University of Michigan Journal of Law Reform

Volume 55

2022

Fighting Global Surveillance: Lessons from the American Muslim Community

Danna Z. Elmasry
University of Michigan Law School

https://doi.org/10.36646/mjlr.55.4.fighting

FIGHTING GLOBAL SURVEILLANCE: LESSONS FROM THE AMERICAN MUSLIM COMMUNITY

By Danna Z. Elmasry*

ABSTRACT

The United States government has been spying on its citizens through a massive surveillance infrastructure that is unrestricted to a particular target or suspicion of wrongdoing. The statutory and regulatory authorities responsible for this infrastructure are sprawling and often secret. Built-in limitations and oversight mechanisms are riddled with loopholes or inaccessible due to exceedingly high thresholds. Litigation challenges to surveillance overreach often fail at standing. Under the current doctrine, plaintiffs must show that their own communications have been surveilled by a specific surveillance program. This Note contributes to surveillance reform by proposing a private right of action that sets the requirements for Article III standing in surveillance cases to broaden access to judicial redress for would-be plaintiffs with meritorious claims.

TABLE OF CONTENTS

* J.D. Candidate, University of Michigan Law School, 2022. Thank you to Professor Leah M. Litman, Professor Brenda Abdelall, Julie M. Moroney, Richard Zhao, and Becca Rogers for making this a better paper and encouraging me along the way.

INTRODUCTION

In early June 2013, news broke that the United States government was spying on its citizens.[1] Information leaked by former CIA officer Edward Snowden described a surveillance infrastructure of unprecedented scale.[2] In one example, a secret order from the Foreign Intelligence Surveillance Court required Verizon to surrender daily to the National Security Agency (NSA) enough data on all calls on its network to easily assemble "a comprehensive picture" of who millions of Verizon customers were contacting.[3] In another, the "Planning Tool for Resource Integration, Synchronization, and Management" (PRISM) surveillance program let the NSA access the servers of major internet companies—including Google, Facebook, and Apple—to collect people's search history, emails, live chats, Google Map searches, and file transfers.[4] The Snowden leaks revealed what this Note calls global surveillance: an immense surveillance infrastructure designed to harvest as much information as possible, unrestricted by a particular target or a suspicion of wrongdoing.

This infrastructure is still in operation. The Snowden leaks inspired minor legislative reform to prohibit bulk collection under the Foreign Intelligence Surveillance Act (FISA) of 1978. But this change was wholly inadequate to the task of reforming global surveillance, in part because it relies on more than one legal authority. In February 2022, partially declassified documents revealed a secret CIA bulk collection program, unknown even to the Senate Intelligence Committee.[5] While the CIA did not disclose the nature of the program or the type of data it collect-

---

1. Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, GUARDIAN (June 6, 2013, 6:05 AM), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order [perma.cc/4FQ7-6GGJ].

2. *Id.*; Ewen Macaskill, *NSA Files Decoded: What the Revelations Mean for You*, GUARDIAN (Nov. 1, 2013), https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded#section/1 [https://perma.cc/B6HY-ZKL7].

3. *Id*. Verizon was required to turn over metadata on all calls over its network including the phone numbers of both parties to a call, the call time and duration, and location data.

4. Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, GUARDIAN (June 7, 2013, 3:23 PM), https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data [perma.cc/Z349-N4DW]; *see also* Ryan Gallagher, *NSA Even Spied on Google Maps Searches, Documents Suggest*, SLATE (July 11, 2013, 3:46 PM), https://slate.com/technology/2013/07/xkeyscore-program-may-have-allowed-nsa-to-spy-on-google-maps-searches.html [perma.cc/9W9D-LTG8].

5. Press Release, Sen. Ron Wyden, Wyden and Heinrich: Newly Declassified Documents Reveal Previously Secret CIA Bulk Collection, Problems With CIA (Feb. 10, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-and-heinrich-newly-declassified-documents-reveal-previously-secret-cia-bulk-collection-problems-with-cia-handling-of-americans-information [perma.cc/76TZ-4AAZ].

ed, the agency did acknowledge that the program was authorized by Executive Order 12,333.[6] Between the two of them, FISA and Executive Order 12,333 authorize the massive infrastructure that continues to conduct global surveillance.

Minor legislative reform to surveillance authorities will not cut it. The experience of the American Muslim community, which has long been subject to heightened government surveillance, suggests that accountability through the courts is necessary to fight global surveillance. This Note seeks to contribute to surveillance reform by offering a way for more would-be plaintiffs to bring meritorious legal challenges to government surveillance. Part I examines the legal authorities that facilitate global surveillance: FISA § 702 and Executive Order 12,333. Part II considers the American Muslim community's long history of heightened surveillance and its litigation victories against surveillance overreach. Finally, because plaintiffs challenging secret government surveillance programs often fail to show standing, Part III proposes a private right of action that would enable more would-be plaintiffs to challenge government surveillance.

I. LEGAL AUTHORIZATION OF GLOBAL SURVEILLANCE: FISA AND EO 12,333

This Part examines the laws that authorize global surveillance: Section 702 of FISA and Executive Order 12,333.

A. *FISA Enables, Rather Than Curbs, Surveillance Overreach*

Congress enacted FISA[7] in the wake of a surveillance scandal. In 1975, after allegations that the CIA had been surveilling anti-war activists, a Senate Select Committee began to investigate abuses of warrantless government surveillance of Americans.[8] Headed by Senator Frank Church, himself a target of an NSA surveillance operation,[9] the Church

6. *Id*.

7. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, (codified at 50 U.S.C. Ch. 36).

8. *See* John F. Schifalacqua, *Insidious Encroachment? Strengthening the "Crown Jewels": The 2018 Reauthorization of FISA Section 702*, 9 AM. U. NAT'L SEC. L. BRIEF 93, 107 (2019); *see generally Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, U.S. SENATE, https://www.senate.gov/about/powers-procedures/investigations/church-committee.htm [https://perma.cc/DW6K-X6TS] (last visited May 8, 2022).

9. *See* Alex Urbelis, *After a Century of Mass Government Surveillance, it's Time for New Limits*, INTERCEPT (Sept. 22, 2015, 9:27 AM), https://theintercept.com/2015/09/22/history-of-us-surveillance-shows-need-for-new-limits/ [perma.cc/H4J2-A4EF].

Committee concluded that the government had "conducted a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association."[10] Speaking about the U.S. government's ability to "monitor the messages that go through the air," Senator Church observed that "that capability at any time could be turned around on the American people, and no American would have any privacy left."[11]

The Church report shocked the public and propelled Congress to act. FISA represented a compromise between Congress and the executive branch; the Act preserved the executive branch's power to conduct secret surveillance while imposing statutory restrictions on when such surveillance was permissible.[12] The Act limited the executive branch's domestic surveillance authority by permitting wiretapping of citizens and non-citizen residents in the United States in foreign intelligence investigations on a showing of probable cause that the target of the surveillance was a "foreign power" or "agent of a foreign power."[13] Later amendments to FISA authorized additional means of surveillance, including physical searches in 1994 and pen/trap surveillance and business records production in 1998.[14]

FISA continued to expand after September 11, 2001. In the immediate aftermath of the attacks, the PATRIOT Act lowered the threshold for authorizing surveillance.[15] One provision enabled the government to seek authorization for electronic surveillance whose "significant purpose"—rather than simply "purpose"—was obtaining foreign intelligence information.[16] Another provision authorized "an order requiring the production of any tangible things" that are merely "relevant" to an

---

10. Zachery Keller, Note, *Big Brother's Little Helpers: Telecommunication Immunity and the FISA Amendment Act of 2008*, 70 OHIO ST. L.J. 1215, 1227 (2009) (quoting Diane Carraway Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 441 n.22 (2006) (quoting staff reports from the Church Committee)).

11. Urbelis, *supra* note 9.

12. *See* Alan Butler, *Standing Up to* Clapper*: How to Increase Transparency and Oversight of FISA Surveillance*, 48 NEW ENG. L. REV. 55, 58 (2013).

13. 50 U.S.C. § 1802(b); *see also* 50 U.S.C. § 1801.

14. Butler, *supra* note 12, at 58 n.8. Pen/trap surveillance covers surveillance by pen registers and trap-and-trace devices, which capture, decode, and record incoming and outgoing signals and information, including dialing and routing information. *Id.* at 58 n.12.

15. *See* UNITING AND STRENGTHENING AMERICA BY PROVIDING APPROPRIATE TOOLS REQUIRED TO INTERCEPT AND OBSTRUCT TERRORISM (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (codified as amended in scattered sections of 8, 15, 18, 21, 50 and 51 U.S.C.) [hereinafter PATRIOT Act]; *see also* Susan M. Akram & Maritza Karmely, *Immigration and Constitutional Consequences of Post-9/11 Policies Involving Arabs and Muslims in the United States: Is Alienage a Distinction Without a Difference?* 38 U.C. DAVIS L. REV. 609, 639 (2005).

