary to satisfy the First and Fourth Amendments' demands.[30]

26. *See infra* Section III.B.
27. *See infra* Subsection II.A.2.
28. *See infra* Subsection II.A.2.
29. *See infra* Subsection II.A.2.
30. *See infra* Section II.B.

1. Traditional FISA Collection

In 1978, Congress passed Title I of the Foreign Intelligence Surveillance Act ("FISA"),[31] sometimes called "original FISA" or "traditional FISA" to distinguish it from subsequent amendments. FISA governs electronic surveillance—phone calls and e-mails, for example—conducted inside the U.S. for the purpose of acquiring foreign intelligence information.[32] To engage in traditional FISA surveillance, the government must demonstrate to the FISC that there is probable cause to believe that the target of the surveillance is a foreign power or an agent of a foreign power[33] and that a significant purpose of the surveillance is to acquire foreign intelligence information.[34]

2. Bulk Collection of Telephone and Internet Metadata

For almost three decades traditional FISA was the only FISA.[35] After 9/11, however, new legislation—along with the government's aggressive interpretation of its new statutory authorities—significantly expanded the footprint of government surveillance.[36] We learned the details of two of these post-9/11 programs designed to identify unknown terrorism suspects inside the United States thanks to Edward Snowden's massive leak of classified information in the summer of 2013.[37]

The first program, which collected internet metadata, relied on an expansive interpretation of a FISA provision authorizing the use of pen registers and trap-and-trace devices (*i.e.*, tools to record noncontent communications data, such as dialing, routing, addressing, or signaling information transmitted to or from a particular communication device).[38] The government may use this authority when the information likely to be obtained is relevant to an ongoing investigation to protect against international terrorism or is foreign intelligence information.[39] In the government's view, this authorized collection of communications metadata not simply to or from a specific individual or account, but rather *all* e-mail routing and addressing information transiting the Internet.[40]

31. 50 U.S.C. §§ 1801–1813.

32. *Id.*

33. 50 U.S.C. §1804(a)(3)(A); 50 U.S.C. § 1801(b) (defining agent of a foreign power).

34. 50 U.S.C. § 1804(a)(6)(A)–(E); 50 U.S.C. § 1801(e) (defining foreign intelligence information).

35. To be sure, it had already expanded in some ways, but it remained a tool for individually targeting foreign powers and their agents inside the United States. *See* 50 U.S.C. §§ 1821–26 (extending FISA to physical searches); 50 U.S.C. §§ 1841–46 (pen register and trap-and-trace devices).

36. PRIVACY & 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 8 (2014) [hereinafter PCLOB SECTION 215 REPORT].

37. *Id.*

38. *See* 50 U.S.C. § 1842.

39. *Id.*

40. PCLOB SECTION 215 REPORT, *supra* note 36, at 38; Opinion and Order, [REDACTED], No. PR/TT [REDACTED], GID.C.00091 (FISC 2002) (Kollar-Kotelly, J.) [hereinafter FISC's Pen/Trap Opinion]. Note that FISC decisions are rarely reported and details regarding docket numbers and case names are redacted, making them difficult to identify through citations. To mitigate this challenge, I have adopted the numbering system used

All of this internet metadata was relevant to investigations into international terrorism, the government argued, because only by collecting *all* communications metadata could it identify individuals involved with terrorist organizations.[41] The FISC approved this aggressive interpretation in 2004, and the government proceeded to acquire vast amounts of metadata about internet communications, such as e-mail—even if those communications were purely domestic (*i.e.*, from one American to another) until the program was discontinued in 2011.[42]

The second program employed a similarly broad interpretation of Section 215 of the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act"), also known as the FISA "business records" provision,[43] to collect telephone call detail records (*e.g.*, the date, time, and duration of a call as well as the participating telephone numbers).[44] From 2001 through 2020, this provision authorized the collection of "any tangible thing" for which the government could demonstrate "reasonable grounds to believe that [it was] relevant" to an ongoing international terrorism or espionage investigation.[45] Section 215 could be used to seize, for example, an individual's banking records or his home computer.[46] What Snowden revealed was that the FISC had also interpreted Section 215 to allow the government to collect nearly *all* call detail records generated by telephone companies in the United States.[47] The vast majority of these records related to purely domestic calls from one American to another.[48]

For each of these programs, the NSA collected the records and stored them in databases, which analysts from various agencies could then "query," or search, using terms, known as "selectors" (usually e-mail addresses or phone numbers), in an effort to identify as-yet-unknown terrorist suspects by analyzing the communications patterns of targets and their associates.[49]

The FISC recognized the privacy implications of these programs, both of which authorized an "exceptionally broad form of collection," involving vast amounts of metadata about Americans' telephone and internet communications.[50] Meanwhile, "only a very small percentage" of the data collected would

in the Foreign Intelligence Law Collection, which was compiled by Professor Laura Donohue at Georgetown Law School and the Georgetown Law Library and can be found at https://repository.library.georgetown.edu/handle/10822/1052698.

41. *See* FISC's Pen/Trap Opinion, *supra* note 40, at 18.

42. *Id*. at 80; PCLOB SECTION 215 REPORT, *supra* note 36, at 97.

43. 50 U.S.C. § 1861 (2001).

44. ADMIN. WHITE PAPER, BULK COLLECTION OF TELEPHONY METADATA UNDER SECTION 215 OF THE USA PATRIOT ACT 3 (2013).

45 50 U.S.C. § 1861 (2001) (the FBI "may make an application for an order requiring the production of any tangible things . . . for an investigation to obtain foreign intelligence information . . . or to protect against international terrorism or clandestine intelligence activities").

46. *See The USA PATRIOT Act: Preserving Life and Liberty*, DEP'T OF JUST., https://www.justice.gov/archive/ll/highlights.htm (last visited Mar. 14, 2023) [https://perma.cc/F5AU-TTQ6].

47. *See* PCLOB SECTION 215 REPORT, *supra* note 36, at 9.

48. *Id.* at 22.

49. *See* PCLOB SECTION 215 REPORT, *supra* note 36, at 39.

50. *See* FISC's Pen/Trap Opinion, *supra* note 40, at 68 ("[T]he extremely broad nature of this collection carries with it a heightened risk that collected information could be subject to various forms of misuse . . . .").

be "directly relevant" to an investigation.[51] As a result, the FISC required the government to implement robust postcollection procedural protections (known as minimization procedures)[52] to govern the retention and use of the acquired data—procedural protections with which the government "frequently" failed to comply.[53]

Each of these programs has since been discontinued. The internet metadata collection was voluntarily discontinued by the government in 2011,[54] while the telephone metadata program was first modified by statute in the 2015 USA Freedom Act,[55] and then discontinued entirely when the statutory provision authorizing it sunset in 2020.[56] The compliance failures that occurred during the life of these programs remain instructive, however, because they demonstrate both that similar types of problems recur across programs and that certain procedural remedies cannot redress the problems.

3. Section 702 Collection

Perhaps the most violation-prone program has been the NSA's Section 702 collection. Section 702, named for a section of the FISA Amendments Act of 2008,[57] authorizes the government to collect the electronic communications content of non-U.S. persons[58] reasonably believed to be located outside the United

51. *Id*. at 48.

52. Minimization procedures are measures that seek to "minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons." 50 U.S.C. § 1801(h). Each agency's minimization procedures set criteria for the retention and dissemination of information on or concerning U.S. persons, provide rules to protect attorney-client information, provide procedures for obtaining assistance from other agencies, and provide rules about what to do when a target originally determined to be a non-U.S. person outside the United States is subsequently determined to be a U.S. person or located inside the United States. *See, e.g.*, U.S. Dep't of Defense, DoD Manual 5240.01, Procedures Governing the Conduct of DoD Intelligence Activities 20, 22 (2016).

53. Mem. Op., [REDACTED], No. PR/TT [REDACTED], GID.C.00092 4 (FISA Ct.) (Bates, J.) [hereinafter Judge Bates undated Pen/Trap opinion].

54. *But see* Charlie Savage, *File Says N.S.A. Found Way to Replace Email Program*, N.Y. TIMES (Nov. 19, 2015), https://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html [https://perma.cc/ZY6R-HF8F] (reporting that the NSA found a "functional equivalent" for the program overseas, where the NSA is subject to fewer restrictions); Timothy Edgar, *Bulk NSA Internet Program Shows the Complete Incoherence of Surveillance Law*, LAWFARE (Nov. 20, 2015, 9:45 AM), https://www.lawfareblog.com/bulk-nsa-internet-program-shows-complete-incoherence-surveillance-law [https://perma.cc/ZE4A-DNX9] (confirming Savage's reporting).

55. *See generally* USA Freedom Act of 2015, Pub. L. No. 114-23; Jennifer Steinhauer & Jonathan Weisman, *U.S. Surveillance in Place Since 9/11 Is Sharply Limited*, N.Y. TIMES (June 2, 2015), https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html [https://perma.cc/CND7-LD67] (describing USA Freedom Act's efforts to curtail collection of telephone metadata).

56. *See* Charlie Savage, *House Departs Without Vote to Extend Expired F.B.I. Spy Tools*, N.Y. TIMES (Mar. 27, 2020), https://www.nytimes.com/2020/03/27/us/politics/house-fisa-bill.html [https://perma.cc/KMQ7-8MGL].

57. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261.

58. FISA defines U.S. person as "a citizen of the United States, an alien lawfully admitted for permanent residence . . ., an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States . . . ." 50 U.S.C. § 1801(i).

States to gather foreign intelligence information.[59] The FISC's role in the Section 702 program differs from its role in traditional FISA in important ways. Unlike traditional FISA, Section 702 does not require the FISC to approve individual surveillance targets. Instead, the government applies to the FISC for a year-long certification.[60] As part of that application, each agency with access to Section 702-acquired data submits to the court its proposed procedures for selecting targets.[61] Once a certification is issued, the government then uses those approved procedures to determine who it will target.[62] Once a target is chosen, a "selector" associated with that target (*e.g.*, a phone number or e-mail address) is "tasked" for collection.[63] There are two methods through which Section 702 collection takes place: PRISM and Upstream. Under PRISM, the NSA acquires communications to or from the tasked selector from the target's communications or internet service providers.[64] In Upstream collection, rather than seeking data from a service-provider intermediary, the NSA captures communications directly from the data stream as it transits the Internet.[65]

In addition to targeting procedures, the government's Section 702 application also must include minimization procedures[66] that establish rules for how the government handles the information it acquires, and as of 2017, procedures for querying the databases containing data collected pursuant to Section 702.[67] The court must then determine whether the proposed targeting, minimization, and querying procedures satisfy both statutory and constitutional requirements.[68]

The FISC assesses the constitutionality of Section 702 surveillance under the Fourth Amendment's "reasonableness" standard, which is a balancing test

59. *See* 50 U.S.C. § 1881a.

60. *See* FISA Amendments Act of 2008, Pub. L. No. 110-261.

61. These procedures are designed to ensure that targets are, in fact, non-U.S. persons located outside the United States and likely to produce foreign intelligence information. *See, e.g.*, PROCEDURES USED BY THE FBI FOR TARGETING NON-U.S. PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE U.S. TO ACQUIRE FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FISA 1978, AS AMENDED (2019) [hereinafter NSA TARGETING PROCEDURES].

62. *See* PRIV. & CIVIL LIBERTIES OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FISA 7 (2014) [hereinafter PCLOB SECTION 702 REPORT].

63. *Id.* at 7.

64. *Id.*

65. *See, e.g.*, James Bamford, *They Know Much More Than You Think*, N.Y. REV. OF BOOKS, Aug. 15, 2013 (quoting NSA's description of upstream collection as "collection of communications on fiber cables and infrastructure as data flows past"). The NSA also collects the contents of telephone calls via Upstream collection, but unlike Upstream internet data collection, it does not result in the collection of communications to/from non-targets. PCLOB SECTION 702 REPORT, *supra* note 62, at 37.

66. PCLOB SECTION 702 REPORT, *supra* note 62, at 51–66.

67. Querying procedures focus on regulating the use of U.S.-person query terms. The CIA, the NSA, and NCTC may query Section 702 information if the queries are "reasonably likely to return foreign-intelligence information," while the FBI may perform U.S.-person queries that are "reasonably likely to return foreign-intelligence information or evidence of a crime." Mem. Op., [REDACTED], No. [REDACTED], GID.C.00289 17 (FISA Ct. 2020) (Boasberg, J.) [hereinafter Judge Boasberg Nov. 18, 2020 opinion]. Querying rules were part of each agency's minimization procedures until the significant Fourth Amendment concerns these procedures implicate prompted Congress in 2017 to require agencies to produce separate querying procedures. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 101.

68. PCLOB SECTION 702 REPORT, *supra* note 62, at 6.

that considers the totality of the circumstances.[69] In these analyses, the court has always stressed that Section 702 is reasonable only when the government complies with not only the statutory dictates of Section 702 itself, but also the approved targeting, minimization, and querying procedures that form part of the government's application.[70] In other words, compliance with each element of the Section 702 regime is necessary for the government to operate within the bounds of the Fourth Amendment.

As the FISC has recognized, "the privacy interests at stake in Section 702 acquisition [are] substantial."[71] Under this program, the government collects the substantive contents of electronic communications to and from targets of the government's choosing.[72] And while these targets themselves are non-U.S. persons outside the United States, the individuals with whom the target is communicating are often—perhaps even usually—*inside* the United States.[73] This "incidental" collection, as the government terms it, results in the collection of a vast number of communications to or from U.S. persons inside the United States.[74] While the NSA has not provided an estimate of the number of Americans' communications acquired under Section 702 (the NSA asserts that providing such an estimate would itself violate Americans' privacy), a 2011 FISA court opinion noted that a total of 250 million internet communications were acquired the previous year under Section 702.[75] If just 10% of these communications involved U.S. persons—a low estimate—that would still result in the collection of 25 million internet communications involving Americans in a single year.[76] These millions of communications are then stored in databases to which the NSA, Central Intelligence Agency ("CIA"), FBI, and National Counterterrorism Center ("NCTC") all have access.[77]

69. *E.g.*, Mem. Op., [REDACTED], No. [REDACTED]. GID.C.00106 26 (FISA Ct. 2014) (Hogan, J.) ("In conducting this assessment, the Court is mindful that the controlling norms are ones of reasonableness, not perfection."); Mem. Op., [REDACTED], No. [REDACTED], GID.C.00130 11 (FISA Ct. 2017) (Collyer, J.) [hereinafter Judge Collyer Apr. 26, 2017 Opinion] (same).

70. *See, e.g.*, *In re* Directives Pursuant to Section 105B of Foreign Intel. Surveillance Act, 551 F.3d 1004 (FISA Ct. 2008); Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69.

71. *E.g.*, Mem. Op., [REDACTED], No. [REDACTED], GID.C.00282 59 (FISA Ct. 2019) (Boasberg, J.).

72. PCLOB SECTION 702 REPORT, *supra* note 62, at 5.

73. *Id.* at 6 ("Although U.S. persons may not be targeted under Section 702, communications of or concerning U.S. persons may be acquired . . . when a U.S. person communicates with a non-U.S. person who has been targeted.").

74. *Id.* at 87 (noting that while U.S. persons may not be targeted under Section 702, their communications are nevertheless collected, "potentially in large numbers").

75. ELIZABETH GOITEIN & FAIZA PATEL, BRENNAN CENTER FOR JUSTICE, WHAT WENT WRONG WITH THE FISA COURT 27 (2015); *see also* Barton Gellman, Julie Tate & Ashkan Soltani, *In NSA-Intercepted Data, Those Not Targeted Far Outnumber the Foreigners Who Are*, WASH. POST (July 5, 2014), https://www.washingtonpost.com/world/national-security/in-nsa-intercepted-data-those-not-targeted-far-outnumber-the-foreigners-who-are/2014/07/05/8139adf8-045a-11e4-8572-4b1b969b6322_story.html [https://perma.cc/DMP4-3LYW] (pointing out that in 2014, nine out of ten internet users whose data the NSA collected under Section 702 were not targets).

76. GOITEIN & PATEL, *supra* note 75, at 27.

77. PCLOB SECTION 702 REPORT, *supra* note 62, at 55.

TABLE 1. FOREIGN INTELLIGENCE SURVEILLANCE PROGRAMS

Program	**Statutory Authority**	**Name(s) of Program**	**Information collected**	**Eligible Targets**	**Current status**
FISA Title I	50 U.S.C. §§ 1804-1805	"Traditional" or "original" FISA	Electronic communications content	Foreign powers or their agents inside the U.S.	Ongoing
Bulk Internet collection	50 U.S.C. § 1842	Pen/trap provision	Internet communications metadata	Information relevant to an international terrorism investigation	Discontinued 2011
Bulk Telephone collection	50 U.S.C. § 1861	Section 215 or "business records" provision	Telephone metadata	Information relevant to an international terrorism investigation	Discontinued in part in 2015, sunset in 2020
Section 702	50 U.S.C. § 1881a	Upstream and Prism	Electronic communications content	U.S. persons reasonably believed to be located outside the U.S.	Ongoing

B. Surveillance Programs: The Violations

Having explicitly decided to operate at the outer limits of the law, the executive branch has inevitably spent a significant amount of time on the wrong side of that line. Moreover, despite the remedies imposed by both the FISC and Congress, noncompliance continues to dog foreign intelligence collection efforts. While I do not purport here to provide an exhaustive account of all foreign intelligence surveillance compliance incidents,[78] the following discussion represents a thick account of the pervasiveness and severity of systemic and recurring compliance problems, which fall into three categories: first, instances in which the government has provided information to the FISC that is inaccurate, incomplete, or misleading; second, persistent overcollection (*i.e.*, the collection of data whose collection is not authorized); and third, failure to abide by rules governing the use of information collected through foreign intelligence surveillance programs.