16. PATRIOT Act § 218.

antiterrorism or counterintelligence investigation.[17] Whereas the government used to have to "articulate specific facts to support a reasonable belief" that the target of surveillance "was a 'foreign power or an agent of a foreign power,'" now it just had to recite the formula of protecting against international terrorism.[18]

In 2008, the FISA Amendments Act (FAA) further broadened the scope of FISA surveillance in two important ways.[19] First, the FAA expanded the definition of "foreign intelligence information" to encompass any information related to U.S. foreign affairs.[20] Second, the FAA permitted warrantless electronic surveillance of communications between someone outside and someone inside the U.S., so long as the surveillance does not "intentionally target" American citizens and the target of that surveillance is a foreign agent "reasonably believed" to be outside of the United States.[21] This change, codified in FISA § 702, gave rise to modern programmatic surveillance.

1. Section 702 Represents a Radical Departure From Traditional FISA Surveillance

Under traditional FISA surveillance, the government seeks a warrant for surveilling a particular person by showing probable cause that they are a foreign power or an agent of a foreign power.[22] Section 702 requires nothing so strenuous. Instead of that particularized showing, under § 702, the government files a certification with the Foreign Intelligence Surveillance Court (FISC) to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[23] The certification asserts that a "significant purpose" of the surveillance is to obtain foreign intelligence information and includes targeting, minimization, and query procedures for the FISC's approval.[24]

---

17. *Id*. §§ 214, 215.

18. Akram & Karmely, *supra* note 15, at 640; 50 U.S.C. § 1862(a).

19. *See* Axel Arnbak & Sharon Goldberg, *Loopholes for Circumventing the Constitution: Unrestrained Bulk Surveillance on Americans by Collecting Network Traffic Abroad*, 21 MICH. TELECOMM'S. & TECH. L. REV. 317, 327–38 (2015).

20. 50 U.S.C. § 1801(e).

21. 50 U.S.C. § 1881a(a), (b)(1)–(2).

22. 50 U.S.C. §§ 1801(a), 1881b(b)(1)(C)(ii).

23. 50 U.S.C. § 1881a(a).

24. 50 U.S.C. § 1881a(h)(2)(A)(v); *see also* Mark M. Jaycox, *No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333*, 12 HARV. NAT. SEC. J. 58, 85–87 (2021).

Section 702 surveillance represents a massive departure from traditional FISA surveillance. Instead of seeking a warrant based on probable cause to surveil a particular target, the government seeks authorization to collect categories of information. [25] And so long as the government is not "intentionally targeting" U.S. persons, it can collect communications conducted inside the U.S.[26] As a result, the government can mount global surveillance operations untethered to particular targets or goals and acquire Americans' communications without a warrant. [27] In short, § 702 facilitates serious surveillance overreach that implicates privacy concerns and the risk of abuse against minority populations.

Section 702 surveillance works in two ways. To conduct "upstream" collection, the government taps into internet or telephone networks via undersea and fiber optic cables and filters passing data to find targeted information.[28] To conduct "downstream" collection, which represents the bulk of § 702 intelligence, the government works with internet service providers to obtain data.[29] This method is particularly useful because encrypted data become unencrypted when they reach an internet service provider.[30] The upshot is hard to overstate. While the NSA refuses to estimate how many Americans' communications are collected under § 702, a 2011 FISC opinion found that the agency collected "250 million Internet communications . . . the previous year under Section 702."[31] Assuming that only ten percent of those communications involved Americans, that still translates to 25 million communications involving Americans collected under § 702 in one year, not including the tens of thousands of purely domestic communications which also get sucked into in the net.[32]

---

25. *See* Jaycox, *supra* note 24, at 86–87.

26. *See* 50 U.S.C. § 1881a(b)(3); Arnbak & Goldberg, *supra* note 19.

27. 50 U.S.C. § 1881b(a)(1); Arnbak & Goldberg, *supra* note 19.

28. Schifalacqua, *supra* note 8, at 115. The government may filter for communications to or from a foreigner abroad (to/from collection) or for communications that mention a foreigner abroad (about collection). The NSA stopped about collection in 2011. *Id.* at 116 n.107.

29. *Id.* at 116–17.

30. *Id.*

31. ELIZABETH GOITEIN & FAIZA PATEL, WHAT WENT WRONG WITH THE FISA COURT 27 (Brennan Ctr. for Just. 2015), https://www.brennancenter.org/media/140/download [https://perma.cc/9JHM-AVAH].

32. *See id.*

2. Section 702's Limitations and Methods of Redress Fail to Contain Overreach

The FAA prescribes certain limits on electronic surveillance. The government may not seek authorization for a surveillance program that intentionally targets someone within the U.S., targets a U.S. citizen outside the U.S., acquires communications whose sender and recipients are known to be in the U.S., or is inconsistent with the Fourth Amendment or the Constitution.[33] The government's application must also make reference to "targeting and minimization" procedures designed to reduce the risk of capturing communications of American citizens or people located inside the U.S.[34] But in reality, these limits are either undermined by the nature of modern data collection or by the lack of effective redress mechanisms.

The nature of § 702 data collection methods make it difficult to preserve the distinction between domestic and foreign targets.[35] Simply by collecting Americans' Internet traffic abroad, the government creates a presumption of foreignness, which enables "largely unrestrained surveillance on Americans."[36] This is not an abstract loophole. It is widely accepted that surveillance operations aimed at foreigners abroad "inevitably picks up swaths of information about Americans who should enjoy constitutional protections."[37] Information collected under § 702 in this manner can be used to prosecute an American citizen, which further undermines constitutional protections that should attach to an American citizen's communications.[38] Additionally, targeting a person often occurs after their communications have already been intercepted, stored, searched, and shared with other government agencies.[39] Taken together, these loopholes hollow out the protections ostensibly baked into FISA and the FAA.

FISA and the FAA envision several limits on the use of § 702, but each comes with problems that undermine its efficacy. The FISC reviews the government's surveillance program applications to determine whether an application's targeting and minimization procedures are "consistent with the requirements of [FISA] and with the Fourth Amendment."[40] Despite recent legislation strengthening their oversight

33. *See* Schifalacqua, *supra* note 8, at 114.
34. *See* 50 U.S.C. § 1881a(c)(1)(A).
35. *See* Schifalacqua, *supra* note 8, at 109.
36. Arnbak & Goldberg, *supra* note 19, at 319.
37. Schifalacqua, *supra* note 8, at 109.
38. *Id.* at 118.
39. *See* Arnbak & Goldberg, *supra* note 19, at 325.
40. 50 U.S.C. § 1881a(j)(3)(A).

and capabilities, the FISC and its appellate court are less organs of searching judicial review than rubber stamps for government surveillance.[41] The FISC regularly approves applications riddled with errors ranging from inadequate factual support to missing documentation.[42] This is both a legal and oversight issue. Because both the FISC and its appellate court are only required to disclose significant opinions,[43] the law around the government's surveillance power, which is replete with broad constitutional questions, is being developed without public scrutiny or oversight.[44]

Additionally, FISC briefing is historically non-adversarial, with only the government making representations.[45] Recently, the FISC has been required to appoint *amicus curiae* from a pool of amici when considering "novel or significant interpretations of the law," but the pool is under the control and oversight of the FISC judges,[46] and research suggests *amici* are appointed sporadically.[47] Perhaps unsurprisingly, the government continues to enjoy an "unparalleled" success rate at the FISC.[48]

Another intended limit on § 702 use is the FISA notice provision. This provision requires the government to give advance notice to an individual if it intends to "enter into evidence or otherwise use or disclose" at trial information "obtained or derived" from electronic surveillance of that person.[49] But the notice provision only applies to "aggrieved per-

---

41. *See* Laura K. Donohue, *Bulk Metadata Collections: Statutory and Constitutional Considerations*, 37 HARV. J.L. & PUB. POL'Y 757, 831 (2014).

42. Ryan Lucas, *Justice Department IG Finds Widespread Problems with FBI's FISA Applications*, NPR (Mar. 31, 2020, 1:37 PM), https://www.npr.org/2020/03/31/824510255/justice-department-ig-finds-widespread-problems-with-fbis-fisa-applications [https://perma.cc/L9F5-LVGE].

43. *See* Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015 or the USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 402, 129 Stat. 268 (2015) (codified in scattered sections of 50 U.S.C.) [hereinafter USA FREEDOM Act]. The statute requires the Director of National Intelligence to conduct a declassification review of FISC and FISCR opinions and orders and declassify those that "include[] a significant construction or interpretation of any provision of law, including any novel or significant construction or interpretation of the term 'specific selection term.'" *Id.* § 402(a)(2)(a).

44. *See* Butler, *supra* note 12, at 64.

45. *See* Faiza Patel & Raya Koreh, *Enhancing Civil Liberties Protections in Surveillance Law*, BRENNAN CTR. FOR JUST. (Feb. 27, 2020), https://www.brennancenter.org/our-work/analysis-opinion/enhancing-civil-liberties-protections-surveillance-law [https://perma.cc/2VRS-NPST].

46. *See* USA FREEDOM Act §§ 401–02.