78. For a sortable, searchable database of publicly available information about Section 702 violations up until 2017, see ROBYN GREENE, OPEN TECH. INST., SECTION 702 COMPLIANCE VIOLATION CHART, at https://na-production.s3.amazonaws.com/documents/Categorized_Compliance_Violation_Document_9.27.17.pdf (last visited Mar. 14, 2023) [http://perma.cc/8W99-DEJU].

1. Inaccurate, Incomplete, or Misleading Submissions to the FISC

The need for the government to provide "'scrupulously accurate'" information to the FISC is a foundational principle of foreign intelligence collection[79] because of the ways in which FISC proceedings differ from those of most Article III courts. First, nearly all of the court's proceedings are *ex parte*, with the government being the sole entity represented.[80] Second, because FISA-derived information consists primarily of foreign intelligence information, it is rarely introduced as evidence in criminal proceedings.[81] This means that targets seldom know about or have the opportunity to challenge the lawfulness of their surveillance. Third, both the FISC's proceedings and its opinions are classified.[82] This lack of both adversarial process and transparency means that "the FISC relies on the U.S. government to provide 'full and accurate presentation of the facts.'"[83] When the government falls short in this duty, it undermines the entire system of safeguards put in place to protect Americans' First and Fourth Amendment rights.

Nevertheless, the FISC has repeatedly found itself lamenting the government's "chronic tendency to mis-describe"[84] or "misrepresent the scope" of its collection activities[85] as well as its institutional "lack of candor."[86] Violations of the government's duty of candor have come in a myriad of contexts. In some, the government's failure to accurately represent the scope of its activities led the FISC to approve a program that, it turns out, violated both statutory minimization rules and the Fourth Amendment.[87] In others, the government not only violated the rules but also compounded the problem by failing to promptly or fully inform the FISC about those violations, allowing noncompliance to persist, sometimes for years. Indeed, at one point, the government was so delinquent in informing

79. *See, e.g.*, OFF. OF THE INSPECTOR GEN., U.S. DEP'T OF JUST., REVIEW OF FOUR FISA APPLICATIONS AND OTHER ASPECTS OF THE FBI'S CROSSFIRE HURRICANE INVESTIGATION 43 (2019) [hereinafter DOJ IG CROSSFIRE HURRICANE REPORT]; Memorandum from Matthew G. Olsen, Acting Asst. Att'y Gen. & Valerie Caproni, FBI Gen. Counsel, for All Off. of Intel. Atty's, All Nat'l Sec. L. Branch Att'ys, & All Chief Div. Couns., Guidance to Ensure the Accuracy of Federal Bureau of Investigation Applications under the Foreign Intelligence Surveillance Act (Feb. 11, 2009).

80. *See* Donohue, *supra* note 24, at 204.

81. *See* Simon Chin, Note, *Introducing Independence to the Foreign Intelligence Surveillance Court*, 131 YALE L. J. 655, 661 (2021).

82. *Id.* at 662.

83. *Id.* at 673.

84. Op., [REDACTED], No. [REDACTED], GID.C.00254, at 13–14 (FISA Ct.) (Hogan, J.) ("These inaccuracies have previously contributed to unauthorized electronic surveillance and other forms of statutory and constitutional deficiency.").

85. Mem. Op., [REDACTED], No. [REDACTED], GID.C.00073 16 n. 14 (FISA Ct. 2011) (Bates, J.) [hereinafter Judge Bates Oct. 3, 2011 Opinion] ("The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program.").

86. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 19; *see also* Donohue, *supra* note 24, at 277 ("About a dozen opinions in the public domain raise concern about inaccurate, materially omitted, erroneous, or false statements to the court.").

87. *See infra* notes 130–43 and accompanying text; Judge Bates Oct. 3, 2011 Opinion, *supra* note 85, at 19.

the court about known violations, a FISA judge felt the need to issue an order explicitly requiring the government to report each violation of its targeting or minimization procedures.[88] There are also numerous examples of the government's much-delayed or nonexistent efforts to comply with judicially imposed remedies for past violations, such as failure to promptly purge material whose collection was unauthorized.[89] These and similar incidents inspired one FISA judge to opine that "the government needs every incentive to provide accurate and complete information to the Court about NSA operations."[90] This conclusion seems entirely inconsistent with the reliance on the government's duty of scrupulous accuracy on which surveillance procedures are based.

The inaccurate and misleading government submission to the FISC that has received perhaps the most public attention is also one of the most recent. As part of the FBI's investigation into Russian interference in the 2016 presidential campaign, the Justice Department targeted Carter Page, a one-time Trump Campaign foreign policy advisor, under a traditional FISA order.[91] A Justice Department Inspector General's ("IG") investigation revealed, however, that the information supporting a finding of probable cause that Page was an agent of a foreign power was inaccurate and misleading.[92] First, and most troubling, when providing evidence of Page's contacts with Russian intelligence officers to support the claim that he was acting as an agent of a foreign power, an FBI attorney intentionally altered an e-mail from the CIA to indicate that Page was not a source for the agency when, in fact, he had been.[93] Had the FISC known about this relationship, "it would raise the issue of whether Page interacted with the Russian intelligence officers at the behest of the [CIA]," thereby casting doubt on his status as an agent of a foreign power.[94] Second, in relying on information contained in the now-infamous Steele Dossier,[95] the government overstated the reliability of Christopher Steele as a source.[96] Third, the government failed to disclose statements that Page made to a confidential informant that actually conflicted with

88. Mem. Op., [REDACTED], No. [REDACTED], GID.C.00051 88 (FISA Ct. 2009) (Hogan, J.).

89. Mem. Op., [REDACTED], No. [REDACTED], GID.C.00121 58 (FISA Ct. 2015) (Hogan, J.) [hereinafter Judge Hogan Nov. 6. 2015 opinion].

90. Op., [REDACTED], No. [REDACTED], GID.C.00254 14 (FISA Ct.) (Hogan, J.).

91. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at vi.

92. Op., *In re* Accuracy Concerns Regarding FBI Matters Submitted to the FISC, No. Misc. 19-02, GID.C.00270 1 (FISA Ct.) (Boasberg, J.) [hereinafter Judge Boasberg Mar. 4, 2020 opinion] (FBI personnel "provided false information" to and "withheld material information . . . which was detrimental to the FBI's case" from DOJ officials responsible for preparing the application).

93. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 8. The attorney, Kevin Clinesmith, pleaded guilty to falsifying the e-mail and was sentenced to a year of probation. Matt Zapotosky, *Ex-FBI Lawyer Avoids Prison After Admitting He Doctored Email in Investigation of Trump's 2016 Campaign*, WASH. POST (Jan. 29, 2021, 12: 28 PM), https://www.washingtonpost.com/national-security/kevin-clinesmith-fbi-john-durham/2021/01/28/b06e061c-618e-11eb-afbe-9a11a127d146_story.html [https://perma.cc/H2DW-6GYP].

94. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 131.

95. The so-called Steele Dossier is a collection of reports from FBI informant Christopher Steele. *Id.* at 4 n.6.

96. *Id.* at 132. The language about Steele that went into the application was much more emphatic about Steele's past contributions than the language his handler provided about him. *Id*. at 161.

information in the government's application.[97] Had the FISC known all of the information the FBI actually had in its possession, there is a serious question of whether it would have found that the surveillance was justified. Three applications to renew the Page order included further omissions of fact, misstatements, and errors.[98]

The good news is that the IG found no evidence that the Carter Page surveillance was politically motivated.[99] The bad news is that the IG reached that conclusion, in part, because the Page application was no anomaly. A review of twenty-nine additional FBI FISA applications left the IG with "no confidence" in the FBI's procedures—known as the "Woods Procedures"—designed to ensure that FISA applications meet the standard of scrupulous accuracy.[100] Of the twenty-nine applications reviewed, four lacked evidence that the Woods Procedures had been followed at all, while the remaining twenty-five each suffered from discrepancies and errors.[101]

The Woods Procedures themselves were a response to a series of similar incidents that took place over two decades prior. Those incidents involved over seventy-five FBI FISA applications containing misstatements or omissions of material facts.[102] In response, the FBI created the Woods Procedures, named after the FBI lawyer who originally authored them,[103] to govern the preparation of FISA applications, "including procedures for reviewing draft FISA applications to ensure their accuracy."[104] The agent who requests the FISA application must create, maintain, and verify the completeness of a "Woods File," containing evidence supporting each factual assertion contained in the application.[105] When a Woods File is inaccurate or incomplete, that means that the factual assertions made to the FISC are, at best, unsubstantiated and, at worst, incorrect or misleading.

The responses to the 2000–2001 and the 2016 incidents violating the government's obligation of scrupulous accuracy were remarkably similar. In both instances, the FBI imposed sanctions on the known wrongdoers and added

97. *Id.* at 169.

98. *Id.* at 5.

99. *Id.* at 352.

100. OFF. OF THE INSPECTOR GEN., MANAGEMENT ADVISORY MEMORANDUM FOR THE DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION REGARDING THE EXECUTION OF WOODS PROCEDURES FOR APPLICATIONS FILED WITH THE FOREIGN INTELLIGENCE SURVEILLANCE COURT RELATING TO U.S. PERSONS 2 (2020).

101. *Id.* at 7–8.

102. *In re* All Matters Submitted to the Foreign Intel. Surveillance Ct., 218 F. Supp. 2d 611 (FISA Ct. 2002) (describing nature of misstatements and omissions); David Kris, *Further Thoughts on the Crossfire Hurricane Report*, LAWFARE (Dec. 23, 2019), https://www.lawfareblog.com/further-thoughts-crossfire-hurricane-report [https://perma.cc/D2XV-JPUP].

103. The original Woods Procedures have been supplemented by additional procedural requirements. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 42–43.

104. *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d at 621; *see also* DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 42–43 (In particular, the Woods Procedures seek to ensure accuracy with respect to the factual assertions supporting probable cause, whether there are any ongoing criminal investigations or prosecutions involving the target, and the nature of any relationship between the FISA target and the FBI.).

105. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 43.

procedural protections in hopes of preventing or detecting similar deficiencies in future applications.[106] The Woods Procedures themselves are, of course, the 2001 version of this strategy. Post-Carter Page, the FBI Director adopted a host of additional process enhancements recommended by the Department of Justice ("DOJ") IG and an amicus appointed by the FISC.[107] These include new FISA standards and procedures to "enhance accuracy and completeness" of applications,[108] a special questionnaire about any use of informants,[109] a greater supervisory role for FBI attorneys, and a requirement that FBI personnel disclose "all information that might reasonably call into question the accuracy of the information in the application or otherwise raise doubts about the requested probable cause findings or the theory of the case."[110] The added measures also included enhanced training[111] and mandatory audits to monitor the effectiveness of the new rules.[112]

Given the similarity between the responses to the flawed applications submitted from 2000–2001 and in 2016, it is unclear whether these procedural requirements will fully ameliorate the problem. The IG's findings demonstrate that the Woods Procedures failed to ensure that applications submitted to the court were accurate or complete;[113] there is no reason the new procedures should be any more effective. As the former head of DOJ's National Security Division and FISA court amicus David Kris argues, the types of inaccuracies identified by the IG require not just procedural reforms but cultural reforms.[114] To be sure, diligent enforcement of the rules implemented by FBI leadership can impact agency culture. But focus on such concerns inevitably ebbs over time, all but ensuring that—absent more drastic changes—similar problems will ultimately recur.

2. Overcollection

When the government engages in "overcollection," that simply means that it is gathering information that the surveillance laws and regulation do not permit it to collect. This has been a recurring problem, often compounded by government efforts to retain unlawfully collected information.[115] And while the FISC has usually (though not always) refused such requests, the government has not always complied promptly and fully with orders to purge the fruits of

106. Kris, *supra* note 102.

107. Letter Brief of Amicus Curiae David Kris, Judge Boasberg Mar. 4, 2020 opinion.

108. *Id*.

109. *Id*. at 5–9 (expanding information required by the form agents use to request FISA surveillance, "emphasizing the need to err on the side of disclosure" when it comes to information "relevant to the consideration of . . . probable cause," and including "all information . . . bearing on the reliability" of a confidential human source).

110. *Id.* at 6.

111. *Id.* at 9.

112. *Id.* at 11.

113. DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 413.

114. Kris, *supra* note 102.

115. *See supra* note 89 and accompanying text.

overcollection.[116] Each of the surveillance programs described above has resulted in overcollection.

a. Traditional FISA

One example of overcollection came in 2010 when the government reported numerous instances of traditional FISA surveillance in which the NSA failed to comply with rules requiring it to "monitor the acquisition of raw data . . . to verify that the surveillance is not avoidably acquiring communications outside the authorized scope."[117] The result was numerous instances (the exact number is redacted) of overcollection that continued "for periods ranging from approximately *15 months to three years*."[118] Despite conceding that this surveillance was unauthorized, the government wanted to retain and use the fruits of that collection.[119] It argued that the rules designed to prevent overcollection were "inapplicable to the communications [acquired] from unauthorized collection."[120] Recognizing that impermissibly collecting data should not be rewarded by permission to profit from that information, the court rejected this argument.[121]

b. Bulk Internet Metadata Collection Program

Overcollection was also a major issue with the bulk internet collection program.[122] When the program was authorized, the FISC approved collection of certain (redacted) *categories* of information.[123] For the first *five years* of that program, however, the government failed to limit its collection to those categories.[124] According to the FISC, "the NSA exceeded the scope of authorized acquisition continuously during the . . . years of acquisition under these orders."[125] This continuous overcollection meant that "'*virtually every record' generated by the program included some data that had not been authorized for collection*."[126] The government blamed this overcollection on "failure to translate technical requirements [redacted] into accurate and precise technical descriptions for the Court."[127] As the court noted, however, that explanation cannot account for why it went on so long, nor how an internal review undertaken explicitly for the

116. *See supra* note 89 and accompanying text.

117. Op. and Order Requiring Destruction of Information Obtained by Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00067 1 (FISA Ct. 2011) (Scullin, Jr., J.) [hereinafter Scullin May 13, 2011 opinion].

118. Op. and Order Regarding Fruits of Unauthorized Electronic Surveillance, [REDACTED], Nos. [REDACTED], GID.C.00059 1–2 (FISA Ct. 2010) (Scullin, Jr., J.) (emphasis added).

119. *Id*. at 3.

120. *Id*.

121. Scullin May 13, 2011 opinion, *supra* note 117, at 1.

122. I do not treat as a violation the existence of the bulk-collection programs, which themselves arguably violated statutory limits by their very existence. *See* PCLOB SECTION 215 REPORT, *supra* note 37, at 57–136.

123. *See* Judge Bates undated Pen/Trap opinion, *supra* note 53, at 2.

124. *Id.* at 2–3.

125. *Id*. at 20–21.

126. *Id*. at 20–21 (emphasis added).

127. *Id*. at 21.

purpose of ensuring compliance with the FISC's orders had overlooked the problem.[128] After this came to light, the court required the NSA's Office of General Counsel to conduct periodic spot checks to ensure that the program was "functioning as authorized by the Court."[129]

c. Upstream Section 702 Collection

Section 702 Upstream collection resulted in the NSA's collection of *millions* of communications beyond those authorized by Section 702 due to two aspects of that program. First, in addition to collecting communications that are to and/or from a tasked selector, Upstream collection also originally captured communications "in which the tasked selector is referenced within the acquired [communication], but the target is not necessarily a participant in the communication"; this is known as "about" collection because it collects communications not to or from a target, but about him.[130] So, Upstream collection netted all internet communications that were to, from, *or* about tasked selectors.[131] The problem is that Section 702 requires that at least one side of the communication must be a non-U.S. person outside the United States.[132] And while the *target* may meet that standard, communications containing a tasked e-mail address within them could be coming and going from anyone anywhere. So, every time such a communication was sent from one U.S. person to another—neither of whom was a surveillance target—acquiring that communication violated the statute. What the court in 2011 said was that, while a FISC opinion two years prior had authorized only certain types of "about" collection, the NSA had actually been collecting *all* "about" communications.[133] As with the internet metadata program, the government had *for years* failed to respect an explicit limitation the FISC had lain down.