47. *See* Patel & Koreh, *supra* note 45 (finding that "in at least four cases, the FISC did not appoint amici, although it seemed to be required by the statute, including one case in which the government obtained permission to expand its authority to query communications collected warrantlessly under Section 702 of the FISA Amendments Act of 2008 for the calls and e-mails of particular Americans.").

48. Donohue, *supra* note 41, at 831.

49. 50 U.S.C. § 1806(c).

sons,"[50] which courts have interpreted to mean a person who can prove that they were the target of a specific surveillance operation.[51] In other words, the government is only required to notify someone that they were the subject of surveillance if that person has already proven that they were the subject of surveillance. This provision is of little assistance to plaintiffs looking to establish that their surveillance was unlawful, particularly before any discovery.[52] The government further evades giving notice by interpreting the provision to attach only during prosecution.[53] In practice, the government uses § 702 information throughout investigation and prosecution but avoids the notice requirement by not introducing § 702 information at trial.[54] Between the courts' interpretation and the government's practice, the notice provision is powerless to inform innocent victims of the government's unlawful surveillance.

Congress's attempts to reform the FISA process have not produced substantial changes. The USA Freedom Act in 2015, passed in response to the Snowden leaks, prohibited bulk collection of call records, tightened targeting requirements for phone record collection, and reauthorized the PATRIOT Act's expansive surveillance framework, all in the same legislative breath.[55] While the pandemic temporarily slowed the PATRIOT Act's reauthorization in the spring of 2020,[56] it also stymied attempts to strengthen the PATRIOT Act's privacy protections. An amendment to the USA FREEDOM Reauthorization Act of 2020 prohibiting warrantless surveillance of Americans' browsing and search history failed by one vote; at least one Senator was unable to vote for the amendment due to consequences of the pandemic.[57] Despite substantial information about § 702's mechanics and its weak privacy protections, Congress has been slow to enact reform.

---

50. 50 U.S.C. § 1801(k).

51. *See* Ctr. for Const. Rts. v. Obama, No. C 07-1115 VRW, slip op. at 20 (N.D. Cal. Jan. 31, 2011) (". . . only by presenting evidence of actual surveillance can a plaintiff establish the 'aggrieved person' status necessary to proceed with a FISA claim."); Butler, *supra* note 12, at 66 n.62.

52. *See, e.g.*, Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013) (holding that plaintiffs lacked standing because their claims of being surveilled by the NSA were "speculative.").

53. *See* Evan R.C. Correia, Note, *Pulling Back the Veil of Secrecy: Standing to Challenge the Government's Electronic Surveillance Activities*, 24 TEMP. POL. & CIV. RTS. L. REV. 185, 201–02 (2014).

54. *See id.*

55. *See* USA FREEDOM Act §§ 101, 301, 401–02.

56. *See* Sara Morrison, *The Senate Voted to Let the Government Keep Surveilling Your Online Life Without a Warrant*, VOX (May 14, 2020), https://www.vox.com/recode/2020/5/13/21257481/wyden-freedom-patriot-act-amendment-mcconnell [https://perma.cc/KXF8-65N5].

57. *See id.*

B. *Executive Order 12,333's Authorization of Large-Scale Collection is Almost Unchecked*

The other major legal authorization for electronic surveillance is Executive Order 12,333.[58] Issued by President Reagan in 1981, the Order authorizes and regulates electronic surveillance conducted abroad.[59] When the Snowden leaks turned attention towards FISA and the FISC, a former State Department official urged the public to demand similar scrutiny of the Order, which the NSA has identified as the "primary legal authority" for its electronic interception operations.[60] Compared to FISA, the public knows relatively little about the programs the Order authorizes. Even the Senate Select Committee on Intelligence has said that it is not "sufficiently" able to oversee activities authorized by the Order.[61]

The Order creates "an immense policy regime" overseeing all foreign electronic surveillance not covered by FISA. [62] It authorizes the collection of a broad array of foreign intelligence except for information "concerning the domestic activities of United States persons."[63] Specifically, the Order authorizes the collection and analysis of communications, metadata, mobile phone numbers, geolocation, and social networks.[64] Collection and analysis is not limited to metadata, but extends to the content of communications.[65] Further, the Order imposes no restrictions on how many communications can be collected and retained.[66]

The Order's permissive targeting and processing procedures allow for large-scale acquisition and retention of Americans' information.[67] With a broad definition of "foreign intelligence" and a presumption that targets outside the U.S. are foreigners, the Order's targeting procedures permit a very wide scope of authorized surveillance.[68] The Order's pro-

---

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

59. *Id*.

60. *See* John Napier Tye, Opinion, *How a Reagan Order Set the NSA Loose*, WASH. POST (July 20, 2014), http://www.washingtonpost.com/opinions/meet-executiveorder-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html [https://perma.cc/KML9-UWNX]; Arnbak & Goldberg, *supra* note 19, at 321.

61. Tye, *supra* note 60.

62. Jaycox, *supra* note 24, at 62, 90. FISA's definitions do not include "most modern methods of preparing a networked communications infrastructure for surveillance." As a result, they are not considered "electronic surveillance" under FISA and are, therefore, regulated only by EO 12333." Arnbak & Goldberg, *supra* note 19, at 331.

63. Exec. Order No. 12,333, 46 Fed. Reg. 59,941, § 2.3(b) (Dec. 4, 1981).

64. *See* Jaycox, *supra* note 24, at 59.

65. *See* 46 Fed. Reg. 59,941, § 2.3(c); Jaycox, *supra*, note 24, at 91.

66. *See* Tye, *supra* note 60.

67. *See* Jaycox, *supra* note 24, at 64–65, 83–102.

68. *See id*. at 83, 104–05 ("Generally, analysts must only have a reasonable belief that the selector is a non-U.S. person outside the United States . . . [h]owever, it is unclear how the reasonable

cessing procedures authorize an unprecedented scale of data retention: one authorized program "analyzes all phone calls and metadata exiting a country," while another acts as a "'front-end search engine' for intelligence analysts . . . send[ing] commands to servers connected to the global telecommunications backbone to prioritize, analyze, and store information into NSA databases."[69] Once collected, that information—including information from or about Americans—is stored in NSA databases until it is "actively reviewed by a human analyst".[70] Taken together, the Order's broad provisions enable a massive amount of information collection, storage, and retention with little protection for privacy.

C. *Conclusion*

In the summer of 2013, the Snowden leaks exposed the massive government surveillance infrastructure capturing, storing, and analyzing the information and communications of millions of Americans. The government was spying on its citizens without warrants, without oversight, and without justification.

This surveillance infrastructure rests primarily on two highly permissive legal authorities: Section 702 of the FISA and Executive Order 12,333. Through programmatic surveillance, outdated protections based on geographic location, and permissive and malleable targeting procedures, these authorities produced a global surveillance effort that harvests data from the internet backbone and service providers without a particular target or suspicion of wrongdoing. Despite minimal legislative reform in 2015, the bulk of this global surveillance system remains unchanged.

II. GLOBAL SURVEILLANCE TEST CASE: THE AMERICAN MUSLIM COMMUNITY'S EXPERIENCE FIGHTING SURVEILLANCE AND ITS EFFECTS.

FISA § 702 and Executive Order 12,333 created a surveillance infrastructure that has had an outsized impact on the American Muslim community.[71] To better explore the impact of heightened surveillance and

---

belief analysis is conducted in practice. Documents show analysts can use selectors that *may* collect foreign intelligence information.").

69. *See id.* at 83–84.

70. *See id.* at 87.

71. *See supra* Part I.

successful strategies for curbing surveillance overreach, this Part examines the American Muslim community's history of surveillance, its litigation victories against government surveillance, and the impact of heightened surveillance on the community.

A. *The American Muslim Community has been Targeted for Increasingly Comprehensive Surveillance*

Far from being a recent or post–9/11 phenomenon, government surveillance of the American Muslim community has evolved over a long history.

1. Initially, American Muslims were Targeted for Heightened Surveillance Due to Ties to Black Liberation Activism

The nexus of Islam and racial politics defined the beginning of heightened surveillance against the American Muslim community. Many of the first Muslims in America were enslaved Africans brought to work on plantations, and the Black Muslim community grew as it intersected with Black opposition to racial oppression.[72] Beginning in the interwar period of the 1930s, racial tensions increased, and the nascent FBI began to surveil specific Black Muslim groups for their association with Black activism against white supremacy.[73] The FBI's messaging framed Islam as a "problematic political symbol that deserved to be disciplined through surveillance."[74] That surveillance continued through the 1960s, overlapping with the Bureau's COINTELPRO program.[75]

---

72. *See* Edward E. Curtis VI, *The Black Muslim Scare of the Twentieth Century: The History of State Islamophobia and its Post-9/11 Variations*, *in* ISLAMOPHOBIA IN AMERICA: THE ANATOMY OF INTOLERANCE 75, 78, 84–99 (Carl W. Ernst ed., 2013) ("In this era of new nativism . . . the Ahmadi linking of domestic struggles for racial liberation to . . . a rising call for self-determination, the deep spirituality of the Qur'an, and black historical achievements under Islam was a powerful message that conviced over 1,025 mostly African American people to convert to Islam from 1921 to 1925."). This Note will refer to the American Muslim community to mean the community of Muslims living in America, which includes both American citizens and foreign nationals.