The second complicating factor with Upstream collection stems from the fact that data moves across the Internet in the form of "transactions" (*i.e.*, packages within which information travels).[134] Some of these packages—known as multiple-communications transactions ("MCTs")—contain information constituting more than one communication.[135] The analog equivalent would be sending two letters in the same envelope. Contrary to what the government originally indicated to the FISC,[136] NSA's Upstream collection devices could neither filter

128. *Id*. at 16–22.

129. *Id*. at 13.

130. PCLOB SECTION 702 REPORT, *supra* note 62, at 37. Whether "about" collection was ever a valid exercise of Section 702 authority is a matter of debate. *See, e.g.*, Donohue, *supra* note 24, at 253; Dia Kayyali, *The Way the NSA Uses Section 702 Is Deeply Troubling. Here's Why*., EFF (May 7, 2014), https://www.eff.org/deeplinks/2014/05/way-nsa-uses-section-702-deeply-troubling-heres-why [https://perma.cc/85NM-V6Z9]; Jameel Jaffer, Dep. Legal Dir., ACLU, Statement at Public Hearing on Section 702 of the FISA Amendments Act (Mar. 19, 2014).

131. PCLOB SECTION 702 REPORT, *supra* note 62, at 36.

132. *Id.*

133. Judge Bates undated Pen/Trap opinion, *supra* note 53, at 14 n.16.

134. PCLOB SECTION 702 REPORT, *supra* note 62, at 39 (defining an internet transaction as "any set of data that travels across the Internet together such that it may be understood by a device on the Internet").

135. *Id*.

136. *Id*. at 16.

out MCTs[137] nor identify the parties to any communications contained within that MCT prior to collection.[138] As a result, if an MCT included at least one communication to, from, or about a tasked selector, the NSA would acquire the *entire* MCT, even if it also contained numerous other communications entirely unrelated to any tasked selectors.[139] The FISC determined that this meant that tens of thousands of entirely domestic communications that were not to, from, *or* about a target of surveillance were finding their way into government databases.[140]

Following the usual playbook, the government delayed in alerting the FISC to the problem. In fact, when the FISC learned about these aspects of Upstream collection in 2011—aspects which had been ongoing since 2006—it noted that "the volume and nature of the information the [NSA] has been collecting is fundamentally different from what the Court has been led to believe."[141] Moreover, the FISA judge was "troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark[ed] the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection problem."[142] The FISC found that the NSA's rules for handling Upstream data were not only insufficiently protective of Americans' rights to satisfy either the FISA Amendments Act or the Fourth Amendment, but also actually enhanced "the risk of error, overretention, and dissemination of . . . information protected by the Fourth Amendment."[143]

Despite the massive overcollection resulting from MCTs and "about" communications, the FISC declined to impose any additional constraints on collection.[144] Instead, it permitted the NSA to continue its collection practices but imposed a series of new minimization procedures focused specifically on retention and dissemination of domestic communications incidentally collected through the NSA's Upstream collection program.[145] Once the government had agreed to comply with these procedures, the FISC once again declared the program statutorily and constitutionally sound.[146]

137. *Id*. at 31.

138. *Id*. at 43.

139. PCLOB SECTION 702 REPORT, *supra* note 62, at 36.

140. Judge Bates Oct. 3, 2011 Opinion, *supra* note 85, at 32–33. A random sample of 50,040 internet transactions taken from the more than 13.25 million acquired through NSA's upstream collection during a six-month period showed that the "NSA acquires approximately 2,000-10,000 [internet transactions] each year that contain *at least* one wholly domestic communication." *Id*. at 33 n.30 (emphasis in the original). Thus, the "NSA is likely acquiring tens of thousands of discrete communications of non-targeted United States persons and persons in the United States" simply because "their communications are included in [a transaction] selected for acquisition by NSA's upstream collection devices." *Id*. at 37.

141. *Id*. at 28.

142. *Id*. at 16 n.14.

143. *Id*. at 78.

144. *Id*. at 28–29.

145. *Id*. at 54–55.

146. Mem. Op., *In re* [REDACTED], No. PR/TT [REDACTED], GID.C.00076 7–11 (FISA Ct. 2011) (Bates, J.) (The additional minimization procedures required that (1) transactions most likely to contain information concerning U.S. persons or persons in the U.S. would be segregated after acquisition; (2) transactions removed from or never subjected to segregation would be marked as such and all transactions acquired through

This was not, however, the end of the matter. In 2016, the FISC learned that since the previous year, some (redacted) portion of the NSA's Section 702-acquired communications had been mislabeled.[147] Some MCTs were erroneously labeled as containing only communications involving a target,[148] and some Upstream collection had been labeled as having been acquired from internet service providers (*i.e.*, having been collected through PRISM).[149] As the court pointed out, these incorrect labels would have exempted these communications from the heightened safeguards imposed in 2011, thereby circumventing one of the procedures that allowed the 2011 court to conclude that Upstream collection was statutorily and constitutionally lawful.[150]

When months of effort failed to produce an effective means of preventing these kinds of violations, the NSA pulled the plug. It rendered all Upstream internet transactions collected prior to March 17, 2017, inaccessible to analysts and, importantly, discontinued "abouts" collection altogether.[151] Such collection going forward would be an incident of noncompliance, and any MCTs acquired through "abouts" collection must be destroyed upon recognition.[152] In other words, in 2017, the NSA finally conceded that the only way it could comply with the FISC's constitutionally derived limits for "about" collection—limits that had theoretically been in place since 2011[153]—was to abandon that aspect of its surveillance altogether.

d. Section 702 "Foreignness" Determinations

A final systemic overcollection problem stems from Section 702's requirement that targets must be reasonably believed to be non-U.S. persons outside the United States.[154] To fulfill this requirement, the NSA must perform what is known as a "foreignness determination" to assess whether a proposed target meets that standard.[155] After a selector associated with that target is tasked for acquisition, the government must take reasonable steps to ensure that the selector *continues* to meet the targeting requirements.[156] If at any time the target enters the United States or is discovered to be a U.S. person, the collection is no longer

Upstream collection would be subject to special handling rules; and (3) all Upstream acquisitions would be retained for two years instead of the usual five).

147. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 80.

148. *Id.*

149. *Id*. at 23 n.24.

150. *Id*. at 80.

151. *Id*. at 25; *see* NSA TARGETING PROCEDURES, *supra* note 61, at 2; MINIMIZATION PROCEDURES USED BY THE NSA 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 [hereinafter NSA MINIMIZATION PROCEDURES].

152. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 69.

153. *Id.* at 28–29.

154. 50 U.S.C. § 1881a.

155. NSA TARGETING PROCEDURES, *supra* note 61, at 1.

156. *Id.* at 6–7.

authorized—it constitutes overcollection, and the information must be "destroyed upon recognition."[157]

Section 702 targets periodically are determined to be either U.S. persons or inside the United States (or both).[158] This problem can arise at any stage of the collection process—at the initial targeting, while collection is ongoing, or in the course of the required post-targeting review.[159] This is yet another area where government communications to the FISC have been less than fully forthcoming. The court identified multiple instances in which the government did not report failure to detask accounts after the NSA discovered that the target was inside the United States[160] and misrepresented to the court its post-tasking review process.[161] There have been relatively isolated instances of inadequate pretargeting screening[162] as well as more systemic violations. In 2010, for example, the government informed the FISC that the NSA had fallen behind in its required post-targeting reviews and that its efforts to purge communications of invalid targets had been incomplete.[163] As a result, information collected under Section 702 that should have been purged appeared in finished intelligence reports that the NSA disseminated.[164] In response, the government updated its targeting procedures, conducted additional training for analysts, and received court orders to purge the remaining data.[165]

In 2016, the compliance and implementation issues in connection with pre- and post-tasking assessments arose once again. The court determined that the method analysts were using to ensure targets were not U.S. persons was not sufficiently reliable.[166] The government blamed the improper taskings on the limitations of the technological tool it had been using to make foreignness determinations, but the court ascribed the problem to human error and "the failure of

157. *Id*. at 7.

158. *Id.* at 2–3.

159. *Id*. at 2–3, 8.

160. Mem. Op., [REDACTED], No. [REDACTED], GID.C.00051 12–14 (FISA Ct. 2009) (Hogan, J.).

161. *See* Mem. Op., [REDACTED], No. [REDACTED], GID.C.00062 19 (FISA Ct. 2010) (McLaughlin, J.) [hereinafter Judge McLaughlin 2010 opinion].

162. *See, e.g.*, ATT'Y GEN & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, December 1, 2014–MAY 31, 2015 (analysts failed to conduct sufficient pretargeting checks to ensure a target was not located in the U.S.).

163. Judge McLaughlin 2010 opinion, *supra* note 161, at 3.

164. *Id.*

165. Letter from George Ellard, Inspector Gen., Nat'l Sec. Agency, to Hon. Silvestre Reyes, Chairman, House Permanent Select Comm. on Intel., (Nov. 30, 2009); Letter from George Ellard, Inspector Gen., Nat'l Sec. Agency, to Hon. Silvestre Reyes, Chairman, House Permanent Select Comm. on Intel., (Nov. 19, 2010); ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, June 1, 2012–Nov. 30, 2012 at 5. *See generally* FBI ANNUAL REPORT ISSUED PURSUANT TO SECTION 702 OF FISA, Sept. 1, 2012–Aug. 31, 2013 at 4–9; ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, Dec. 1, 2012–May 31, 2013 at 6; ATT'Y GEN & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, June 1, 201–Nov. 30, 2014 at 6; Q. REP. TO THE FISC CONCERNING COMPLIANCE MATTERS UNDER SECTION 702 OF FISA, Dec. 1, 2014–Feb. 28, 2015.

166. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 70–75.

analysts" to be sufficiently diligent.[167] The NSA then developed a new tool to employ in its foreignness assessments, but the court warned that the new tool "should not be seen as a panacea."[168] Errors in foreignness determinations also necessitated significant modifications to information sharing between the NSA and the FBI with respect to tasking decisions.[169]

Overcollection concerns have thus dogged foreign intelligence collection across programs and over the course of many years. The court has always required the government to take steps to address these problems, but compliance has often been delayed and purges of improperly collected information have often been incomplete.

3. Improper Use of Collected Data

The point of surveillance is not the collection itself, of course, but the use to which the collected information can be put. The justification behind requiring the government to develop FISC-approved querying and minimization procedures is that the retention, use, and dissemination of the fruits of foreign intelligence surveillance also can have significant privacy implications.[170] Some of the most frequent compliance incidents—and the ones with some of the most significant impacts on Americans' privacy—have come in the postcollection context.

a. Improper Queries

A significant, recurring area of noncompliance is in querying the databases containing the data the government has collected. As with overcollection, these concerns have plagued several different surveillance programs.

167. *Id*. at 75.
168. *Id*.
169. *Id*.
170. *Id*. at 60.

TABLE 2. QUERYING STANDARDS BY PROGRAM AND AGENCY

Program	Agency	Querying Standard	
Internet and telephone metadata	All	Required a "reasonable articulable suspicion" that the selectors queried are associated with a targeted terrorist organization.	
Section 702	FBI	Non-U.S.-person queries and U.S.-person queries for foreign intelligence or evidence of a national-security-related crime	Selectors queried must be reasonably likely to retrieve foreign intelligence information, as defined by FISA, *or evidence of a crime*.
		U.S.-person queries for evidence of a non-national-security-related crime	FBI must apply to the FISC for an order by providing "a statement of the facts and circumstances relied upon ... to justify the belief ... that the contents sought would provide" evidence of criminal activity, contraband, or property used in committing a crime.
	CIA, NSA, NCTC	Non-U.S.-person queries	Selectors queried must be reasonably likely to return foreign intelligence information.
		U.S.-person queries	Requires a statement of facts establishing that the query is reasonably likely to return foreign intelligence information.

i. Bulk Collection Queries

Analysts could query the bulk telephone and internet metadata only when they had a "reasonable articulable suspicion" that the selectors used in the query were associated with a targeted terrorist organization.[171] Three years after the FISA court approved the programs, however, it discovered that the NSA had regularly disregarded this requirement.[172] As one unhappy FISA judge put it in 2009,

> The FISC's authorizations of this vast collection program have been premised on a flawed depiction of how the NSA uses [bulk record metadata]. This misperception by the FISC existed *from the inception* of its authorized collection in May 2006, buttressed by *repeated inaccurate statements* made in the government's submissions . . . The [required] minimization procedure[s] . . . have been so frequently and systemically violated that *it can fairly be said that this critical element of the overall [bulk records] regime has never functioned effectively*.[173]

171. PCLOB SECTION 215 REPORT, *supra* note 37, at 8–9.

172. *See* Judge Bates undated Pen/Trap opinion, *supra* note 53, at 14; Order Regarding Preliminary Notice of Compliance Incident Dated Jan. 15, 2009 at 2, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13, GID.C.00035 (FISA Ct. 2009) (Walton, J.).

173. Order at 11, *In re* Production of Tangible Things from [REDACTED], No. BR 08-13, GID.C.00036, (FISA Ct. 2009) (Walton, J.) (emphasis added); *see also* Mem. Op., [REDACTED], No. [REDACTED], GID.C.00061 8 n.10 (FISA Ct. 2010) (Bates, J.).

In other words, the NSA spent years digging through databases built through "exceptionally broad" collection activities and full of details about Americans' telephone and e-mail communications without the requisite justification.[174]

In response, the FISC required the Justice Department to periodically spot-check the NSA's justifications for querying data,[175] and it required the NSA to submit periodic reports to the FISC regarding the queries it performed.[176] The Justice Department's National Security Division also took on a greater role in assessing the adequacy of training and compliance.[177] Finally, the incident prompted an in-depth review at the NSA, whose results, among other things, ultimately led Congress to create a new position: NSA Director of Compliance.[178] Whether these responses would have effectively put a stop to the widespread violations of querying rules is unclear. The government discontinued the internet metadata collection program just two years later,[179] and Congress significantly curtailed the telephone metadata collection program in the USA Freedom Act of 2015.[180]

ii. Section 702 Queries

The FISC has stressed that "given the lenient retention standards for Section 702 information, . . . access restrictions are particularly important."[181] In other words, because the authorized targeting and collection rules are relatively permissive, back-end privacy protections, such as querying rules, assume outsized importance. Recall that despite the absence of any probable cause requirement or judicial approval of individual targets, Section 702 will necessarily collect a large number of communications involving U.S. persons.[182] Any query could therefore return the contents of Americans' communications—material the government could not have *targeted* for collection absent a showing of probable cause to a neutral magistrate.

174. *See* FISC's Pen/Trap Opinion, *supra* note 40, at 23.

175. Order at 6–11, *In re* Application of the Fed. Bureau of Investigation for an Ord. Requiring the Production of Tangible Things from [REDACTED], BR 06-05, GID.C.00006 (FISA Ct. 2006) (Howard, J.).

176. *See* Order Regarding Further Compliance Incidents, *In re* Application of the Fed. Bureau of Investigation for an Ord. Requiring the Production of Tangible Things from [REDACTED], No. BR 09-13, GID.C.00046 2 (FISA Ct. 2009) (Walton, J.); Judge Bates undated Pen/Trap opinion, *supra* note 53, at 19, 95–96.

177. Order Regarding Further Compliance Incidents, No. BR 09-13, at 3.

178. Intelligence Authorization Act for Fiscal Year 2010, Pub. L. No. 111-259, 124 Stat. 2653, 2732 (codified as amended at 50 U.S.C. § 402); John DeLong & Susan Hennessey, *Understanding Footnote 14: NSA Lawyering, Oversight, and Compliance*, LAWFARE (Oct. 7, 2016, 7:44 AM), https://www.lawfareblog.com/understanding-footnote-14-nsa-lawyering-oversight-and-compliance [https://perma.cc/VET2-2VV9].

179. *See* Charlie Savage, *File Says N.S.A. Found Way to Replace Email Program*, N.Y. TIMES (Nov. 19, 2015), https://www.nytimes.com/2015/11/20/us/politics/records-show-email-analysis-continued-after-nsa-program-ended.html [https://perma.cc/ZY6R-HF8F].

180. USA Freedom Act of 2015, Pub. L. No. 114-23 secs. 501–03, 129 Stat. 267, 283. The FISA business records provision subsequently reverted back to even more circumscribed, pre-Patriot Act language when Congress failed to extend a sunset deadline in 2020. *See* Savage, *supra* note 56.

181. Mem. Op., [REDACTED], No. [REDACTED], 402 F. Supp. 3d 45, GID.C.00258 64 (FISA Ct. 2018) (Boasberg, J.) [hereinafter Judge Boasberg Oct. 18, 2018 opinion].

182. *See supra* notes 58–77 and accompanying text.

Violations of rules for querying Section 702 data, in particular by the NSA and the FBI, have been extensive. We begin with the NSA, which may query such data only using terms, "such as phone numbers or key words," that are "reasonably likely to return foreign intelligence information."[183] The rules governing queries of terms associated with a U.S. person—so-called "U.S.-person queries"—are more stringent. When employing U.S.-person queries on data collected through PRISM, the agency must "prepare a statement of facts establishing that it is reasonably likely to return foreign intelligence information."[184] In the Upstream context, however, U.S.-person queries were forbidden so long as "about" collection continued due to the presence in that data pool of Americans' domestic communications unrelated to any valid target.[185]

What the court learned in 2016, however, is that the NSA had not been adhering to these rules.[186] Instead, it had been conducting U.S.-person queries of Upstream data "with much greater frequency than had previously been disclosed."[187] The court characterized the problem as "widespread" and noted that it constituted "a very serious Fourth Amendment issue."[188] The NSA laid the blame at the feet of both human error and systems design.[189] Even if the cause of the problem was a technical one, however, the NSA engaged in the now-familiar habit of failing to notify the FISC about the violations until over a year after they had been discovered—a delay that the FISA judge characterized as an "institutional lack of candor."[190] It was due to the NSA's inability to determine the exact scope of the problem or to ensure compliance with sufficiently protective minimization and querying rules[191] that it discontinued "about" collection entirely.[192]

Nor were the impermissible U.S.-person queries limited to Upstream data. That same year, the NSA informed the court that, for the previous four years, analysts had been inadvertently querying PRISM Section 702 data in violation of the rules for U.S.-person queries as well.[193] This problem was prevalent when using a particular (redacted) tool; in one five-month period, 85% of the queries using that tool failed to comply with requirements.[194] The government was "unable to provide a reliable estimate of the number of non-compliant queries since 2012," but the FISC found no reason to believe that the five-month sample

183. NSA MINIMIZATION PROCEDURES, *supra* note 151, at 4–5 § 3(b)(5).

184. *Id*.

185. *Id*. at 4 § 3(b)(4)b.; *NSA Stops Certain Section 702 "Upstream" Activities*, NAT'L SEC. AGENCY (Apr. 28, 2017), https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/1618699/nsa-stops-certain-section-702-upstream-activities/ [https://perma.cc/6DR6-PAGZ].

186. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 19.

187. *Id.*

188. *Id*.

189. *Id*. at 20–21.

190. *Id.* at 19. It was during this same time period that some of the Upstream data was not correctly labeled as such, thereby making that data available for U.S.-person queries when it should not have been. *Id.* at 23 n.24.

191. *Id.* at 23.

192. *See supra* note 151 and accompanying text.

193. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 81–82.

194. *Id.* at 82.

already reviewed was not representative.[195] The problem was addressed through additional training and technological fixes.[196]

In addition to these particularly significant incidents discovered in 2016, problematic NSA queries have been a constant throughout the lifetime of Section 702. Violations of the querying requirement that they must be likely to return foreign intelligence information, that querying U.S.-person data without proper approval, and that continuing to query selectors after they are determined to belong to a U.S.-person appear in compliance reports year after year.[197] The remedies for most of these incidents have been to remind the relevant analysts of the applicable rules and to delete the query results.[198]

FBI queries of Section 702 data pose particularly significant threats to constitutional rights for at least two reasons. First, while the NSA, CIA, and NCTC are limited to queries reasonably likely to return foreign intelligence information, FBI queries "must be reasonably likely to retrieve foreign intelligence information . . . *or evidence of a crime*."[199] The FBI is thus permitted to query Section 702 information for purposes entirely independent of the foreign intelligence purposes that justified the initial collection. This means that the FBI may run a query about someone even if its intent is solely to find "evidence of crimes, whether or not those crimes relate to foreign intelligence."[200]

Second, the FBI conducts many more queries of U.S.-person identifiers than other intelligence agencies.[201] The FBI's querying practices are therefore both more likely to impact Americans' interests than those of the other agencies and are available in a broader swath of circumstances. The actual impact on

195. *Id.*

196. *Id.* at 82–83.

197. *E.g.*, ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, June 1, 2015–Nov. 30, 2015 20 (2016); ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA, Dec. 1, 2014–May 31, 2015 19 (2015) [hereinafter 2015 SEMIANNUAL REPORT]; QUARTERLY REPORT TO THE FISC CONCERNING COMPLIANCE MATTERS UNDER SECTION 702 OF FISA 58 (2015); QUARTERLY REPORT TO THE FISC CONCERNING COMPLIANCE MATTERS UNDER SECTION 702 OF FISA 46 (2014); ATT'Y GEN. & DIR. OF NAT'L INTEL., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUED PURSUANT TO SECTION 702 OF FISA 17 (2013); Letter from George Ellard, Dir. Nat'l Intel. Inspector Gen. to Hon. Silvestre Reyes, Chairman, Permanent Select Comm. on Intel., (Dec. 19, 2012); Letter from George Ellard, Dir. Nat'l Intel. Inspector Gen. to Hon. Silvestre Reyes, Chairman, Permanent Select Comm. on Intel., (Dec. 30, 2011); Letter from George Ellard, Dir. Nat'l Intel. Inspector Gen. to Hon. Silvestre Reyes, Chairman, Permanent Select Comm. on Intel., (Nov. 19, 2010).

198. *E.g.*, Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 82–83.

199. QUERYING PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIFN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 3 § IVA1 (2020) (emphasis added). Information about a U.S. person can be used as evidence only in criminal cases involving national security implications or other serious crimes. Judge Hogan Nov. 6. 2015 opinion, *supra* note 89, at 30 n.28. This rule says nothing, however, about using as evidence the fruits of Section 702 information.

200. Judge Hogan Nov. 6. 2015 opinion, *supra* note 89, at 33.

201. Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 66 ("In 2017, NCTC, the CIA, and NSA collectively used approximately 7500 terms associated with U.S. persons to query content information acquired under Section 702, while during the same year FBI personnel on a single system ran approximately 3.1 million queries against raw FISA-acquired information, including section 702-acquired information.").

Americans' privacy of these querying practices for years was impossible to assess, because the FBI declined to document its use of U.S.-person queries until ordered to do so by both Congress and the FISC.[202] But the potential implications of permitting the FBI to query Section 702 data for U.S.-person communications without probable cause and a warrant have led many commentators to argue that such queries pose too great a threat to Americans' Fourth Amendment rights.[203]

The controversial nature of U.S.-person queries of Section 702 data for law-enforcement purposes prompted statutory reform. The FISA Amendments Reauthorization Act required that, first, when a query performed "in connection with a predicated criminal investigation . . . that does not relate to the national security of the United States" returns the contents of U.S.-person communications, the FBI must apply to the FISC for an order authorizing such a query.[204] To secure such an order, the FBI must provide to the FISC "a statement of the facts and circumstances relied upon . . . to justify the belief . . . that the contents sought would provide" evidence of criminal activity.[205] So the standard still does not rise to the level of probable cause—which is what would normally be required to collect an American's electronic communications—but it interposes the FISC between the FBI's analysts and their querying decisions in investigations unrelated to national security. Second, Congress required the FBI to keep a record "of each United States person query term used."[206]

Unfortunately, the FBI's compliance problems regarding access to Section 702 data have been even more pronounced than that of the NSA. Throughout the Section 702 program, there have been isolated instances of FBI noncompliance with existing querying rules.[207] After the heightened protections of the FISA

202. *See id.* at 47–48, 95.

203. *See* Elizabeth Goitein, *The NSA's Backdoor Search Loophole*, BOS. REV. (Nov. 14, 2013), https://www.bostonreview.net/articles/the-nsas-backdoor-search-loophole/ [https://perma.cc/YG8V-X44Q]; Julian Sanchez, *Reforming Surveillance Authorities*, *in* CATO HANDBOOK FOR POLICYMAKERS 100–07 (8th ed. 2017); Laura Donohue, *The Case for Reforming Section 702 of U.S. Foreign Intelligence Surveillance Law*, COUNCIL ON FOREIGN RELS. (June 26, 2017), https://www.cfr.org/report/case-reforming-section-702-us-foreign-intelligence-surveillance-law [https://perma.cc/2NXW-PSUU].

204. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, sec. 101 § 702(f)(2)(A), 132 Stat. 3, 4. There is an exception for content that "could assist in mitigating or eliminating a threat to life or serious bodily harm." § 702(f)(2)(E); *see also* Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 65 ("Given the importance and prevalence of querying, it is a logical focus for efforts to balance protection of U.S. persons' privacy interests against foreign-intelligence needs. The enactment of Section 702(f) indicates Congress drew a similar conclusion."); H.R. REP. NO. 115-475, pt. 1, at 17 (2017) ("[C]ertain lawmakers and privacy advocates worry about the ability of the Intelligence Community to query lawfully acquired data using query terms belonging to United States persons."). It was this legislation that for the first time required agencies to submit to the FISC for approval a standalone set of querying procedures (previously, querying rules had been part of an agency's minimization procedures). FISA Amendments Reauthorization Act of 2017, sec. 101, § 702(f)(1)(A).

205. Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 47; FISA Amendments Reauthorization Act of 2017, sec. 101 § 702(f)(2)(C)(ii). Failure to obtain such an order precludes the use of information concerning a U.S. person obtained through the pertinent query in a criminal proceeding against that person "unless the AG determines the criminal proceeding relates to the national security or one of several specified serious crimes." Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 47.

206. FISA Amendments Reauthorization Act of 2017, sec. 101 § 702(f)(1)(B).

207. In 2015, for example, one FBI employee repeatedly searched Section 702 data for their own communications and those of several colleagues. 2015 SEMIANNUAL REPORT, *supra* note 197, at 43.

Amendment Reauthorization Act went into effect, the violations were far from isolated. As an initial matter, the FBI defied Congress's record-keeping mandate, asserting that its practice of keeping records of *all* query terms—without differentiating between U.S.-person and non-U.S.-person terms—was sufficient.[208] The FISC disagreed, insisting that the plain language of the statute required that the FBI develop a system of tracking U.S.-person queries separately.[209] Evasion of record-keeping requirements may not seem like a significant problem. But in the absence of FISC oversight of individual queries, agency records become the only means of enabling oversight or audits by supervisors, IGs, and Congress.[210] In their absence, violations can easily go undetected. Record-keeping also provides a deterrent to misuse. The FBI's resistance to providing this critical element of meaningful oversight displays a disappointing lack of concern about the privacy implications of Section 702 queries.

Nor were the problems isolated to the FBI's clerical practices. While the FISC found in 2018 that the FBI's querying procedures were consistent with the law *on paper*, it found that *in practice* they were insufficient[211] because "the reported querying practices present a serious risk of unwarranted intrusion into the private communications of a large number of U.S. persons."[212] And while "[r]easonableness under the Fourth Amendment does not require perfection," the FBI practices "demonstrated risks of serious error and abuse" alongside procedures inadequate to "guard against that risk."[213]

More specifically, the FBI had run "a large number" of queries that failed to meet the querying standard (*i.e.*, they were not likely to return foreign intelligence information or evidence of a crime).[214] The FISC concluded that a large number of these queries evidenced "a misunderstanding of the querying standard –or an indifference toward it"[215] and provided an illuminating list of examples:

- Ignoring the advice of the FBI's Office of General Counsel, in March of 2017, the FBI conducted queries using 70,000 identifiers "associated with" people who had access to FBI facilities and systems.
- One day in December of 2017, the FBI conducted over 6,800 queries using U.S. persons' Social Security Numbers.
- In February of 2018, the FBI conducted forty-five U.S.-person queries in order to collect information on individuals under consideration to serve as informants.
- On multiple occasions, FBI personnel conducted U.S.-person queries accidentally or for improper personal purposes.[216]

208. Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 49, 52.

209. *Id.*

210. H.R. REP. NO. 115-475, pt. 1, at 18 (2017); Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 58.

211. Judge Boasberg Oct. 18, 2018 opinion, *supra* note 181, at 68.

212. *Id.* at 89.

213. *Id.* at 91.

214. *Id.* at 81.

215. *Id.* at 72.

216. *Id.* at 68–72.

These queries, the FISC noted—which constitute accessing and examining "private communications of particular U.S. persons on arbitrary grounds"—squarely implicate the Fourth Amendment, whose purpose "is to safeguard the privacy and security of individuals against arbitrary invasions by governmental officials."[217]

As problematic as these queries were on their own, the FISC pointed out that the severity of the issue they represent is actually understated for three reasons. First, oversight of FBI field offices is extremely infrequent: some offices go more than two years between audits.[218] As a result, the number of queries subject to audits is dwarfed by the number of queries that are performed. These infrequent audits are no doubt one factor contributing to delays in detecting querying violations,[219] but also suggest that large numbers of improper U.S.-person queries may have gone undetected.[220]

Second, FBI policy sends mixed messages to agents.[221] On the one hand, Section 702 queries must be narrowly drawn to return foreign intelligence information or evidence of a crime.[222] On the other hand, the FBI's minimization procedures refer to Section 702 queries as "a routine and encouraged practice," even at the very early stages of an investigation.[223] The court concluded that these competing messages "create an environment in which unduly lax applications of the . . . querying standard[s] are more likely to occur."[224]

Finally, the FBI seems to have adopted an overbroad interpretation of the querying standard to allow for so-called "batch" queries.[225] A batch query is one in which a *group* of identifiers is run as one query because there is reason to believe that one of those identifiers will return foreign intelligence information or evidence of a crime.[226] The government provides the following example: imagine that the FBI has information that an employee at a particular defense contractor plans to sell classified technology.[227] If 100 employees have access to that information, the government maintains that it could run a "categorical query of the identifiers associated with these 100 employees" simply because, as a group, there is reason to believe that the query will return foreign intelligence information or evidence of a crime.[228] As the court put it, the government's view is that "an aggregation of individual queries can satisfy the querying standard, even

217. *Id.* at 89 (quoting Camara v. Mun. Ct. of City and Cnty. of S.F., 387 U.S. 523,528 (1967)).
218. *Id.* at 73.
219. *Id.*
220. *Id.* at 74. Even when oversight does take place, it may not be effective. Unlike the CIA and NSA, the FBI did not require agents to memorialize their reasons for believing that a querying term met the relevant standard, thereby depriving oversight personnel of "basic information that would assist in identifying problematic queries." *Id.* at 73–74.
221. *See id.* at 75–76.
222. *Id.* at 73–74.
223. *Id.* at 75.
224. *Id.* at 76.
225. *Id.* at 78.
226. *Id.*
227. *Id.*
228. *Id.*

if each individual query in isolation would not."[229] The FISC rejected this interpretation emphatically, pointing out that "justification-by-aggregation" is not consistent with the requirement that "[e]ach query" meet the standard.[230]

The court's response was not, however, to impose any sanctions or to require the FBI to discontinue Section 702 queries or even to discontinue U.S.-person queries. Instead, the FISC required the FBI to amend its querying procedures to

> require that the FBI's query records differentiate between U.S. person queries and all other queries; the FBI record a written justification stating why a U.S. person query was reasonably likely to retrieve foreign intelligence information or evidence of a crime prior to reviewing the contents returned by such a query; and the FBI make available records generated under these requirements to enable oversight by the Department of Justice and the ODNI.[231]

As of the most recently available opinion, the FISA court "continues to be concerned about the FBI's querying practices" with respect to both substance and procedure.[232] In fact, there remains evidence of "widespread violations of the querying standard."[233] Substantively, the court noted that at least forty U.S.-person queries should have gotten a certification from the FISC but did not; that, despite the FISC's rejection of batch queries as unlawful, at least one analyst ran a "batch query" on Section 702-acquired information and failed to record whether U.S.-person query terms were employed; and that there were instances in which the government allowed users to view the content of Section 702 information without entering a justification in the system.[234] The court did impose several new reporting requirements related to batch queries, but nevertheless determined that, because the FBI's systems and training *could* eventually serve to stave off these violations, the existing querying and minimization procedures meet statutory and Fourth Amendment requirements.[235]

b. Other Violations of Minimization Procedures

In addition to the above, periodic additional violations, such as failing to follow rules about information dissemination, have been common. In the context of the bulk metadata collection programs, for example, the NSA at times disseminated information in contravention of the FISC's orders.[236] The government has

229. *Id.*

230. *Id.* at 79.

231. *Release of Documents Related to the 2018 FISA Section 702 Certifications*, INTEL.GOV (Oct. 8, 2019), https://www.intelligence.gov/ic-on-the-record-database/results/951-release-of-documents-related-to-the-2018-fisa-section-702-certifications [https://perma.cc/2AK6-P5WA].

232. Judge Boasberg Nov. 18, 2020 opinion, *supra* note 67, at 39.

233. *Id.* at 44.

234. *Id.* at 42–43.

235. *Id.* at 60–66.