73. *See id.* at 90.

74. *Id.* at 93.

75. *Id.* at 94–99.

2. Later, American Muslims were Targeted for Heightened Surveillance Based on Their Perceived Religion, Ethnicity, and Race

Once effectively "othered" as "foreign, disloyal, and imminently threatening,"[76] American Muslims routinely experienced heightened surveillance during times of crisis. For example, after the 1972 attack on the Munich Olympics, President Nixon authorized the FBI to investigate people of "Arabic background" for ties to terrorism.[77] Similarly, in the wake of the Iran hostage crisis, President Carter initiated a registration campaign, forcing thousands of Iranians across the country to register with the federal government.[78] In the 1980s, amid heightened targeting of Palestinians and pro-Palestine activists, President Reagan authorized a plan to detain and intern thousands of Arab and Iranian immigrants at designated sites in Louisiana.[79] And after the 1990 U.S. invasion of Kuwait, President Bush launched a program to fingerprint all American residents and immigrants of Arab origin.[80]

These surveillance efforts turned up specious information that the government used to prosecute American Muslims. For example, in the late 1990s, the government began prosecuting American Muslims in immigration courts based on secret evidence obtained through surveillance. Misapplying the secret evidence provisions of the Anti-Terrorism and Effective Death Penalty Act of 1996 (AEDPA), Immigration and Naturalization Services (INS) denied bond to Arab and Muslim defendants designated as suspected terrorists; detained them for years (sometimes in solitary confinement); and tried them on evidence the defendants had

---

76. Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration after September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.U. ANN. SURV. AM. L. 295, 301 (2002).

77. *Id.* at 314.

78. *See id.*; John M. Goshko, *Carter Orders Deportation of Illegal Students*, WASH. POST (Nov. 11 1979), https://www.washingtonpost.com/archive/politics/1979/11/11/carter-orders-deportation-of-illegal-students/2f242d98-cf30-46bb-8e8a-c0898f45eda8/ [https://perma.cc/9XSR-PBAN] (". . . all Iranian students will be required in the next few days to report their location and status to the Immigration and Naturalization service."); Narenji v. v. Civiletti, 617 F.2d 745, 746 (D.C. Cir. 1979), *cert. denied sub nom.* Confederation of Iranian Students v. Civiletti, 446 U.S. 957 (1980) (upholding an immigration regulation promulgated by the Attorney General that required "all nonimmigrant alien postsecondary school students who are natives or citizens of Iran to report to a local INS office or campus representative to 'provide information as to residence and maintenance of nonimmigrant status.'").

79. *See* Akram & Johnson, *supra* note 76, at 316; Ben Wofford, *The Forgotten Government Plan to Round Up Muslims*, POLITICO (Aug. 19, 2016), https://www.politico.com/magazine/story/2016/08/secret-plans-detention-internment-camps-1980s-deportation-arab-muslim-immigrants-214177 [https://perma.cc/6NZV-MGMG].

80. Akram & Johnson, *supra* note 76, at 315.

never seen.[81] Once declassified, the evidence was routinely found to be "hearsay, conjectural, unreliable, or utterly unpersuasive of the government's charges."[82] Nevertheless, the use of secret evidence kneecapped litigants' ability to obtain justice through the courts.[83] The secret evidence provisions were almost exclusively applied to immigrants and residents of Arab or Muslim background.[84] The only secret evidence case against a non-Arab or Muslim was against an Indian Sikh.[85] When news about the use of secret evidence came to light in the press, Arab, Muslim, and civil liberties groups pressured Congress to repeal the use of secret evidence in immigration proceedings, but the repeal bill lost support after 9/11.[86]

Registration programs continued after 9/11. Once again, Arabs, Muslims, and South Asians living in America disproportionately bore the brunt of this surveillance expansion. Beginning in 2002, the National Security Entry Exit Registration System (NSEERS) required all male teenage and adult immigrant and permanent resident nationals of twenty-five countries to be fingerprinted and registered or be subject to removal.[87] Of the twenty-five countries, all but one, North Korea, were majority Arab or Muslim. NSEERS was expanded, without notice, to people whose national origin was a designated country, even if they held other citizenship.[88] The federal government even repurposed other registration programs to target Arab and Muslim immigrants, using, for example, the Alien Absconder Initiative intended for Latin American immigrants to register some 6,000 men from Muslim-majority countries.[89]

The routine surveillance of American Muslims by the state spawned private-actor copycats. For example, the Anti-Defamation League of B'nai B'rith (ADL) employed a former San Francisco Police Department

---

81. Michael J. Whidden, *Unequal Justice: Arabs in America and United States Antiterrorism Legislation*, 69 FORDHAM L. REV. 2825, 2847 (2001); Anti-Terrorism and Effective Death Penalty Act of 1996 (AEDPA), Pub. L. No. 104-132, § 504(e), 110 Stat. 1214, 1262 (1996).

82. Akram & Karmely, *supra* note 15, at 618.

83. *See* Rafeedie v. I.N.S., 880 F.2d 506, 516 (D.C. Cir. 1989) ("It is difficult to imagine how even someone innocent of all wrongdoing could meet such a burden.").

84. *See* Secret Evidence Repeal Act of 2000, H.R. 2121, 106th Cong. (2000) at 6; Akram & Karmely, *supra* note 15, at 617.

85. *See* Akram & Karmely, *supra* note 15, at 617.

86. *See id.* at 619–20; *see also* H.R. 2121.

87. *See* Ty S. Wahab Twibell, *The Road to Internment: Special Registration and Other Human Rights Violations of Arabs and Muslims in the United States*, VT. L. REV. 407, 443– 44 (2005).

88. *See* Akram & Karmely, *supra* note 15, at 660–61.

89. *See* Yaser Ali, Comment, *Shariah and Citizenship – How Islamophobia is Creating a Second-Class Citizenry in America*, 100 CALIF. L. REV. 1027, 1047 (2012).

officer to surveil Arab American Individuals and organizations.[90] The ADL shared the information obtained through surveillance with Israel, resulting in the arrest of at least one U.S. citizen of Arab descent when he visited Palestine, and with the FBI, triggering the case of the "LA Eight."[91] In a pre-dawn operation, more than 100 law enforcement officers arrested eight activists—seven Palestinian and one Kenyan—beginning a twenty-year ordeal in which the U.S. failed to get any charges to stick until an immigration judge finally dismissed the case, calling it "an embarrassment to the rule of law."[92]

3. After 9/11, the NYPD Targeted American Muslims Through Global Surveillance

In the wake of the September 11 attacks, the New York Police Department (NYPD) mounted a global surveillance campaign against the American Muslim community.[93] The "expansive" program reached from Philadelphia to New Haven, Newark to Queens.[94] Officers covered more than 250 mosques and businesses, mounting video surveillance cameras across from entrances; collecting patrons' and congregants' license plate numbers; spying on sermons and conversations; and infiltrating Muslim student associations (MSAs) at colleges and universities across the Tri-State Area.[95] In one instance, an officer posing as an MSA member went on a rafting trip to eavesdrop and record how often the students prayed.[96] The NYPD even surveilled its partners in anti-terrorism work, "including imams who frequently appeared at the Mayor's side."[97] The NYPD program typified global surveillance in that its goal was to obtain as much information as possible. Except for its religious and ethnic frames, the program had no specific target and was not based on a concrete or articulable suspicion of wrongdoing.

---

90. *See* Akram & Johnson, *supra* note 76, at 306–07.

91. *See id.* at 307–08.

92. Neil MacFarquhar, *U.S., Stymied 21 Years, Drops Bid to Deport 2 Palestinians*, N.Y. TIMES (Nov. 1, 2007), https://www.nytimes.com/2007/11/01/us/01settle.html?_r=0 [https://perma.cc/X39E-4Y8A]; *see also* Wofford, *supra* note 79.

93. *See, e.g.*, Matt Apuzzo & Adam Goldman, *With CIA Help, NYPD Moves Covertly in Muslim Areas*, ASSOCIATED PRESS (Aug. 23, 2011); *see also* Hassan v. City of New York, 804 F.3d 277 (3d Cir. 2015).

94. DIALA SHAMAS & NERMEEN ARASTU, MAPPING MUSLIMS: NYPD SPYING AND ITS IMPACT ON AMERICAN MUSLIMS 11 (2013).

95. *See id.* at 11, 39–40; *see also Hassan*, 804 F.3d at 285.

96. *See* Hassan, 804 F.3d at 285.