236. *See, e.g.*, Spencer Ackerman, *FISA Court Documents Reveal Extent of NSA Disregard for Privacy Restrictions*, GUARDIAN (Nov. 19, 2013, 1:42 PM), https://www.theguardian.com/world/2013/nov/19/fisa-court-documents-nsa-violations-privacy [https://perma.cc/W4WE-YCAG].

also permitted unauthorized access to data or included in intelligence reports disseminated to other agencies U.S.-person information without complying with the minimization requirements designed to protect U.S. persons' privacy.[237] In fact, at one point the FISA court determined that the "NSA generally disregarded the special rules for disseminating United States person information outside of NSA until it was ordered to report such disseminations and certify to the FISC that the required approval had been obtained."[238] Similarly, the FBI has shared unminimized Section 702 data with private contractors not authorized to review it[239] and has had recurring problems with its treatment of attorney-client communications.[240] Failure to purge information collected in violation of the rules in a timely fashion has also been a recurring issue across agencies.[241] As with so many of the compliance incidents detailed in this Section, the remedy for these violations has been increased training, more procedural protections, and promises from the government to do better.[242]

***

As the foregoing discussion demonstrates, the government repeatedly violates the rules designed to protect Americans' rights. These violations, moreover, recur repeatedly despite efforts to prevent them. This leads me to draw several conclusions. First, the country's foreign intelligence surveillance officials are prone to overstepping limits, and the FISC is loath to order the government to

237. *See, e.g.*, KEVIN J. O'CONNOR, U.S. DEP'T OF JUST., QUARTERLY REPORT TO THE FOREIGN INTELLIGENCE SURVEILLANCE COURT CONCERNING COMPLIANCE MATTERS UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (2015) (NSA issued a report that included U.S.-person information); U.S. DEP'T OF JUST., SEMIANNUAL ASSESSMENT OF COMPLIANCE WITH PROCEDURES AND GUIDELINES ISSUES PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, SUBMITTED BY THE ATTORNEY GENERAL AND THE DIRECTOR OF NATIONAL INTELLIGENCE 32–33 (2014) (NSA analysts used automation to disseminate FISA-acquired information without ensuring it did not include U.S.-person information); Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 85–86 (The FBI gave a contractor access to unminimized Section 702 data).

238. *See* Judge Bates undated Pen/Trap opinion, *supra* note 53, at 95; Order, *In re* Application of the Fed. Bureau of Investigation for an Ord. Requiring the Production of Tangible Things from [REDACTED], No. BR 09-06, GID.C.00041 4 (FISA Ct. 2009) (Walton, J.).

239. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 83–86 (describing non-FBI personnel getting access to raw Section 702 information).

240. The FBI's law enforcement mission means that its targets for foreign intelligence might also be targets of criminal investigation. When that is the case, minimization procedures require the establishment of a "separate review team whose 'members have no role in the prosecution of the charged criminal matter'" whose job is to identify and sequester privileged communications. Judge Hogan Nov. 6. 2015 opinion, *supra* note 89, at 47–48. In numerous instances, the FBI failed to establish such teams when they were required, significantly delayed the establishment of such teams, and displayed other deficiencies that remain redacted. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 89–93; *see also id*. at 89 ("Failures of the FBI to comply with this 'review team' requirement for particular targets have been a focus of the FISC's concern since 2014."). The FBI failed to establish the appropriate teams in 2014, had not adequately addressed these failures by the time the government applied for the 2015 Section 702 reauthorization, and the issue remained a concern for the court in 2016. *See* Judge Hogan Nov. 6. 2015 opinion, *supra* note 89, at 47–52. The court was satisfied, however, that appropriate remedial measures were underway by that point and therefore held that these past failures did not render the FBI's minimization procedures insufficient. *See id.* at 50–52.

241. *See, e.g.*, Scullin May 13, 2011 opinion, *supra* note 117, at 1, 9; Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 87–89; Judge Hogan Nov. 6. 2015 opinion, *supra* note 89, at 55–60.

242. Judge Boasberg Nov. 18, 2020 opinion, *supra* note 67, at 61–66.

discontinue use even of programs that are persistently problematic. This is not an indictment of the individuals involved in these programs or of the judges on the FISC. Rather (and this is the second conclusion), even government officials sincerely trying to follow the rules will sometimes stray—perhaps without even knowing they have done so. But even when the violations are hard to explain by anything other than disregard for the rules, the FISC has proved unwilling to impose on the intelligence agencies constraints that go beyond augmenting procedural protections in an effort to reinforce existing rules. Even when it was clear that the NSA could not engage in Upstream "about" collection while satisfying targeting and minimization rules, the court continued to reauthorize the program; ultimately, it was the NSA that decided to discontinue "about" collection. This leads to the third conclusion I draw from this information: if one views the preceding examples as problematic—that current levels of noncompliance pose an unacceptable threat to Americans' privacy rights—it is time to consider whether there are mechanisms available that are more likely to effectively safeguard individual rights. The next Part will explore one theoretical concept that can help devise such mechanisms.

III. THE INEVITABILITY OF CHRONIC UNDERENFORCEMENT

Scholars have identified several structural factors that render systemic underenforcement of legal norms likely. This Part argues that many of these structural features are inherent in surveillance activities, and therefore the chronic underenforcement detailed in Part II is both predictable and inevitable. Section A will briefly flesh out the concept of underenforcement, before Section B identifies the characteristics of surveillance that lead to underenforcement.

A. Constitutional Meaning and Constitutional Enforcement

Since Henry Monaghan's seminal 1975 article, *Constitutional Common Law*,[243] commentators have recognized a distinction between constitutional *meaning*—what the words of the Constitution actually protect or proscribe—and constitutional *doctrine*—the rules judges use to decide constitutional questions.[244] Any application of the Constitution requires a judge to first derive

243. *See* Monaghan, *supra* note 19.

244. *See id.* at 20 ("[The Supreme Court has] explicitly drawn a line between the basic rights authoritatively declared to inhere in the Constitution and the formulation of their specific and admittedly variable components."); Sager, *supra* note 19, at 1214 ("[T]he important difference between a true constitutional conception and the judicially formulated construct is that the judicial construct may be truncated for reasons which are based" on pragmatic concerns rather than "analysis of the constitutional concept"); Fallon, *supra* note 19, at 57 ("[T]he Court often must craft doctrine that is driven by the Constitution, but does not reflect the Constitution's meaning precisely."); Strauss, *supra* note 19, at 207 (arguing that constitutional doctrine reflects both "principles and values" and "institutional realities"); Klein, *supra* note 19, at 1035; Landsberg, *supra* note 19, at 926; Berman, *supra* note 19, at 36 (noting that some scholars divide "judge-announced constitutional law into two conceptually distinct components— . . . constitutional meaning and constitutional doctrine"); Kermit Roosevelt III, *Aspiration and Underenforcement*, 19 HARV. L. REV. F. 183, 193 (2006). *But see* Levinson, *supra* note 19, at 858 (positing that the substance of constitutional rights is defined by the available remedies).

meaning from a constitutional provision and then to translate that meaning into workable doctrinal rules.[245] The key insight of this literature is that the resulting doctrinal framework can, at times, produce rules that are not coextensive with the meaning of the Constitution itself. In other words, doctrine might either over- or underenforce constitutional rights. That is to say, the chosen means of implementing the constitutional principle at issue will inevitably sometimes allow violations of the Constitution to go unredressed and at other times prohibit some conduct that should be considered constitutionally permissible.[246]

Some scholars refer to rules that self-consciously guard against the risk of underenforcing constitutional rights as "prophylactic rules,"[247] while others find that label unhelpful because, in their view, there is no means of identifying which rules qualify for the label.[248] Both camps agree, however, that there are multiple possible doctrinal rules among which judges may choose for the implementation of each constitutional provision and that some will be more protective of rights than others.[249] The form that doctrinal rules take depends on many factors, such as the institutional competence of the decision-maker or the relative costs of over- and underinclusiveness.[250] But among these factors is the perceived risk of

245. *See, e.g.*, Caminker, *supra* note 19, at 7 (arguing that constitutional interpretation requires a judge to "translate" abstract constitutional norms first into rights and then into "a more specific and workable set of doctrinal rules" to "enforce that duty").

246. *See, e.g.*, Fallon, *supra* note 19, at 66 ("[T]he Court does not necessarily betray its obligation of constitutional fidelity if it fails to craft judicially enforceable rules that fully protect constitutional norms."); Caminker, *supra* note 19, at 1 n.2 (recognizing that doctrine is sometimes "self-consciously crafted by courts for the instrumental purpose of . . . safeguarding against the violation of constitutional norms").

247. *See, e.g.*, Klein, *supra* note 19, at 1032 (defining prophylactic rules as "judicially-created doctrinal rule[s] . . . [that] may be triggered by less than a showing that the explicit rule was violated"); Michael Abramowicz, *Constitutional Circularity*, 49 UCLA L. REV. 1, 43 (2001) (defining a prophylactic rule as "a rule of law beyond what the text of the Constitution explicitly requires"); Landsberg, *supra* note 19, at 926–27 ("[Prophylactic rules] . . . are predicated on a judicial judgment that the risk of a constitutional violation is sufficiently great that simple case-by-case enforcement of the core right is insufficient to secure that right."); Michael C. Dorf & Charles F. Sabel, *A Constitution of Democratic Experimentalism*, 98 COLUM. L. REV. 267, 457 (1998) ("Wherever judicially established rules comprise an effort to give effect to more deeply established but vaguer legal norms, the judicial doctrine may be regarded as prophylactic. . . ."). *But see* Grano, *supra* note 19, at 123–56 (arguing that intentionally overprotective rules are sometimes illegitimate); Thomas S. Schrock & Robert C. Welsh, *Reconsidering the Constitutional Common Law*, 91 HARV. L. REV. 1117, 1118 (1978) (same); Dickerson v. United States, 530 U.S. 428, 446 (2000) (Scalia and Thomas, JJ., dissenting) (same).

248. *See, e.g.*, Levinson, *supra* note 19, at 915–16; *id*. at 922 ("[A]ny constitutional right can be described as overenforced, or prophylactic, relative to some hypothesized 'core' principle."); Strauss, *supra* note 19, at 195 ("'Prophylactic' rules are, in an important sense, the norm, not the exception."); Caminker, *supra* note 19, at 2 ("[T]here is no difference in kind, or meaningful difference in degree, between . . . [a] prophylactic rule and the run-of-the-mill judicial doctrines routinely constructed by the Court . . . .").

249. Levinson, *supra* note 19, at 873–74; Berman, *supra* note 19, at 9; David A. Strauss, *Miranda, the Constitution, and Congress*, 99 MICH. L. REV. 958, 960 (2001) (arguing that "constitutional rules—routinely, unavoidably, and quite properly—treat 'the Constitution itself' as requiring 'prophylaxis'").

250. *See, e.g.*, Caminker, *supra* note 19, at 9 ("Sometimes, the Court will conclude that the likelihood of false-negatives is unacceptably high; in other words, the direct doctrinal inquiry actually proves to be insufficiently protective of the constitutional values at stake."); Strauss, *supra* note 249, at 962–64 (explaining that the error rate of a case-specific-voluntariness test is one factor in a judgment regarding how best to implement the right against self-incrimination); Susan R. Klein, *Miranda Deconstitutionalized: When the Self-Incrimination Clause and the Civil Rights Act Collide*, 143 U. PA. L. REV. 417, 482–83 (1994) (arguing that the Supreme Court has an obligation to adopt rules that safeguard constitutional provisions that might otherwise be at risk).

underenforcement: in crafting constitutional doctrine, courts might opt for a rule that is more likely to fully protect constitutional rights than the alternatives.[251]

The quintessential example of such a rule is the requirement in *Miranda v. Arizona* that unwarned statements made during custodial interrogations may not be introduced against a criminal defendant as part of the prosecutor's case-in-chief.[252] The Constitution's Fifth Amendment itself proscribes the use of involuntary or coerced confessions.[253] Having determined that custodial interrogation will frequently produce involuntary statements, however, the Court decided to bar the use of *all* such statements not preceded by *Miranda* warnings, on the theory that many of those statements would actually be involuntary, but courts would not be able to accurately identify them as such.[254] The Court recognized that barring use of *all* un-*Mirandized* statements might result in disallowing the introduction of some statements that were not, in fact, involuntarily given.[255] As Professor Strauss put it, "*Miranda* represents [a] deliberate choice to exclude some voluntary confessions, in exchange for the benefits of excluding or deterring some compelled confessions that would otherwise escape detection."[256] In other words, recognizing that a rule simply barring the use of involuntary confessions would result in underenforcement of the Fifth Amendment, the Court opted to hedge against that risk by using a rule that would instead tend to create a buffer between the constitutional guarantee of voluntariness and permissible government action.

B. Surveillance Law's Tendency Towards Underenforcement

Commentators have identified three, sometimes overlapping, circumstances that tend to produce underenforcement. The first is when there are systemic factors likely to lead to rules violations. The second is when rules violations are difficult to detect. And finally, there are instances in which effective enforcement requires clear rules for both deterrence and ease of administration. This Section will discuss these factors and explore how they apply to surveillance rules.

251. *See, e.g.*, Monaghan *supra* note 19, at 21 (arguing that sometimes "it is necessary to overprotect a constitutional right because a narrow, theoretically more discriminating rule may not work in practice"); Landsberg, *supra* note 19, at 950 (pointing out that prophylactic rules "are predicated on a judicial judgment that the risk of a constitutional violation is sufficiently great that simple case-by-case enforcement of the core right is insufficient to secure that right"); Caminker, *supra* note 19, at 9 ("[S]ometimes, the Court will conclude that the likelihood of false-negatives is unacceptably high; in other words, the direct doctrinal inquiry actually proves to be insufficiently protective of the constitutional values at stake . . . .").

252. *See generally* 384 U.S. 436, 444 (1966).

253. U.S. CONST. amend. V.

254. *Miranda*, 384 U.S. at 457–58, 478–79.

255. *Id.* at 467.

256. Strauss, *supra* note 249, at 962. Of course, the prophylactic nature of *Miranda* has been called into question by *Dickerson*. *Id.* at 958.

1. Systemic Pressures Toward Underenforcement

Certain rules will consistently and predictably underenforce the norms they are meant to protect.[257] When it comes to surveillance law, the very nature of the project invites underenforcement of rules designed to protect privacy. The *raison d'etre* of the programs—and thus the mission of the officials implementing them—is nothing less than the physical security of the homeland. It is no surprise that the professionals in the intelligence community will value national security over other, sometimes conflicting, values.[258] Indeed, as General Hayden's statement about getting chalk on the government's cleats indicates, pushing the envelope was the foundational strategy behind the development of some of these programs.[259] This is no indictment of government officials who have dedicated their careers to keeping Americans safe. It is their job to prioritize these security goals. It does, however, skew the playing field in favor of the underenforcement of First and Fourth Amendment requirements.

Pervasive secrecy will also increase the likelihood of underenforcing surveillance rules. More specifically, underenforcement flows from the relative absence of transparency and accountability that accompanies such secrecy. Reliance on internal executive oversight or oversight by the congressional intelligence committees is no substitute for the disinfectant provided by sunlight, as Justice Brandeis might put it.[260] Foreign intelligence surveillance is particularly opaque. The FISC's proceedings are closed, its opinions are presumptively classified, and—because surveillance targets rarely know they have been targeted—even *post hoc* review of surveillance activities is vanishingly infrequent.[261] And in the cases where criminal defendants have been notified that evidence against them came from foreign intelligence surveillance authorities, those defendants and their attorneys have been denied meaningful access to information about that surveillance.[262] This lack of transparency renders public scrutiny of surveillance activities minimal. To the extent the public has been able

257. *See Miranda*, 384 U.S. at 447; *see also, e.g.*, N.Y. Times v. Sullivan, 376 U.S. 254, 279 (1964) (justifying overprotective rule in libel cases on the grounds that "[a] rule compelling the critic of official conduct to guarantee the truth of all his factual assertions" would unduly limit speech protected by the First Amendment); Fallon, *supra* note 19, at 63 ("As the Court recognized . . . mistakes are 'inevitable in free debate,' and a rule allowing all false and defamatory utterances to be actionable would have a predictable effect . . . in chilling critical commentary.").

258. *See* Emily Berman, *Regulating Domestic Intelligence Collection*, 71 WASH. & LEE L. REV. 3, 38–42 (2014).

259. HARRIS, *supra* note 6.

260. *See* LOUIS BRANDEIS, OTHER PEOPLE'S MONEY 92 (1914).

261. *See supra* note 17 and accompanying text.

262. *See, e.g.*, United States v. Muhtorov, 20 F.4th 558, 632 (2021) (rejecting the defendant's argument that he should have access to notice of the specific surveillance techniques used against him).

to weigh in, that has been the result of IG reports,[263] unlawful leaks of classified information,[264] or government disclosures prompted by those leaks.[265]

The *ex parte* nature of FISA applications is another aspect of surveillance law that inherently promotes underenforcement. Our judicial system is largely built on the premise that an adversarial system is more likely to reveal the truth. In the absence of adversarial testing, the government is much more likely to provide inaccurate, misleading, or incomplete information. This is particularly true in the case of material omissions, such as the ones in the Carter Page FISA application.[266] Imagine that Page had an attorney designated to argue that the court should *not* deem the government's evidence sufficient to establish probable cause that he was an agent of a foreign power. That attorney would have seen the assertion regarding Page's contacts with Russian officials and been able to provide the important additional context that Page had served as a source for the CIA.[267] Without someone tasked with the responsibility of revealing such omissions, they are much less likely to come to light. Even a rigorous *post hoc* auditing regime will struggle to prevent the government from submitting incomplete (as opposed to factually incorrect) applications to the FISC because it would require examination not only of each of the assertions made in the application to ensure they are supported but also of all other information in the government's possession related to the investigation to ensure no relevant information was omitted.