97. SHAMAS & ARASTU, *supra* note 94, at 11.

This massive effort mobilized numerous forms of surveillance. In addition to undercover officers, the NYPD had informants in mosques and MSAs within a 250-mile radius of New York City.[98] But human sources were not the only tool mobilized in this global effort. Geo-mapping emerged as a way to reveal patterns in crime scenes, but quickly became a tool for collecting data on specific communities.[99] The NYPD and the FBI used geo-mapping to collect enormous amounts of data on the American Muslim community, ranging from warrants to sex offender lists to cellular tower data.[100] Agents used these maps to recruit and maintain informants and to plot out the contours of targeted communities.[101]

By focusing on neighborhoods that were home to clusters of different ethnic, racial, or religious groups, intelligence officials were effectively targeting individuals on the basis of those protected characteristics. This heightened and discriminatory targeting resulted in an "'extremely pernicious' practice of ascribing propensity to crimes to people based on their ethnicity or religion."[102] In one example, the FBI designated Arab-American and Muslim communities in Michigan as potential terrorist recruitment ground on the basis of the community's religious and ethnic makeup alone.[103]

---

98. *See Hassan*, 804 F.3d at 285–86.

99. Inside the FBI: *New Intelligence Tools*, FBI (Dec. 12, 2008), https://www.fbi.gov/audio-repository/news-podcasts-inside-new-intelligence-tools.mp3/view [https://perma.cc/BQH2-H4G6]. In 2008, the regulations around targeting changed to allow data collection on communities: "If, for example, intelligence reporting reveals that members of certain terrorist organizations live and operate primarily within a certain concentrated community of the same ethnicity . . . the location of that community is clearly valuable – and properly collectible – data." Spencer Ackerman, *FBI Crime Maps Now "Pinpoint" Average Muslims*, WIRED (Oct. 24, 2011, 1:30 PM), https://www.wired.com/2011/10/fbi-geomaps-muslims/ [https://perma.cc/4SD8-LN6X] (quoting FBI, DOMESTIC INVESTIGATIONAL OPERATIONS GUIDE (Dec. 2008)).

100. Inside the FBI: *New Intelligence Tools*, FBI (Dec. 12, 2008), https://www.fbi.gov/audio-repository/news-podcasts-inside-new-intelligence-tools.mp3/view [https://perma.cc/BQH2-H4G6].

101. *Id.*

102. Charlie Savage, *F.B.I. Scrutinized for Amassing Data on American Communities*, N.Y. TIMES (Oct. 20, 2011), https://www.nytimes.com/2011/10/21/us/aclu-releases-fbi-documents-on-american-communities.html [https://perma.cc/FKF5-LJAZ].

103. *See id.*

B. *Heightened Surveillance of the American Muslim Community Produced Negative Stereotypes, Bred Self-Censorship, and Stymied Opposition to Surveillance*

The American Muslim community's long history of heightened surveillance produced devastating consequences for the community, and broader ripple effects on the general population.

One consequence of this heightened targeting, which is grounded in the perception of American Muslims as threats to national security, is a body of literature and "expertise" that defines the characteristics of suspicious activity against Muslimness.[104] This literature describes radicalization as a "purely Muslim phenomenon" and imagines an inevitable trajectory for the pious or engaged Muslim, a kind of express train to terrorism.[105] By framing radicalism as an exclusively Muslim problem, this approach ensures that even religiously-neutral radicalism literature is read and applied exclusively against Muslims. [106] Far from being a fringe perspective held by a small number of theorists, this misguided point of view underpins the approach of police departments across America, including the NYPD.[107]

In addition to producing uneven and discriminatory results, this approach generates incoherent policing policies. One guide for assessing radicalism published by the National Counterterrorism Center identifies both "Connection to Group Identity" and "Isolation and Social Exclusion" as indicators of radicalism.[108] Other indicators include wearing traditional Islamic clothing, growing a beard, giving up drinking or cigarettes, and becoming involved in the community.[109] By measuring suspicion against ordinary characteristics of adolescence or pious Muslim behavior, this misguided policy puts the average, visibly Muslim person at an unreasonable risk of unlawful surveillance.

---

104. *See, e.g.*, Khaled A. Beydoun, *"Muslim Bans" and the (Re)making of Political Islamophobia*, 2017 U. ILL. L. REV. 1733, 1753 (2017) ("In practice, CVE [Countering Violent Extremism] Policing links radicalization - or propensity for radicalization - with Muslim identity. CVE is specifically focused on monitoring observant Muslim Americans, particularly those transitioning from secular to devout lifestyles, members of the community holding 'critical politics,' or individuals who express their faith conspicuously.").

105. *Id.* at 1753–54 (quoting Amna Akbar, *Policing "Radicalization,"* 3 U.C. IRVINE L. REV. 809, 818 (2013)).

106. *See id.* at 1754.

107. *See* SHAMAS & ARASTU, *supra* note 94, at 13.

108. NATIONAL COUNTERTERRORISM CTR., COUNTERING VIOLENT EXTREMISM: A GUIDE FOR PRACTITIONERS AND ANALYSTS 19–21 (2014).

109. *See* SHAMAS & ARASTU, *supra* note 94, at 13.

Other consequences of heightened targeting include significantly depressed community engagement and self-censorship.[110] In the wake of 9/11, Tri-State Area mosques became tense sites "marred by mutual suspicion" instead of vibrant community spaces that facilitated intimate spiritual development.[111] During the NYPD surveillance campaign, Muslims in the New York and New Jersey areas reported pervasive self-censorship.[112] Political debate, comments on current events, and merely speaking in Arabic or Urdu could attract unwanted attention.[113] Muslim Student Associations put up signs warning members against having political conversations in their meeting rooms.[114] The threat of heightened police surveillance inhibited community development and free expression.

Perhaps most insidiously, heightened targeting produces a chilling effect that suppresses not only political discourse, but also the possibility of effective, community-wide opposition to the surveillance itself.[115] In this sense, the American Muslim community's experience is portable to anyone who suspects that they, their communications, and their movements could be the target of surveillance. This suspicion is no longer the sole province of tinfoil-hatted conspiracy theorists. Activists and protestors the world over communicate through encrypted platforms.[116] Some American Black Lives Matter protestors take substantial measures to avoid detection by facial recognition software.[117] The impact of global surveillance targeting is already percolating through to the mainstream. Luckily, the American Muslim community's efforts to combat surveillance overreach suggest a way forward.

---

110. *See id.* at 15, 20.

111. *Id.* at 18; *see also* Hassan v. City of New York, 804 F.3d 277, 288 (3d Cir. 2015) (stating that mosques under NYPD surveillance saw declined attendance "because their congregants can no longer worship freely knowing that law-enforcement agents or informants are likely in their midst.").

112. *See* SHAMAS & ARASTU, *supra* note 94, at 20–23.

113. *See id.*

114. *See id.* at 25.

115. *See id.* at 22.

116. *See* Andy Greenberg & Lily Hay Newman, *How to Protest Safely in the Age of Surveillance*, WIRED (May 21, 2020), https://www.wired.com/story/how-to-protest-safely-surveillance-digital-privacy/ [https://perma.cc/2TS9-CGKK]. The advice in this article, though generally applicable, was in response to Black Lives Matter protests, as evidenced by its sources. *See, e.g.*, Matthew Dessem, *Police Erupt in Violence Nationwide*, SLATE (May 31, 2020, 1:37 AM), https://slate.com/news-and-politics/2020/05/george-floyd-protests-police-violence.html?via=homepage_taps_top [https://perma.cc/2QQG-Q2WT]; Evan Greer (@evan_greer), TWITTER (May 30, 2020, 9:41 PM), https://twitter.com/evan_greer/status/1266907715437121536 [perma.cc/5CB8-7RE4].

117. Greenberg & Newman, *supra* note 116.

C. *Litigation Victories Show that Courts are Willing to Check Surveillance Overreach*

Time and again, the American Muslim community has prevailed against unlawful and unconstitutional surveillance in court. Both the secret evidence cases and the litigation against the NYPD's post-9/11 surveillance program demonstrate that courts are willing to enforce due process and equal protection guarantees, even in the heady context of national security.

1. Courts Held that the Use of Secret Evidence Against Defendants Violates their Constitutional Right to Due Process

Beginning in 1995, federal courts began to hold that the use of secret evidence in regular deportation proceedings is unconstitutional under the Fifth Amendment's due process protections.[118] The court's analysis in *Kiareldeen v. Reno* is typical of the line of cases that rolled back the use of secret evidence. Hany Kiareldeen was a Palestinian living in New Jersey and managing an electronics store when he was arrested for overstaying his student visa.[119] The INS opposed his application for relief, relying on secret evidence proffered by the FBI alleging that Kiareldeen was a member of an unnamed terrorist group with ties to the World Trade Center bombing.[120] He remained in detention for nearly two years.[121]

The *Kiareldeen* court applied the *Mathews v. Eldridge* procedural due process balancing test, considering "1) the private interest affected; 2) the risk of erroneous deprivation of the interest and the value of additional or alternative procedural safeguards; and 3) the government's interest in utilizing the procedure."[122] The court noted that Mr. Kiareldeen had been removed from his home and family and "denied rights that '[rank] high among the interests of the individual.'"[123] The risk of erroneous deprivation was high because without knowledge of the evidence against him, it was nearly impossible for Mr. Kiareldeen to defend himself.[124] The court went further, calling the use of secret evidence "a one-

---

118. *See* Am.-Arab Anti-Discrimination Comm. v. Reno, 70 F.3d 1045 (9th Cir. 1995); *see also* Rafeedie v. I.N.S., 880 F.2d 506, 516 (D.C. Cir. 1989); Kiareldeen v. Reno, 71 F. Supp. 2d 402 (D.N.J. 1999).

119. *See* Whidden, *supra* note 81, at 2878, *Kiareldeen*, 71 F. Supp. 2d at 413.

120. *Kiareldeen*, 71 F. Supp. 2d at 416.

121. *Id.* at 413.

122. *Id.* at 412.

123. *Id.* at 413 (quoting Landon v. Plasencia, 459 U.S. 21, 32 (1982)).

124. *See id.* at 413.

sided process by which the protections of our adversarial system are rendered impotent."[125] In other words: "It is difficult to imagine how even someone innocent of all wrongdoing could [defend himself against secret evidence]."[126] Finally, the court laid into the government's interest in using secret evidence, noting that "even the government does not find its own allegations [in this case] sufficiently serious to commence criminal proceedings."[127]

The *Kiareldeen* opinion and others like it were important for several reasons. First, they affirmed noncitizens' liberty interest in staying in the U.S. and held that this interest is protected by the Due Process Clause of the Fifth Amendment.[128] Second, they excoriated the underpinning logic of secret evidence and emphasized its incongruity with the adversarial system. And third, they demonstrated that courts are necessary to fight government surveillance, particularly against minority groups. Political pressure and public outcry were not enough to move the needle; after 9/11, support for repealing AEDPA's secret evidence provisions evaporated.[129] In that contentious climate, only federal courts were willing to address the absurdity of these provisions, their devastating impact on due process, and their selective deployment against Arab and Muslim defendants.

Courts also played an instrumental role in questioning the "reliability of government processes initiated and prosecuted in darkness."[130] In open court, a plaintiff can hold the government accountable to the foundational promises of the Constitution—in this case, due process protections for "citizens and resident aliens alike."[131] These cases also revealed how much the secret evidence provisions were abused. The provisions were not used pursuant to their statutory authorization, nor was their use limited to individuals who posed a threat to national security.[132] Without judicial redress, American Muslims would have had to rely on the court of public opinion, which was unlikely to look favorably on their plight.

---

125. *Id.*

126. *Id.* at 412 (quoting Rafeedie v. I.N.S., 880 F.2d 506, 516 (D.C. Cir. 1989)).

127. *Id.*

128. *See e.g.*, *id.* at 411–12 (quoting *Rafeedie*, 880 F.2d at 516).

129. *See* Akram & Karmely, *supra* note 15, at 619–20; Secret Evidence Repeal Act of 2000, H.R. 2121, 106th Cong. (2000).

130. *Kiareldeen*, 71 F. Supp. 2d at 413.

131. *Id.* at 414.

132. *See* H. COMM. ON THE JUDICIARY, SECRET EVIDENCE REPEAL ACT OF 2000, H.R. REP. NO. 106-981, at 8 (2000).

2. Litigation Against NYPD Global Surveillance Pushed the City to Reform its Policing Policies

Courts similarly constrained the NYPD's covert global surveillance program. The program was common knowledge within the American Muslim community, which was alert to the presence of informants and undercover officers and aware of the NYPD's "widely publicized" surveillance reports.[133] But it was not until the Associated Press broke the story in 2011 that the program's purpose, scope, and methods became known.[134]

On the back of that reporting, a group of advocates sued the City of New York.[135] The plaintiffs in this case argued that the NYPD intentionally discriminated against the American Muslim community by targeting its members for surveillance using religion as a "proxy for criminality."[136] The plaintiffs in this case argued, in part, that the surveillance campaign's failure was proof of its discriminatory nature.[137] In a separate case, the Assistant Chief of the NYPD Intelligence Unit had testified that the surveillance campaign "never led to a single lead or investigation."[138] In other words, the fact that the program never produced a single criminal lead proved that it was not based on a reasonable suspicion of wrongdoing.[139] The District Court dismissed the suit, finding that the plaintiffs lacked standing and had failed to state a claim.[140] Instead of discrimination, the court reasoned, the "more likely explanation" for the surveillance was "a desire to locate budding terrorist conspiracies."[141] The Third Circuit reversed, finding injury sufficient for standing in the "indignity" of the government creating special burdens on the basis of religion.[142] The court then applied a heightened standard of review and found that the plaintiffs plausibly alleged intentional discrimination based on religious affiliation.[143] The Third Circuit rejected the City's national security and public safety concerns and, citing *Korematsu*, noted that "it is often where the asserted interest appears most

133. *See* Hassan v. City of N.Y., 804 F.3d 277, 286–87 (3d Cir. 2015).
134. *See* Apuzzo, *supra* note 93.
135. Hassan v. City of N.Y., No. 12-cv-3401, 2014 WL 654604 (D.N.J. Feb. 20, 2014).
136. *See Hassan*, 804 F.3d at 295.
137. *Hassan*, 804 F.3d at 296.
138. SHAMAS & ARASTU, *supra* note 94, at 9.
139. *Id.*
140. *Hassan*, 2014 WL 654604, at *1.
141. *Id.* at *7.
142. *Hassan*, 804 F.3d at 289.
143. *Id.* at 307.

compelling that we must be most vigilant in protecting constitutional rights."[144]

The City settled, committing to several important policy changes. In addition to agreeing not to engage in suspiciousness surveillance on the basis of religion or ethnicity, the City agreed to attend a public meeting with the plaintiffs, pay damages for lost income as a result of the surveillance, and solicit plaintiff input to a "first-ever" Policy Guide, which would govern the Intelligence Unit's activities and be publicly available.[145] Although the litigation forced the City to make significant concessions, it was clear that the American Muslim community in the Tri-State Area would have had a harder time fighting unlawful global surveillance without judicial recourse.[146]

D. *Conclusion*

Before September 11, 2001, American Muslims were stereotyped and vilified during times of national crisis.[147] After 9/11, they were considered "a presumptive threat to the nation's security."[148] This extreme othering prevailed over due process, effectively stripping American Muslims of their right to a presumption of innocence until proven guilty.[149] As a test case for global surveillance, the choice of community made sense: society is more willing to accept aggressive measures when they target "small and politically disempowered groups."[150] But, as some prescient commentators noted as far back as 2002, aggressive measures

---

144. *Id*. at 306–07.

145. Stipulation of Settlement at 5–11, *Hassan*, 2014 WL 654604.

146. Years after the settlement, while running for President, former New York City Mayor, Michael Bloomberg, continued to defend the surveillance program, saying "We had just lost 3,000 people at 9/11. Of course we're supposed to do that[.]" Bobby Allyn, *'We're Supposed to Do That': Bloomberg Defends NYPD's Spying of Muslims After 9/11*, NPR (Feb. 27, 2020), https://www.npr.org/2020/02/27/810181314/we-re-supposed-to-do-that-bloomberg-defends-nypd-s-spying-of-muslims-after-9-11 [https://perma.cc/XDW5-NX9A].

147. *See* Ali, *supra* note 89, at 1034–35.

148. *Id*. at 1032.

149. *See id*. at 1049. Some writers have argued that denying American Muslims aspects of citizenship is merely a primer for an organized movement attempting to deprive American Muslims of their legal rights on the basis of their religion. This movement is evinced by the coordinated legislative proposals banning the consideration of Islamic law in federal and state courts and campaigns against mosque building. *See e.g.*, OK CONST. amend. Save Our State (2010) *invalidated by* Awad v. Ziriax, 670 F.3d 1111 (10th Cir. 2012) (holding that the amendment discriminated among religions and failed strict scrutiny); United States v. Rutherford Cty., Tenn., No. 3:12-0737, 2012 WL 2930076 (M.D. Tenn. July 18, 2012) (granting a temporary restraining order enjoining Rutherford County to process the Islamic Center of Murfreesboro's request for an occupancy certificate).

150. Akram & Johnson, *supra* note 76, at 300.

have ripple effects.[151] Global surveillance against a vilified community without suspicion bred global surveillance against everyone without suspicion.

Precluded from wielding political influence by their religious and ethnic identities, the plaintiffs in the NYPD litigation turned to the courts to enforce the legal protections guaranteed to them under the U.S. Constitution. Although they ultimately prevailed in the Third Circuit, the plaintiffs initially lost in the District Court for failing to establish standing. The current interpretation of standing doctrine poses one of the most serious hurdles for surveillance plaintiffs. Part III proposes reforming standing doctrine to allow more eligible plaintiffs to challenge global surveillance.

III. REFORMING STANDING DOCTRINE FOR SURVEILLANCE CASES THROUGH FEDERAL LEGISLATION: A POLITICAL AND JUDICIAL SOLUTION

The American Muslim community's litigation victories against government surveillance suggest a way forward through the courts. But legal challenges to global surveillance often falter at standing. This Part proposes a private right of action defining the requirements for Article III standing in surveillance cases so that would-be plaintiffs with meritorious claims can proceed to the merits.