The same argument holds true for targeting and querying decisions. Assigning someone to argue that such decisions fail to satisfy the constitutional standards might be infeasible in the selection of all Section 702 targets or in determining whether there is reasonable articulable suspicion for each and every query. But recognizing that the absence of adversarial testing increases the likelihood of overcollection and improper queries (*i.e.*, underenforcement of Fourth Amendment requirements) spotlights the need to seek some means of averting that underenforcement.

The targeting rules designed to restrict targets of Section 702 surveillance to individuals reasonably believed to be located outside the U.S.—the so-called foreignness determinations—are another example. According to one news report, this reasonable belief was defined as 51% confidence that the target was a non-U.S. person outside the U.S.[268] And while the NSA has contested this

263. *See, e.g.*, DOJ IG CROSSFIRE HURRICANE REPORT, *supra* note 79, at 10.

264. *See, e.g.*, Andy Greenberg, *Intelligence Officials Admit That Edward Snowden's NSA Leaks Call for Reforms*, FORBES (Sept. 13, 2013, 3:37 PM), https://www.forbes.com/sites/andygreenberg/2013/09/13/intelligence-officials-admit-that-edward-snowdens-leaks-call-for-reforms/?sh=50abbc1cde6a [https://perma.cc/5LCW-GEKA].

265. *See* OFF. OF THE DIR. OF NAT'L INTEL., *IC on the Record: Declassified*, IC ON THE RECORD, https://icontherecord.tumblr.com/tagged/declassified (last visited Mar. 14, 2023) [https://perma.cc/W9AB-E4SE].

266. *See supra* notes 92–98 and accompanying text.

267. *See supra* notes 93–94 and accompanying text.

268. *See* Baron Gellman, *NSA Slides Explain the PRISM Data-Collection Program*, WASH. POST (July 10, 2013), https://www.washingtonpost.com/wp-srv/special/politics/prism-collection-documents/ [https://perma.cc/MT5G-PK2S].

characterization,[269] however the standard is articulated, violations are inevitable if that standard approved by the FISC sets the constitutional floor. It is unreasonable to think that the NSA will meet the standard in 100% of its targeting decisions. And, of course, the NSA has fallen far short of this mark.[270]

If these theoretical predictions of consistent underenforcement are not enough, consider that concerns about under protection also can stem from observed behavior. The *Miranda* Court, for example, partially justified its holding by noting that, despite the constitutional bar on involuntary statements in prosecution, state and local law enforcement officials continued to employ coercive interrogation methods and concluded that without some limitation upon the interrogation process, there could be "no assurance that practices of this nature [would] be eradicated in the foreseeable future."[271]

The track record of noncompliance laid out in Part II is analogous. Time and again, agencies seem incapable of following the rules. Whether this is the result of disregard for those rules or inadvertent errors, the impact on Americans' privacy is the same. In fact, in all but a handful of instances,[272] there is no intimation that the government seeks to intentionally evade the regulatory limits that Congress and the FISC have identified. Rather, despite the government's best efforts, and despite numerous additional procedures imposed in the wake of compliance problems,[273] violations continue to occur. A legal regime that defies the government's best efforts at compliance is guaranteed to underenforce the rights it is meant to protect.

2. Difficulty Determining Whether a Constitutional Violation Has Occurred

Overprotective doctrinal rules may also be appropriate when determining whether a particular constitutional provision has been violated is difficult to ascertain. Again, *Miranda* provides a concrete example. Innumerable factors might be relevant to the question of whether a custodial interrogation has, in fact, overborne a defendant's will.[274] This renders any effort to paint a picture that accurately captures the experience of any given detainee immensely difficult.[275] *Miranda* was thus the culmination of "more than thirty years of experience with the voluntariness test, a test that had been described as 'useless,' 'elusive,' and a

269. NATIONAL SECURITY AGENCY DIRECTOR OF CIVIL LIBERTIES AND PRIVACY OFFICE REPORT: NSA'S IMPLEMENTATION OF FOREIGN INTELLIGENCE SURVEILLANCE ACT SECTION 702 4 (2014).

270. *See supra* notes 155–64 and accompanying text.

271. Miranda v. Arizona, 384 U.S. 436, 447 (1966); *see also* Klein, *supra* note 19, at 1053 ("[S]tate police departments were . . . frequently engaging in excessively coercive interrogation techniques.") (citing *Miranda*, 384 U.S. 436 and earlier cases); Grano, *supra* note 19, at 108 (citing *Miranda's* reference to "third-degree" techniques being used on criminal suspects justifying imposing some limitation upon the interrogation process).

272. *See, e.g.*, *supra* notes 87–90 and accompanying text.

273. *See supra* Section II.B.

274. *See* Strauss, *supra* note 249, at 962 ("It is very difficult for a court, after the fact, imaginatively to recreate the conditions that existed in a custodial setting."); Caminker, *supra* 19, at 10 ("[I]t is quite difficult to imagine that a trial court could, through the normal factfinding process, determine the historical set of events surrounding a custodial interrogation with 100% accuracy.").

275. *See* Strauss, *supra* note 249, at 962; Caminker, *supra* note 19, at 10.

form of 'doubletalk'; a test which made everything relevant and nothing determinative."[276] The Court sought to elide these challenges by replacing case-by-case determinations of voluntariness with the application of a new, easy-to-administer rule.[277] Moreover, when detecting violations is difficult, the government faces more temptation to push the limits.[278]

Due to the secret nature of surveillance activities, nearly all the compliance incidents plaguing surveillance programs will be difficult to detect. Consider again the material omissions of fact that plagued the Carter Page FISA application. Factual inaccuracies might be detected through traditional oversight and good communication between investigating agents and DOJ lawyers preparing FISA applications. Determining what an application might be *missing*, however, is a much more complicated needle to thread. Kris suggests that the FISC should insist that the government performs more, and more comprehensive, accuracy reviews designed to identify errors of omission as well as errors of commission.[279] Such oversight will be time and resource intensive; however, requiring reviewers to look at all potentially relevant information in the FBI's possession, rather than just the information actually included in a FISA application. As a result, such an auditing system would cover a vanishingly small number of applications, leaving ample opportunity for violations to go undetected.

Then there are the technological challenges to detecting noncompliance. As Part II explained, there have been many instances in which violations resulted from misunderstanding the technological architecture of the system,[280] an absence of technical tools to limit collection to authorized material,[281] or the government's failure to realize that it was acting in violation of existing rules until significant time had passed.[282] And if the government is unaware of ongoing violations, external overseers such as Congress and the FISC certainly will be none the wiser. Moreover, even when the government discovered that its programs are exceeding their authority, there was often a lag—sometimes a lag of months or even years—between that discovery and informing the FISC.[283] Multiple FISA judges have expressed frustration with this tendency and the resulting delays in addressing violations.[284] These technical challenges thus present another argument to err on the side of overprotection.

There is an additional difficulty in detecting constitutional violations in the context of bulk collection regimes as well as Section 702 collection. The hallmark of these programs is that the rules are not "transactional"; they are

276. Grano, *supra* note 19, at 108–09 (citing *Miranda*, 384 U.S. at 468–69, 471–72 and numerous commentators).

277. *Id.* at 109.

278. *See* Landsberg, *supra* note 19, at 929–30 ("People tend to take advantage of ambiguity, the difficulty of detecting a violation of the law, or weakness of enforcement.").

279. *See* Judge Boasberg Mar. 4, 2020 opinion, *supra* note 92, at 15, 16.

280. *See supra* note 127 and accompanying text.

281. *See supra* notes 136–38 and accompanying text.

282. *See supra* notes 117–18 and accompanying text.

283. *Id.*

284. *See, e.g.*, *supra* note 88 and accompanying text.

"programmatic."[285] That is to say, the rules do not regulate single transactions, such as an individual targeting decision, but rather how the government decides which transactions to carry out and what to do with the information those transactions yield collectively.[286] The FISC's role here is to consider whether the entire program, under the totality of the circumstances, is consistent with the Fourth Amendment and other constitutional and statutory requirements.[287] Because the reasonableness of the program is assessed as one undifferentiated whole, the nature of any given rule will depend on the rest of the regime. If the statute narrowly constrains the type and amount of data the government may collect, for example, minimization and querying rules need not play as large a privacy-protection role. By contrast, when the scope of collection is broad, more protections are needed on the back end to ensure a sufficient overall level of privacy protection. In assessing reasonableness, the FISC must therefore consider not only the statutory provisions under which the collection is taking place, but also the targeting, minimization, and querying procedures that each agency has adopted.[288] It must then decide whether, taken together, this entire regime satisfies the Fourth Amendment.[289]

In making this determination, as the court repeatedly points out, it has to assess the procedures not as they are written, but as they are actually implemented.[290] And in making that assessment, the court is reliant on the government both to accurately describe how the program will operate and to comply with the established procedures.[291] The court cannot know how these procedures are implemented—and whether and to what extent they are complied with—until informed by the government. The FISC approves a set of procedures on the understanding that they will operate in a particular fashion. If that understanding is incorrect in any one respect, it might lead the FISC to approve a regime that is insufficiently protective overall. The MCT incident in Section 702 Upstream collection is an example. When the court learned that the collection was not as narrowly circumscribed as it had been led to believe, it determined that minimization procedures needed to be more robust to satisfy the Fourth Amendment's demands.[292] Of course, the court can have no idea that modifications to the minimization standards are needed if it does not have an accurate picture of how the rest of the program is operating.

285. *See* Daphna Renan, *The FISC's Stealth Administrative Law*, *in* GLOBAL INTELLIGENCE OVERSIGHT: GOVERNING SECURITY IN THE TWENTY-FIRST CENTURY 121, 130 (Zachary Goldman & Samuel J. Rascoff eds., 2016) ("The conventional Fourth Amendment test is transactional. It focuses on the one-off interaction, quintessentially at a particular moment in time.").

286. *Id.* at 131. ("The privacy implications of surveillance programs . . . are cumulative. And they are meaningfully determined not solely by acquisition, but also by use.").

287. *See supra* note 143 and accompanying text.

288. Mem. Op., [REDACTED], No. [REDACTED], GID.C.00282 8 (FISA Ct. 2019) (Boasberg, J.).

289. *Id.*

290. *See, e.g.*, Judge Boasberg Oct. 18, 2018, *supra* note 181, at 68.

291. *See supra* note 83 and accompanying text.

292. *See supra* notes 144–46 and accompanying text.

Shortcomings in the querying regimes are also going to be hard to detect. Recall the discussion above with respect to the nature and frequency of audits.[293] If there are entire offices whose queries are reviewed on a biannual basis, it means that years might go by with no indications of any problem. Even if reviews are more frequent, they will necessarily apply to a sampling of queries. The likelihood that any particular instance of improper querying will be detected is thus relatively small.

3. Providing Deterrence and Clear Guidance

Another commonly expressed justification for certain forms of doctrinal rules—those that take the form of simple, bright-line rules—is that they articulate clear parameters in order to both provide sufficient guidance for government officials and deter violations.[294] As one commentator put it, "the more fuzzy the line, the more tempting it will be for [government actors] to approach that line."[295] The continued pattern of recurring violations of surveillance rules speaks to a need for either clearer guidance or more deterrence. Apropos of clarity, the foreign intelligence surveillance activities of the United States are complex—both legally and technologically. It is this complexity that accounts for at least some of the government's failures to follow various rules over the years. Minimizing the complexity of the legal regime by adopting more straightforward rules would not only make the rules easier to comply with, but also could reduce the administrative burden imposed on intelligence agencies.

Some of the issues that have arisen also cry out for more deterrence. Violations that recur year after year or the agencies' repeated delays in reporting compliance issues seem amenable to rules that deter this repetition. To date, the FISC has been reluctant to impose consequences in all but the most egregious examples.[296] If known violations are going to go unpunished, it is all the more important to deploy mechanisms to deter those violations from taking place at all.

IV. REMEDYING UNDERENFORCEMENT OF SURVEILLANCE RULES

This Part seeks to reimagine surveillance rules through the lens of their tendency towards underenforcement and to advocate for the adoption of several specific measures designed to combat this tendency. Section IV.A will briefly provide a menu of available techniques for implementing such reforms, and Section IV.B will present the proposals themselves.

293. *See supra* notes 218–20 and accompanying text.

294. Strauss, *supra* note 249, at 962 (arguing that "case-by-case determinations . . . give law enforcement authorities who want to do the right thing too little guidance about how they should proceed").

295. *See* Caminker, *supra* note 19, at 18.

296. *See supra* Section II.B.

A. A Brief Typology of Rules Preventing Underenforcement

When justified, rules intentionally crafted to avoid underenforcement tend to take one of three forms, each of which can play a role in meaningful surveillance reform.

Categorical Rules. Categorical rules provide the clearest possible guidance to government actors tasked with implementing constitutional doctrine, eliminating the complications that come from rules that rely on difficult factual inquiries and analysis. In short, they substitute the complexity involved in weighing multiple factors and uncertain facts with an easy-to-answer bright line. Criminal procedure is replete with examples of such rules.[297] By now it should be clear that *Miranda* is one such rule: in determining whether a prosecutor may use a suspect's statement as evidence in their case-in-chief, the question is simply whether the defendant was Mirandized before giving his statement.[298] There is no need to engage in the multifactor, case-by-case inquiry necessary to assess the voluntariness of a statement.[299]

Similarly, criminal defendants have a Sixth Amendment right to counsel at lineups that take place after "initiation of adversarial judicial proceedings," such as an indictment.[300] The rule is designed to ensure that lineups are not conducted in ways that prejudice the defendant.[301] The relevant question for courts is not whether the lineup was prejudicial—an inquiry requiring application of an amorphous legal standard to innumerable details regarding how a particular lineup was conducted (*e.g.*, where it took place, how similar to the defendant the other potential suspects presented at the lineup looked, what officials conducting the lineup said or did that may have influenced the witness, etc.).[302] Instead, courts must simply determine whether the defendant's counsel was present, thus eliminating the complexities of a multifactor inquiry.[303]

Presumptions and burden-shifting frameworks. Presumptions and burden-shifting frameworks provide the same benefits as categorical rules: they simplify complicated or difficult evidentiary inquiries. They are not as conclusive as *per se* rules, as the parties may seek to rebut a presumption or meet a heightened

297. *See* Klein, *supra* note 19, at 1037–51.

298. Miranda v. Arizona, 384 U.S. 436, 478–79 (1966).

299. Whether a statement is, in fact, involuntary remains a relevant inquiry for other purposes. *See, e.g.*, Caminker, *supra* note 19, at 4–5 ("[S]tatements that were considered 'freely given' as measured by the case-specific-voluntariness-test yet obtained in violation of *Miranda* . . . could be used for various purposes other than evidence in the prosecution's case-in-chief.").

300. Moore v. Illinois, 434 U.S. 220, 231 (1977).

301. United States v. Wade, 388 U.S. 218, 236–37 (1967) ("[T]here is grave potential for prejudice, intentional or not, in the pretrial lineup, which may not be capable of reconstruction at trial, and . . . presence of counsel itself can often avert prejudice.").

302. Another categorical rule applies when a defendant can show that her attorney's representation of multiple clients created a conflict of interest. If a defendant makes such a showing, she need not also demonstrate that the conflict of interest actually prejudiced her defense. Cuyler v. Sullivan, 446 U.S. 335, 350 (1980). Yet another applies to inventory searches of vehicles, which the Supreme Court has held qualify for an exception to the Fourth Amendment's warrant requirement so long as the police employ "standardized criteria or established routine." Colorado v. Bertine, 479 U.S. 367, 375 (1987); Florida v. Wells, 495 U.S. 1, 4 (1990).

303. *See Wade*, 388 U.S. at 241–42.

burden of proof. By placing a thumb on one side of the scale, however, they streamline the inquiry. First Amendment doctrine provides a useful example. Under the First Amendment, regulations of speech on the basis of its content are presumed unconstitutional unless they fall within a few narrow exceptions.[304] This presumption provides the strong free speech protection necessary to prevent chilling the expression of groups or individuals with disfavored or dissenting views.[305] It nevertheless allows regulation if the government can present a sufficiently compelling interest.[306]

Justice Brennan described the rational basis standard of review used to analyze many equal protection challenges as a presumption justified by the difficulty in assessing the basis for legislative decisions. Legislative enactments, Justice Brennan points out, are "cloaked by the presumption that the legislature has, as it should, acted within constitutional limitations."[307] He goes on to explain that this presumption relieves courts from having to reach conclusions on "complex factual questions of the kind so often involved in constitutional adjudication."[308] Instead, legislators' factual conclusions will be overturned only if their findings are so clearly wrong that they "may be characterized as 'arbitrary,' 'irrational,' or 'unreasonable.'"[309] The same is true for strict scrutiny, but in the other direction—there, the courts adopt a presumption of *un*constitutionality that the government can overcome by demonstrating that it has employed a narrowly tailored means of achieving a compelling interest.[310]

Enhanced procedural protections. Enhanced procedural protections are one tool to reduce underenforcement already frequently employed in the surveillance context. The FISC has consistently used this technique to ensure that the government satisfies Fourth Amendment requirements.[311] Reason-giving requirements are one example.[312] Take the FISC's order that FBI queries of U.S.-person identifiers when accessing Section 702 data must be preceded by a written

304. *See, e.g.*, R.A.V. v. City of St. Paul, 505 U.S. 377, 382 (1992) ("Content-based regulations are presumptively invalid."); Brandenburg v. Ohio, 395 U.S. 444, 447 (1969); Chaplinsky v. New Hampshire 315 U.S. 568, 573 (1942); Strauss, *supra* note 249, at 963.