A. *Legal Challenges to Global Surveillance Often Fail to Establish Injury-in-Fact and Causation Sufficient for Standing*

In a series of cases beginning in 2006, civil liberties organizations filed suits challenging FISA § 702, Executive Order 12,333, and their attendant surveillance programs.[152] These challenges were largely unsuccessful because courts imposed a standing threshold that plaintiffs could rarely meet. To satisfy Article III standing, a plaintiff must (1) establish an injury-in-fact that is concrete and particularized as well as actual and imminent; (2) show that the injury is fairly traceable to the challenged action; and (3) show that the injury is redressable with a favorable decision.[153] The lower court decisions culminated in the Supreme Court's

151. *Id.*

152. *See, e.g.*, ACLU v. Nat'l Sec. Agency, 438 F. Supp. 2d 754 (E.D. Mich. 2006), *vacated,* 493 F.3d 644 (6th Cir. 2007); Al-Haramain Islamic Foundation, Inc. v. Bush (*Al-Haramain I*), 507 F.3d 1190 (9th Cir. 2007); Al-Haramain Islamic Foundation, Inc. v. Obama (*Al-Haramain II*), 705 F.3d 845 (9th Cir. 2012).

153. *See generally* Lujan v. Defs. of Wildlife, 504 U.S. 555 (1992).

ruling in *Clapper v. Amnesty International*, which exemplifies the standing problems for plaintiffs challenging government surveillance.[154]

In *Clapper*, a collection of civil rights, media, labor, and legal organizations filed suit on the day the FISA Amendments Act (FAA) was enacted, arguing that the FAA was unconstitutional and seeking a permanent injunction.[155] The plaintiffs argued two injuries. The first was a future, Fourth Amendment injury: an "objectively reasonable likelihood" that their communications with clients would be intercepted under § 702 based on the clients' locations and personal characteristics.[156] The second was a present, First Amendment injury: as a result of the likely interception of their communications, and pursuant to their professional obligation to keep certain communications confidential, the plaintiffs had stopped communicating by phone and email and taken "costly and burdensome measures" to protect the confidentiality of certain communications.[157] In other words, the plaintiffs experienced a chilling effect because they believed that their communications would be subject to surveillance.

The Court found that the plaintiffs had failed to establish standing for their future, Fourth Amendment injury because their "highly speculative" claim fell far short of the majority's "certainly impending" requirement.[158] The Court invoked an attenuated chain of causation to hold that plaintiffs had not shown: 1) that the government intended to target their communications with their clients; 2) that it would do so under § 702; 3) that the FISC would authorize this proposed surveillance program; 4) that the government would succeed in intercepting the communications; and 5) that plaintiffs would be party to the intercepted communications.[159] The Court held that without facts to prove this full chain, plaintiffs failed to show that their future, threatened injury was "certainly impending" and that it was fairly traceable to the FAA.[160]

Unpersuaded that the plaintiffs' future, Fourth Amendment claim of surveillance was sufficiently concrete, the Court refused to consider their present, First Amendment injury of chilled speech and costs sustained to protect the confidentiality of their communications.[161] Justice Alito minced no words: "Because they do not face a threat of certainly

---

154. Clapper v. Amnesty Int'l, 133 S. Ct. 1138 (2013) (referring to § 702 as codified at 50 U.S.C. 1881a).

155. *Id.* at 1140.

156. *Id.* at 1147.

157. *Id.* at 1146.

158. *Id.* at 1143, 1148.

159. *Id.* at 1148.

160. *Id.* at 1148.

161. *Id.* at 1151.

impending interception under § 1881a [§ 702], their costs are simply the product of their fear of surveillance, which is insufficient to create standing."[162]

The Court made much of the fact that plaintiffs' "highly speculative" claims rested on "no actual knowledge of the Government's [§ 702] targeting practices."[163] This is, of course, exactly the problem with challenges to secret government surveillance programs: their details are not frequently publicized and notice provisions are enforced in exceedingly narrow circumstances.[164] The Court's decision in *Clapper* made it impossible for a plaintiff to proceed to discovery and obtain information that could substantiate plausible allegations of unlawful surveillance.

If the Court thought it had laid the matter to rest, it was wrong. Some three months later, the Guardian reported on the secret FISC order requiring Verizon to turn over all call records to the NSA on a daily basis.[165] This information offered a path forward for Fourth Amendment challenges to FISA § 702 and Executive Order 12,333 surveillance. Relying on the leaked documents, victims of the leaked surveillance programs argued the Fourth Amendment injury that their communications had been unlawfully intercepted by the government.[166]

In one such challenge to the NSA's bulk collection of telephone metadata in cooperation with Verizon, a District Court found that the plaintiffs' status as Verizon customers during the period of the FISC order was "strong evidence" that their data had been collected.[167] The more information plaintiffs could furnish, the better. The Ninth Circuit was persuaded that a class of AT&T customers in San Francisco alleged "concrete harms," in part because they could describe in detail the specific facility and equipment the NSA used to obtain AT&T's telephone and internet records.[168] Similarly, the Second Circuit clarified that collection was sufficient for standing and that a plaintiff did not have to prove that the government reviewed the collected information to establish injury.[169] The Second Circuit then considered the merits of the NSA's telephone

---

162. *Id*. at 1141.

163. *Id*. at 1148.

164. *See supra* Part I.A.ii.

165. Greenwald, *supra* note 1.

166. *See* Klayman v. Obama, 957 F.2d 1, 7 (D.D.C. 2013) (holding that plaintiffs established standing because they were Verizon subscribers during the period of the FSIC order).

167. *Id*. at 26.

168. Jewel v. Nat'l Sec. Agency, 673 F.3d 902, 908, 910 (9th Cir. 2011). For more on the NSA's "unique and especially productive" relationship with AT&T, see Julia Angwin, Jeff Larsen, Charlie Savage, James Risen, Henrik Moltke & Laura Poitras, *NSA Spying Relies on AT&T's 'Extreme Willingness to Help*,' PROPUBLICA (Aug. 15, 2015), https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help [https://perma.cc/792J-JBCJ].

169. ACLU v. Clapper, 785 F.3d 787, 801 (2d. Cir. 2015).

metadata collection program, holding that the agency exceeded its statutory authority under FISA.[170]

This post-*Clapper* line of cases offers two important takeaways. The first is that federal courts are willing to grant standing for Fourth Amendment injuries if plaintiffs can show that their own communications were collected by the government. The second is that once plaintiffs establish standing, they have a chance at a favorable merits decision.[171]

B. *A Private Right of Action Will Offer More Would-Be Plaintiffs Relief Without Opening the Floodgates to Frivolous Litigation*

The problem is, of course, that not every unlawfully surveilled plaintiff can show that their own communications were collected by the government through specific surveillance programs. Government surveillance is secret by nature and statutory notice provisions, where they exist, are weak. The size and scope of the surveillance infrastructure revealed through the Snowden leaks suggest that we have glimpsed only a small part of a much bigger iceberg. Throwing out plaintiffs with plausible allegations for failing to meet an artificially high standing threshold shields the government from judicial scrutiny and denies plaintiffs their day in court. Clearly, reform is required.

This Part proposes a private right of action that would enable more meritorious challenges to government surveillance than the current doctrine provides for. The private right of action would grant standing to any person who (1) has a reasonable fear of surveillance based on the acknowledged activities of the government, and (2) may reasonably incur costs to mitigate or avoid harm as a result of that fear. While the proposed private right of action would help would-be plaintiffs in general, it would be especially helpful to minority plaintiffs, including American Muslims.

---

170. *Id*. at 821.

171. This paper's focus on standing should not suggest that standing is the only threshold obstacle to surveillance challenges. The state secrets doctrine is a separate and sometimes insurmountable obstacle to plaintiffs. *See, e.g.*, Al-Haramain Islamic Foundation, Inc. v. Bush, 451 F. Supp. 2d 1215 (D. Or. 2006) (holding that the classified government document the plaintiffs relied on for standing was protected by the state secrets privilege), *rev'd*, *Al-Haramain I*.

1. Congress Has the Authority to Create This Private Right of Action.

It is well-established that Congress can make certain harms the basis for legal action.[172] Under the Court's recent decision in *TransUnion LLC v. Ramirez*, Congress may elevate for judicial cognizance only those harms that have "a close historical or common law analogue."[173] Physical and monetary harms easily qualify, as do certain intangible harms, including "reputational harms, disclosure of private information, and intrusion upon seclusion."[174] Rather than create a new justiciable harm, this Note's proposed private right of action offers a different way to assess a longstanding basis for legal action.