305. *See supra* notes 257–96 and accompanying text.

306. *See, e.g.*, Holder v. Humanitarian L. Project, 561 U.S. 1, 40 (2010) (holding that the provision of advice and training to a foreign terrorist organization qualifies as material support for terrorism—even if that advice and training is for purely lawful purposes).

307. Oregon v. Mitchell, 400 U.S. 112, 247 (1970) (Brennan, J. dissenting).

308. *Id.* at 247–48.

309. *Id.* at 248.

310. *See* Grutter v. Bollinger, 539 U.S. 306, 326 (2003) (explaining the strict scrutiny standard).

311. The Due Process Clauses, of course, impose their own rules on the mechanisms by which government acts. The enhanced procedures I discuss here are those not dictated by the Fifth or Fourteenth Amendments but rather employed to heighten protections for other constitutional values.

312. *See, e.g.*, North Carolina v. Pearce, 395 U.S. 711, 725 (1969) (holding that "[w]henever a judge imposes a more severe sentence upon a defendant [after the defendant succeeded in getting new trial,] the reasons for him doing so must affirmatively appear" to ensure that "vindictiveness against a defendant for having successfully attacked his first conviction" did not motivate the sentence he receives after a new trial); *see also* Grano, *supra* note 19, at 112 ("[A] sentence may violate the *Pearce* rules without necessarily violating the Constitution."). The Court subsequently limited the *Pearce* presumption to circumstances "in which there is a 'reasonable likelihood,' that the increase in sentence is the product of actual vindictiveness." Alabama v. Smith, 490 U.S. 794, 799 (1989).

justification for the query.[313] This requirement augmented previous querying procedures, making it more difficult to act contrary to the substantive rules.

Note that even where more protective measures are called for, decision-makers—whether Congress or the FISC—will frequently have to choose among a wide range of possible rules. They might have to select between different types of rules—that is, whether to employ a categorical rule, a presumption, or enhanced procedures. At other times they might have to choose among several categorical rules. Determining which rule will result in better constitutional compliance without imposing unacceptable costs will require a context-specific analysis that weighs competing interests.[314]

B. Proposed Reforms

This Section will revisit the compliance concerns detailed in Part II and offer some reforms inspired by the concept of systemic underenforcement laid out in Part III. The items on this list are likely neither necessary nor sufficient; these are not the only measures that could achieve the aims of these particular reforms, nor would adopting all of them guarantee 100% compliance. Indeed, when it comes to operationalizing constitutional rules, there are no "right" and "wrong" measures.[315] Instead, there is a range of options, each of which will effectively protect constitutional rights to a greater or lesser degree, from which courts and policy-makers must choose. Nevertheless, the suggestions that follow would address some of the most problematic and persistent compliance challenges detailed above.

1. Global Reforms

There are some intelligence-community-wide or agency-wide measures that would combat underenforcement across surveillance programs. Most of these take the form of enhanced procedural protections. When it comes to the FBI, for example, both the Justice Department's Inspector General and David Kris, former head of the National Security Division and sometime FISC amicus, have argued that problems with compliance stem not only from failures by individual government officials but also from failures of leadership and institutional

313. *See supra* note 231 and accompanying text.

314. Such interests will include the government's interest in the intelligence at issue, the likelihood of false positives and the costs of false negatives, administrative costs, the potential for unintended consequences, and the institutional competencies of the decision-maker. *See, e.g.*, Caminker, *supra* note 19, at 13; Landsberg, *supra* note 19, at 926 ("[A] court should base the content of the rule on a balancing that takes into account not only necessity, but also federalism, the separation of powers, and three predictive difficulties: predicting the need for the rule, its efficacy, and its unintended consequences."); Strauss, *supra* note 19, at 193 ("Will the presumption bring about savings in the resources spent—by courts, parties, witnesses, and law enforcement agencies—in administering the criminal justice system?"); Monaghan, *supra* note 19, at 26 ("The Court might . . . proceed on a frankly experimental basis in the hope of achieving the 'best' implementing rule on a cost-benefit analysis."); Caminker, *supra* note 19, at 25 ("[W]e aim for a constitutionally tolerable" amount of error, "taking into account the government interests on the other side.").

315. *See* Michael C. Dorf & Barry Friedman, *Shared Constitutional Interpretation*, 2000 SUP. CT. REV. 61, 67 (2000); Klein, *supra* note 19, at 1060.

culture.[316] Kris, therefore, argues that senior leadership must foster cultural reform in order to build a culture of scrupulous accuracy.[317] While the IG and Kris's discussion of cultural reform focuses on the FBI in the context of ensuring complete and accurate FISA applications,[318] establishing or enhancing a culture of meticulous compliance would benefit all surveillance programs.

One means of showing this leadership is to clearly articulate expectations and to hold government officials accountable for meeting those expectations. In other words, in addition to adopting the right rules, agency leadership can demonstrate the importance of actually following those rules. To send this message, compliance should form part of intelligence-community officials' performance evaluations. Supervisors should track which officials perform unlawful searches, are careless or delinquent in conducting foreignness assessments, or fail to document appropriately factual assertions in submissions to the FISC. These failures should then factor into career advancement decisions, such as raises and promotions. Imposition of consequences affecting career advancement would convey the seriousness with which the executive branch takes its compliance responsibilities and incentivize conscientiousness on the part of investigators and analysts. Conversely, agents who are particularly diligent when it comes to compliance should be rewarded for that behavior.

Another general hedge against underenforcement is to mandate one or more sources of external oversight, which currently comes only from executive branch officials and the FISC.[319] The Privacy and Civil Liberties Oversight Board ("PCLOB") is a promising entity to enlist in this effort. The PCLOB has proved adept at evaluating the civil liberties implications of the legal and policy issues surrounding surveillance rules.[320] To date, their involvement has been subject to two limits, each of which should be relaxed. First, their statutory mandate is limited to assessing the civil liberties implications of counterterrorism policies.[321] This narrow focus on counterterrorism is a relic of the immediate post-9/11 era, where international terrorism concerns dominated security policy. Two decades later, policymakers recognize that, while international terrorism is by no means a thing of the past, neither is it necessarily the most severe threat facing the

316. Peter Margulies, *Searching for Accountability Under FISA: Internal Separation of Powers and Surveillance Law*, 104 MARQ. L. REV. 1155, 1193 (2021).

317. *See* Letter Brief of Amicus Curiae David Kris, Judge Boasberg Mar. 4, 2020 opinion, *supra* note 92 (pointing to the FBI Director and the Attorney General in particular).

318. *See id.*

319. *See Who Monitors or Oversees the FBI*, FBI, https://www.fbi.gov/about/faqs/who-monitors-or-oversees-the-fbi (last visited Mar. 14, 2023) [https://perma.cc/43K2-NGFA]; Foreign Intelligence Surveillance Court, ELEC. PRIV. INFO. CTR., https://epic.org/foreign-intelligence-surveillance-court-fisc/ (last visited Mar. 14, 2023) [https://perma.cc/CLJ5-95YS].

320. *See, e.g.*, PCLOB SECTION 215 REPORT, *supra* note 36, at 2; PCLOB SECTION 702 REPORT, *supra* note 62, at 5.

321. 42 U.S.C. § 2000ee.

country.[322] Congress should expand the PCLOB's remit to cover the full range of national security policy.

The second way in which the PCLOB's activities have been limited is that the PCLOB has engaged in one-off deep dives into particular programs. These deep dives have proven incredibly valuable,[323] but the PCLOB should also engage in audits or reviews of surveillance programs at regular intervals. As the FISC has recognized, the Fourth Amendment analysis of surveillance law must consider government programs as they are implemented, not as they are conceived of on paper.[324] As we have seen, violations can be difficult to detect, and the FISC cannot always rely on the government to identify constitutional concerns in a timely fashion. If the PCLOB were to examine closely government surveillance programs on an annual or biannual basis, it might catch compliance issues that escape the notice of the government and the FISC.

Periodic evaluation of these programs is particularly important given the nature of Fourth Amendment analysis, which requires surveillance programs to be "reasonable," taking account of the totality of the circumstances. Over time, circumstances can change. Imagine, for example, that a technological advancement allowed the government to identify, with certainty, the location of any given surveillance target at any given time. If such technology existed, it might no longer be reasonable to use the current methods of assessing the foreignness of Section 702 targets. Similarly, if the NSA developed a means of collecting only those communications to, from, or about a particular target during its Upstream collection—as opposed to collecting all the communications within a multicommunication transaction[325]—it might be reasonable to reinstate "about" collection in the Upstream context. In other words, an outside entity familiar with both the law and the technology involved could take a fresh look periodically to identify whether the Fourth Amendment balance had changed and recommend corresponding changes to the rules.

Technology itself might also play a role in preventing underenforcement. Artificial intelligence and machine-learning tools pervade decision-making in both the public and private sectors. Government agencies should explore the possibility of turning this form of evaluation on itself in order to identify and prevent compliance risks. If algorithms can detect likely Medicaid fraud[326] or determine which advertisements should be targeted to particular consumers,[327] perhaps they

322. *See* Eileen Sullivan & Katie Benner, *Top Law Enforcement Officials Say the Biggest Domestic Terror Threat Comes from White Supremacists*, N.Y. TIMES (May 12, 2021), https://www.nytimes.com/2021/05/12/us/politics/domestic-terror-white-supremacists.html [https://perma.cc/2J6V-UKTN].

323. *See* PCLOB SECTION 215 REPORT, *supra* note 36, at 167; PCLOB SECTION 702 REPORT, *supra* note 62, at 149.

324. *See, e.g.*, October 2011 Bates Opinion and Order, at 80.

325. PCLOB SECTION 702 REPORT, *supra* note 62, at 41.

326. Cade Metz & Adam Satariano, *An Algorithm That Grants Freedom, or Takes It Away*, N.Y. TIMES (Feb 7, 2020), https://www.nytimes.com/2020/02/06/technology/predictive-algorithms-crime.html [https://perma.cc/QD74-TYC4].

327. *See* Spandana Singh, *The Algorithms Behind Digital Advertising*, NEW AM. (Feb. 19, 2020), https://www.newamerica.org/oti/blog/algorithms-behind-digital-advertising/ [https://perma.cc/234G-TZMP].

could learn to flag problematic FISC applications or unlawful queries. Imagine training an algorithm on a dataset composed of FISC applications identified as "excellent" (*i.e.*, applications that were complete and contained sufficient probable cause) or "flawed" *(i.e.*, missing information or containing internal contradictions). Or a dataset identifying queries that met the reasonable articulable suspicion standard and those that did not. Such analytic tools could potentially identify problematic FISC applications or agents who systematically performed unjustified queries. Creating this kind of tool is concededly complex, and it might be more easily employed to prevent some errors than others. But given the complex analyses already entrusted to algorithmic decision-making in many contexts, the tool holds promise for improving surveillance compliance as well.

A final government-wide reform to reduce underenforcement is an increase in transparency. In particular, the presumption that FISC opinions will remain secret should be reversed.[328] In all other Article III courts, litigants' filings and courts' rulings are presumed to be publicly available absent compelling justification to the contrary.[329] FISC opinions should be no different. To be sure, publicly available versions of these documents may require more redactions than the average judicial opinion. But it is only through leaked or declassified opinions that the public has learned of compliance problems.[330] They are therefore a valuable source in any effort to impose democratic oversight on otherwise-secret surveillance activities.

These suggestions could address noncompliance across the broad range of surveillance programs and techniques. There are also specific types of compliance problems that merit specific attention and tailored reforms. The balance of this Section turns to those issues.

2. Addressing Inaccurate, Incomplete, or Misleading Submissions to the FISA Court

The FBI and the Justice Department already have taken significant steps to address the flaws in traditional FISA applications discovered as a result of the investigation into the Carter Page surveillance. These include reforms to pro-

328. Litigation seeking to reverse the presumption and arguing that "secrecy [surrounding the surveillance court] has allowed the government's surveillance policies to become unmoored from the democratic consent essential to their legitimacy." Cole et al., *supra* note 17; *see also In re* Ops. & Ords. by the FISC Addressing Bulk Collection of Data under the Foreign Intel. Surveillance Act, 957 F.3d 1344, 1344 (FISA Ct. Rev. 2020) (per curiam) (rejecting argument that First Amendment requires public access to certain FISC opinions); *In re* Ops. and Ords. of This Ct. Containing Novel or Significant Interpretations of L., No. Misc. 16-01, 2020 WL 5637419, at *1 (FISA Ct. 2020), *aff'd.*, No. Misc. 20-02, 2020 WL 6888073 (FISA Ct. Rev. 2020) (mem.) (same).

329. *See* Richmond Newspapers, Inc. v. Virginia, 448 U.S. 555, 573 (constitutional right of access); Nixon v. Warner Commc'ns, Inc., 435 U.S. 589, 597 (1978) (common-law right of access).

330. *See* Adam Liptak, *At the Supreme Court, a Plea to Reveal Secret Surveillance Rulings*, N.Y. TIMES, https://www.nytimes.com/2021/09/20/us/supreme-court-fisa-surveillance-rulings.html (Oct. 3, 2021) [https://perma.cc/T5K2-PXTV].

cedures and training protocols, which are surely needed.[331] Recall, however, that the Woods Procedures violated in the Carter Page investigation were themselves a response to an earlier spate of inaccurate FISA applications,[332] yet they failed to prevent a recurrence of the problem.[333] This implies that lasting reform might need to go beyond such measures.

There are several ways to address the concern that Americans' constitutional rights are prone to underenforcement in the traditional FISA regime. First, we could impose a categorical rule barring FISA surveillance of U.S. persons. The statute already treats U.S. persons and non-U.S. persons differently.[334] Establishing probable cause that a target is an "[a]gent of a foreign power"—and therefore a valid target of a traditional FISA order—is more difficult when the target is a U.S. person.[335] Relatedly, the so-called "lone wolf" provision, which was in effect from 2004–2020 and permitted FISA surveillance of individuals suspected of engaging in international terrorism even if they were not working on behalf of a foreign power, was always limited to non-U.S. persons.[336] Simply excluding U.S. persons from the universe of permissible targets would effectively eliminate underenforcement in that context. While easily administrable and effective, a bar on traditional FISA surveillance of U.S. persons might prove too costly in the sense of lost intelligence information—a question only those within the intelligence community could answer.[337] Perhaps more importantly, it is likely a political nonstarter.

A less drastic version of this approach would be to reserve the targeting of U.S. persons under traditional FISA to investigations that are deemed particularly significant. Already the FBI subjects some investigations—those raising the possibility of "public notoriety and sensitivity," such as investigations of political figures, religious organizations, members of the media, or academia—to different rules than others by designating them "sensitive investigative matters."[338] These investigations must be brought to the attention of FBI management and DOJ officials before moving forward, and they are subject to special approval

331. DEP'T OF JUST., THE DEPARTMENT OF JUSTICE AND THE FEDERAL BUREAU OF INVESTIGATION ANNOUNCE CRITICAL REFORMS TO ENHANCE COMPLIANCE, OVERSIGHT, AND ACCOUNTABILITY AT THE FBI (Sept. 1, 2020).

332. *See supra* notes 102–05 and accompanying text.

333. DEP'T OF JUST., 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. 1, 2020).

334. *See* 50 U.S.C. § 1801(b)(1)-(2).

335. *Compare* 50 U.S.C. § 1801(b)(1), *with* § 1801(b)(2).

336. 50 U.S.C. § 1801(b)(1)(C); *see* Michael J. Orlando, *Reauthorizing the USA Freedom Act of 2015*, FBI (Nov. 6, 2019), https://www.fbi.gov/news/testimony/reauthorizing-the-usa-freedom-act-of-2015-110619 [https://perma.cc/S2WN-CMDM].

337. About 12–15% of FISA surveillance orders that require a showing of probable cause target U.S. citizens annually. *See* OFF. OF THE DIR. OF NAT'L INTEL. ANNUAL STATISTICAL TRANSPARENCY REPORT REGARDING THE INTELLIGENCE COMMUNITY'S USE OF NATIONAL SECURITY SURVEILLANCE AUTHORITIES, CALENDAR YEAR 2020 11 fig.2a (2021). It is impossible to know how many of those targets could have been targeted using a Title III wiretap.

338. FBI, DOMESTIC INVESTIGATIONS & OPERATIONS GUIDE, § 10.1.1 (2016).

and reporting requirements.[339] The FBI could identify a subset of investigations to which targeting U.S. persons using traditional FISA would be limited. The relevant subset could be defined in many ways—it could be limited to investigations into threats to U.S. national security, for example, or to investigations involving the threat of violence. This is simply another categorical rule to limit the most intrusive form of investigation to instances in which that intrusion is justified.

We could achieve a similar goal through a burden-shifting or presumption approach. If we worry that current rules make it too likely that the government will employ traditional FISA to engage in unjustified surveillance of U.S. persons, we could make FISA orders more difficult to acquire. The standard that the government must meet in cases involving U.S.-person targets could be ratcheted up. Under traditional FISA, the government must demonstrate probable cause that the target is an agent of a foreign power.[340] As noted above, this definition already is harder to satisfy with respect to U.S. persons than it is with respect to non-U.S. persons.[341] Further narrowing that definition, or adopting a presumption that U.S. persons are not agents of a foreign power, would thus not significantly disrupt the existing regime. This would not place U.S.-person targets off limits, but it would require the government to make a stronger showing to the FISC in order to overcome the presumption. To the extent that the problem with the Carter Page application was that the government's probable cause showing was relatively weak,[342] demanding stronger evidence before issuing an order could address the concern.

The concern about difficult-to-detect errors of omission in FISA applications is less amenable to categorical rules or burden-shifting. To paraphrase Donald Rumsfeld, the FISC doesn't know what it doesn't know.[343] If the FBI has information in its files that fails to make it into a FISC application, no level of judicial scrutiny of that application is going to uncover the omission. As the FBI has implicitly acknowledged through the measures it already has taken, this concern is best addressed through enhanced procedural protections.[344] The additional procedures already adopted, however, do not go far enough. Training for

339. *Id.* § 10.1.

340. 50 U.S.C. § 1805(a)(2).

341. *See supra* text accompanying notes 334–37.

342. Order Regarding Handling and Disposition of Information, *In re* Carter W. Page, A U.S. Person, Nos. 16-1182, 17-52, 17-375, 17-679 (FISA Ct. Jan. 7, 2020); *see also Justice Dept. Admitted It Lacked Probable Cause in Carter Page FISAs*, CHUCK GRASSLEY (Jan. 23, 2020), https://www.grassley.senate.gov/news/news-releases/justice-dept-admitted-it-lacked-probable-cause-carter-page-fisas [https://perma.cc/V66H-TLUW].

343. *See* Sec'y Donald Rumsfeld & Gen. Richard Myers, *Defense Department Briefing*, C-SPAN, at 37:45 (Feb. 12, 2002), https://www.c-span.org/video/?168646-1/defense-department-briefing%20(8 [https://perma.cc/9XVC-Y6WK] (distinguishing between "known unknowns," when we are aware there are some things we do not know, and "unknown unknowns"—the ones we don't know we don't know).

344. *See* FBI, DOMESTIC INVESTIGATION AND OPERATIONS GUIDE § 10 (2016) (describing how the FBI requires special approvals for investigations involving public notoriety or sensitivity); U.S. DEP'T JUST., 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 7 (2021), https://oig.justice.gov/sites/default/files/reports/21-129.pdf [https://perma.cc/5ZA9-G4HN].

agents and additional documentation requirements simply raise the administrative costs of the program without effectively ensuring against errors of omission. After all, the Woods Procedures themselves were designed to address a similar problem but failed to do so effectively in the long term.[345]

This is one area in which cultivating an agency culture of accuracy and imposing career consequences on agents who fail to follow all the rules hold promise. But there is another means of tackling this problem that does not bury the investigating agents in additional paperwork: more extensive use of amici curiae in FISA proceedings. Currently, the law provides that the FISC should appoint amici to argue against the government's position when a case "presents a novel or significant interpretation of the law" (unless the court finds that appointment inappropriate).[346] Congress or the FISC itself could expand the universe of cases involving an amicus to include all instances in which the target is a U.S. person.[347] Tasking one of the precleared, expert amici available to the FISC with representing the proposed target's interests, and providing that amicus with access to all of the relevant material, could help confront the difficulty in detecting errors of omission. Consider, for example, what would have happened had an amicus been given access to the FBI's materials on Carter Page. She could have raised the question of his former relationship with the CIA or pointed out when assertions in the application were inconsistent with the statements of a confidential informant. In other words, rather than relying on the FBI to self-police, we should employ the adversarial process—the process already used in the lion's share of American judicial proceedings—to ensure all that the full picture is presented to the FISC.[348]

3. Addressing Overcollection

On numerous occasions, sometimes for periods lasting years, the NSA has collected data beyond the limits of what was authorized.[349] Sometimes these incidents were due to technical constraints imposed by the various collection and storage systems the NSA employs. Upstream Section 702 collection, for example, amassed millions of purely domestic communications because the NSA could not screen these out from MCTs containing communications to, from, or

345. *See* Jack Marshall, *The Woods Procedures*, ETHICS ALARMS (Feb. 7, 2018), https://ethicsalarms.com/2018/02/07/the-woods-procedures/ [https://perma.cc/Z8BB-26C8]; U.S. DEP'T JUST., AUDIT, *supra* note 344, at i, 17; Press Release, Dep't of Just. Off. of the Inspector Gen., DOJ OIG Releases Audit Report on the FBI's Execution of its Woods Procedures for Applications Filed with the Foreign Intelligence Surveillance Court Relating to U.S. Persons (Sept. 30, 2021).

346. 50 U.S.C. § 1803(i)(2)(A).

347. Professor Laura Donohue supports a recent legislative proposal to require amicus in all cases raising significant First Amendment concerns. *See* Donohue, *supra* note 24, at 244; Patrick J. Leahy & Mike Lee, *FISA Needs Reform. Our Amendment Would Do That—and Protect Constitutional Rights*, WASH. POST (May 10, 2020, 8:00 AM), https://www.washingtonpost.com/opinions/2020/05/10/fisa-needs-reform-our-amendment-would-do-that-protect-constitutional-rights/ [https://perma.cc/TT5Z-2WUD].

348. *See generally* Chin, *supra* note 81, at 664, 711.

349. *See supra* Subsection II.B.2.

about a target.[350] Bulk internet data collection captured categories of data not intentionally targeted by NSA systems.[351] And more recently, the FISC has expressed concerns regarding the government's ability to accurately determine whether a particular Section 702 target is a non-U.S. person outside the United States—the so-called "foreignness" determination.[352]

As an initial matter, there are two categorical rules that should be triggered by any incident of overcollection. First, the immediate consequence should be the required deletion of all data whose collection was not authorized. For the most part, the FISA court and the government have followed this rule, but the government has not always done so promptly or completely.[353]

Second, when the overcollection is systemic or due to a technological hurdle, rather than the result of individual misconduct, all collection should be halted until the agency comes into compliance. Regardless of the scope or severity of the overcollection it discovered, at no point has the FISC ordered the government to suspend its collection operations until it could proceed in compliance with the rules.[354] Instead, the programs have been allowed to continue while the government and the FISC together generated a remedial plan and initiated its implementation.[355] Indeed, it was the government itself, not the FISC or Congress, that made the decision to discontinue "abouts" collection because it could not be accomplished within the confines of the Fourth Amendment.[356] The possibility of adverse consequences for noncompliance can only increase the government's incentives to avoid compliance incidents. This is not to say that agencies or their employees should be disciplined for occasional inadvertent missteps. But when systemic, unauthorized collection is discovered, it should not be permitted to continue.

Overcollection problems stemming from inaccurate foreignness assessments should be addressed by imposing a higher standard of proof. The challenge of the "reasonably believed to be outside the United States" standard is that it is, of course, difficult to pinpoint the location of a given individual at a given moment. Any standard based on the idea that foreignness assessments can be made with a high level of accuracy will systemically err on the side of underenforcement. If Section 702 is reasonable, according to the FISC, because it assumes the government can make location assessments accurately, then if that is not the case (*i.e.*, location assessments are frequently inaccurate) the standard that the FISC

350. *See supra* notes 136–138 and accompanying text.

351. *See supra* notes 141–143 and accompanying text.

352. Judge Collyer Apr. 26, 2017 Opinion, *supra* note 69, at 73–75.

353. *Id.* at 72, 94–95.

354. *See, e.g.*, *supra* notes 143–46, 151 and accompanying text; Judge Boasberg Oct. 18, 2018, *supra* note 181, at 64.

355. *See, e.g.*, *supra* notes 143–46, 151 and accompanying text; Judge Boasberg Oct. 18, 2018, *supra* note 181, at 64.

356. *See, e.g.*, *supra* notes 143–46, 151 and accompanying text. Congress or the FISA court should codify the ban on "abouts" collection, which currently may be reinstated if the government provides Congress thirty days' notice. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, § 103(b)(2), 132 Stat. 3 (2018).

determined was reasonable actually is not what is being implemented in practice. Evidence indicates that this has sometimes been the case.[357] Setting a higher threshold for determinations that any given target is, in fact, eligible for Section 702 surveillance would reduce overcollection stemming from erroneous foreignness determinations. In other words, Congress or the FISC could overprotect against erroneous foreignness determinations by replacing the "reasonably believed to be outside the United States" standard with "clear and convincing evidence that the target is outside the United States," or some similar, relatively demanding, standard.[358]

4. Addressing Querying Violations

Perhaps the most troubling breaches of surveillance rules include the FBI's and NSA's improper queries of Section 702 data using U.S.-person identifiers. Recall that such queries access databases containing massive numbers of communications of U.S. persons who were in contact with overseas targets.[359] So when a government official runs improper queries in the Section 702 database, she is searching through the contents of vast amounts of U.S. persons' communications that were collected without judicial oversight or a showing of probable cause.

All the surveillance programs have suffered from impermissible U.S.-person queries—both bulk collection programs prior to their termination;[360] NSA Upstream data, where they were categorically impermissible until "abouts" collection was suspended;[361] NSA PRISM data;[362] and FBI queries of Section 702-acquired data.[363] Compliance with querying standards is one of those areas where violations will be difficult to detect. We are reliant on the government to self-police and self-report. Despite this challenge, there is ample evidence that querying rules have been repeatedly underenforced.[364] What follows are a series of proposals to reverse this underenforcement.

There are at least two categorical rules that should be relatively noncontroversial. First, as with overcollection, whenever systemic violations of the rules regarding U.S.-person queries are discovered—violations, for example, stemming from improper settings or default rules placed on particular querying tools—those queries should be suspended entirely until the problem is resolved. Second, to the extent it has not already done so, the FISC should explicitly bar "batch" queries. The FISC found that such queries were inconsistent with

357. *See supra* notes 154–69 and accompanying text.

358. None of these suggestions ask the more fundamental question of whether—given modern methods of communications, the nonterritoriality of data, and the ease of global travel—surveillance targeting laws should be based on location. Rethinking the use of location, which currently plays a role in target eligibility across multiple investigative methods, is beyond the scope of this Article.

359. *See supra* notes 71–77 and accompanying text.

360. *See supra* notes 122–29 and accompanying text; discussion *supra* Subsection II.B.3.a.i.

361. *See supra* notes 151–53 and accompanying text; *supra* notes 186–92 and accompanying text.

362. *See supra* notes 193–96 and accompanying text.

363. *See supra* notes 199–203 and accompanying text.

364. *See, e.g.*, *supra* text accompanying note 231.

querying rules,[365] but that does not seem to have stopped the FBI from using them.[366] If the FBI fails to comply with the FISC's interpretation of the querying rules, the FISC should suspend the agency's authority to conduct queries, particularly U.S.-person queries, until it can credibly demonstrate its willingness and ability to follow the rules.

With regard to the querying rules themselves, there are multiple potential categorical rules that would mitigate the repeated querying violations that we have seen. In a perfect world, we would simply bar querying Section 702-acquired data with U.S.-person identifiers, full stop.[367] Numerous commentators as well as President Obama's expert commission on surveillance reform have endorsed this idea.[368] The logic behind this recommendation is simple. The Fourth Amendment normally requires the government to demonstrate probable cause and secure an individualized court order to collect the communications of Americans.[369] The communications in the Section 702 databases were collected without such protections, due simply to the fact that an American was in contact with a valid target overseas.[370] Allowing the government to access U.S.-person communications swept up through this "incidental" collection, therefore, creates an end-run around the Fourth Amendment, providing to the government indirectly the contents of Americans' communications it would not have had the authority to collect directly. For this reason, Section 702 queries using U.S.-person identifiers are often referred to as "back door" searches.[371]

Even if there is no appetite for foreclosing U.S.-person queries altogether, the FBI's use of those queries should be constrained in two ways. First, a categorical rule should limit the FBI's queries to the same rules that all the other agencies with access to Section 702-acquired data follow. The NSA, CIA, and NCTC's querying rules permit queries only when they are likely to return foreign intelligence information,[372] whereas the FBI's rules allow queries for evidence of crime as well.[373] The communications' collection was justified based on the information presumed foreign intelligence value.[374] The government's use of those communications should thus be limited to foreign intelligence purposes. Allowing Section 702 U.S.-person queries to seek information regarding

365. *See supra* notes 229, 234–35 and accompanying text.

366. Judge Boasberg Oct. 18, 2018, *supra* note 181, at 64–65.

367. This recommendation emerged from a panel that President Barack Obama appointed in 2013 to review the government's foreign intelligence programs in the wake of Edward Snowden's disclosures. *See* Geoffrey Stone & Michael Morell, *The One Change We Need to Surveillance Law*, WASH. POST (Oct. 9, 2017), https://www.washingtonpost.com/opinions/the-one-change-we-need-to-surveillance-law/2017/10/09/53a40df0-a9ea-11e7-850e-2bdd1236be5d_story.html [https://perma.cc/9FQV-LLJC]; Peter Swire & Richard Clarke, *Reform Section 702 to Maintain Fourth Amendment Principles*, LAWFARE (Oct. 19, 2017, 2:02 PM), https://www.lawfareblog.com/reform-section-702-maintain-fourth-amendment-principles [https://perma.cc/Y3RS-Q8EW].

368. *See* Stone & Morell, *supra* note 367; Swire & Clarke, *supra* note 367; sources cited *supra* note 203.

369. *See* Dalia v. United States, 441 U.S. 238, 255 (1979).

370. *See supra* note 27 and accompanying text; *supra* notes 71–74 and accompanying text; *supra* notes 141–43 and accompanying text.

371. *See* Swire & Clarke, *supra* note 367.

372. *See supra* note 183 and accompanying text; Table 2.

373. *See supra* notes 199–200 and accompanying text.

374. *See supra* notes 57–59 and accompanying text.

criminal activity amounts to providing the FBI with authority to engage in fishing expeditions for potential wrongdoing by Americans.

Second, the contexts in which the FBI may run U.S.-person queries should be narrowed. Currently, the FBI's investigative guidelines permit agents to query any government database during "assessments"—the lowest level of investigation, which may be initiated without any factual predicate.[375] Assessments are thus proactive efforts at

> detecting criminal activities; obtaining information on individuals, groups, or organizations of possible investigative interest, either because they may be involved in criminal or national security-threatening activities or because they may be targeted for attack or victimization by such activities; and identifying and assessing individuals who may have value as human sources.[376]

Actually *collecting* communications pursuant to FISA is reserved for full investigations,[377] the highest level of investigation, which require "an articulable factual basis . . . that reasonably indicates" a crime or threat.[378] If that collection is sufficiently intrusive to be reserved for the most clearly predicated investigations, it also makes sense that the fruits of that collection not be accessible in investigations without any predicate whatsoever. Thus, U.S.-person queries should be limited to full investigations.

V. CONCLUSION

The United States' surveillance state has grown significantly over the past two decades.[379] That expansion in authority has been accompanied by a proliferation of rules and regulations meant to contain that authority within constitutional boundaries. As this Article has demonstrated, the system has repeatedly failed to achieve that goal, and the mechanisms routinely employed in response have been too anemic to deliver meaningful corrections.

This Article has argued that these shortcomings should not come as a surprise, because the basic nature of surveillance—especially when paired with the aggressive post-9/11 attitude toward surveillance—will frequently lead to the underenforcement of existing rules, including constitutional norms. Fortunately, commentators long ago identified the risk of underenforcement, as well as the tools available to guard against it. Policy-makers should rely on this theoretical work to reimagine surveillance enforcement by implementing categorical rules, presumptions, and enhanced procedures that can successfully combat the underenforcement of constitutional norms.

375. THE ATTORNEY GENERAL'S GUIDELINES FOR DOMESTIC FBI OPERATIONS 19, 29 (2008).
376. *Id*. at 17.
377. *Id*. at 31–32.
378. *See id*. at 21–22.
379. *See generally* discussion *supra* Part II.