Both the common law and the Constitution recognize harms relating to the invasion of privacy. For example, the common law tort of intrusion upon seclusion is defined as the intentional intrusion (physical or otherwise) "upon the solitude or seclusion of another or his private affairs or concerns."[175] This includes opening a person's mail, wallet, and bank accounts.[176] Liability for such conduct attaches even without publication of the private information.[177] Such a definition clearly includes surveillance programs that collect private information, whether metadata or content. This conduct is also clearly covered by the Fourth Amendment's prohibition on unreasonable search and seizure.[178] The Court has long recognized that the Fourth Amendment protects people's privacy from governmental intrusion, including across modern forms of private communication.[179] Accordingly, it is well within Congress's authority to create the proposed private right of action, which merely offers a different way to assess an established harm.

Additionally, rather than apply a new standing test to future threatened injuries, the proposed private right of action applies the Court's existing standard. The proposed standard's "reasonable fear" language

---

172. TransUnion LLC v. Ramirez, 141 S. Ct. 2190, 2204–05 (2021) ("[C]ongress may 'elevate to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law.'").

173. *Id*. at 2204.

174. *Id*.

175. RESTATEMENT (SECOND) OF TORTS § 652B (AM. L. INST. 1977).

176. *Id*.

177. *Id*.

178. *See, e.g.*, Jewel v. Nat'l Sec. Agency, 673 F.3d 902, 906, 908, 910 (9th Cir. 2011) (finding that plaintiff alleging that the NSA collected the content of AT&T customers' "phone calls, emails, instance messages, text messages, web communications, and other communications" had standing for her Fourth Amendment claim).

179. *See* Katz v. United States, 88 S. Ct. 507, 510–11 (1967) (noting that while the Fourth Amendment "protects individual privacy against certain kinds of governmental intrusion," several other constitutional provisions protect individual privacy.).

and focus on costs combine two of the Court's standing tests for future injuries. In footnote five, the *Clapper* court noted that plaintiffs may show standing based on a "substantial risk" of harm that prompts them to "reasonably incur costs to mitigate or avoid that harm."[180] The Court applied that standard in *Susan B. Anthony List v. Dreihaus*, holding that the petitioner organization had standing because it showed a substantial risk that the Ohio Elections Commission would undertake enforcement proceedings against it based on the Commission's history of past enforcement and the organization's stated intentions to continue its challenged conduct.[181] The Court has also applied a "reasonable fear" test to assess plaintiffs' claims of future harm.[182] In *Friends of the Earth, Inc. v. Laidlaw Environmental Services (TOC), Inc.*, the Court applied a "reasonable fear" standard to find that a group of environmental organizations had standing to seek injunctive relief against a hazardous waste incinerator facility with a record of dumping toxic chemicals in unlawful quantities into a local river.[183] Both the "substantial risk" and "reasonable fear" standards invite a court to consider the plaintiff's context in assessing the likelihood of the alleged injury and its harms. By combining "reasonable fear" with incurred costs, the proposed standard aims to encourage a more holistic injury-in-fact analysis that weighs both the risk of the harm as well as its magnitude.[184] In this way, the proposed standard would admit would-be plaintiffs with meritorious claims to a merits analysis, rather than punishing them for failing to prove facts about secret government surveillance programs.

2. The Proposed Standard is Better Suited to the Surveillance Context, Would Benefit Minority Communities, and Would Bolster the Government's Legitimacy

The proposed standard confers standing on would-be plaintiffs with meritorious claims while still imposing reasonable bounds on who may bring suit. It does so in two ways. First, it establishes a route to standing for harms precluded by the "certainly impending" standard. Under the proposed standard, a plaintiff could show standing for present, First Amendment injuries by focusing on the chilling effect of sur-

180. Clapper v. Amnesty Int'l, 133 S. Ct. 1138, 1150 n.5 ((2013).

181. *See* Susan B. Anthony List v. Dreihaus, 134 S. Ct. 2334, 2342–46 (2014).

182. Friends of the Earth, Inc. v. Laidlaw Env't Services (TOC), Inc., 528 U.S. 167, 176, 183–85 (2000).

183. *Id.*

184. *See* Andrew C. Sand, Note, *Standing Uncertainty: An Expected-Value Standard for Fear-Based Injury in Clapper v. Amnesty International USA*, 113 MICH. L. REV. 711, 730 (2015).

veillance (reasonable fear) and the attendant costs such a chilling effect might produce (reasonably incurred costs). This approach is grounded in an older, established tradition of First Amendment jurisprudence that imposed a less restrictive standard of justiciability and refused to balance national security against constitutionally protected speech.[185] Plaintiffs could also show standing for future, threatened Fourth Amendment injuries because the proposed standard's "reasonable fear" prong is more easily satisfied than "certainly impending," especially before discovery. A court might find fear reasonable by looking to social, historical, or political facts, including the characteristics of the plaintiff, the nature of the targeted communication, or the admitted activities of the government. While the proposed standard invites context, it avoids exposing courts to a deluge of claims by binding the standing showing to admitted activities of the government. This creates a zone of inference around acknowledged activities that ensures such challenges are rooted in commonly agreed-upon facts.

Second, the proposed standard is more likely to admit surveillance plaintiffs with meritorious claims to a merits analysis than the "certainly impending" standard because it more accurately fits the surveillance context.[186] The requirement that a plaintiff show that their own communications were collected comes from the foundational case of *Rakas v. Illinois*.[187] But the stark differences between *Rakas* and a surveillance challenge should preclude importing the *Rakas* test into the surveillance arena. *Rakas* involved the narrow context of criminal defendants seeking to suppress evidence obtained during a car search where the defendants owned neither the evidence nor the car.[188] In denying the defendants' motion, the Court held that Fourth Amendment can be asserted only by the individual "whose own protection was infringed by the search and seizure."[189] Whereas *Rakas* involved a challenge to a specific search or seizure clearly targeting a discrete set of people, *Clapper* and its ilk challenge global surveillance programs whose programmatic nature and permissive targeting procedures ensure that they are not aimed at any specific person, and whose status as national security tools ensure that they are shrouded in secrecy.[190] Rather than rely on an inappropriate analogy to physical searches, the proposed standard cap-

185. *See* Jeffrey L. Vagle, Laird v. Tatum *and Article III Standing in Surveillance Cases*, 18 U. PA. J. CONST. L. 1055, 1061 (2016).

186. *See* Michael C. Miller, Note, *Standing in the Wake of the Terrorist Surveillance Program: A Modified Standard for Challenges to Secret Government Surveillance*, 60 RUTGERS L. REV. 1039, 1069 (2008).

187. Rakas v. Illinois, 493 U.S. 128, 132 (1978).

188. *Id.* at 130.

189. *Id.* at 138–39 (quoting Simmons v. United States, 390 U.S. 337, 389 (1968)).

190. *See* Miller, *supra* note 186, at 1069.

tures the real dynamics of surveillance and makes them grounds to show standing. In doing so, the proposed standard will more accurately identify meritorious challenges to global surveillance.

The proposed standard would also be a boon to minority communities, especially the American Muslim community. In *Friends of the Earth*, the Court found that the plaintiffs' fear of toxic pollution was reasonable, given the defendant's history of repeatedly polluting the river. [191] A court applying the proposed standard could similarly consider important contextual questions precluded by the "certainly impending" test. Does the government have a history of surveilling people who share that plaintiff's background, including race, religion, ethnicity, national origin, sexual orientation, gender identity, or political ideology? Is the plaintiff a member of a community stigmatized by the current socio-political climate? Could the plaintiff reasonably be the target of acknowledged surveillance programs? These questions are particularly important for minority plaintiffs because they invite the court to consider multiple layers of context that more accurately describe the dynamics around heightened government surveillance than a test that only considers hard proof.

A final benefit of the proposed standard is that it bolsters the government's legitimacy and the separation of powers. Empowering plaintiffs to challenge government surveillance ensures that the government is held to its own constitutional obligations. The proposed standard also upholds the separation of powers by maintaining the courts' check on the political branches through judicial review of global surveillance. Finally, the proposed standard advances democratic principles by putting the burden on Congress rather than the courts to decide who has standing to challenge surveillance programs. As a national security tool, surveillance is a touchy political subject. Judges ruling one way or the other are subject to accusations of offering the government impunity for its abuses or robbing the nation of essential defense mechanisms. By having Congress set the standing requirements for surveillance challenges, the proposed standard relocates accountability for surveillance programs from the courts to the political branches.

There is a rich body of literature suggesting reforms to surveillance law. But this Note's focus on the American Muslim community suggests a need for a broad, political solution. Statutory amendments to FISA—including to the notice provision,[192] the FISC,[193] or the targeting proce-

191. *See* Friends of the Earth, Inc. v. Laidlaw Env't Services (TOC), Inc., 528 U.S. 167, 176, 183–85 (2000).

192. *See* Correia, *supra* note 53.

dures[194]—would have no effect on the surveillance programs authorized by non-FISA authorities, including Executive Order 12,333. Increasing the government's reporting requirements[195] or empowering internal civil rights offices[196] will not produce the intensity of external pressure necessary for change. And while many of these reforms are academic in nature,[197] the proposed standard is practical. Though a citizen suit provision can be controversial, the proposed standard's focus on fighting surveillance abuse could inspire a bipartisan coalition spanning progressives advocating for minority rights and conservatives concerned with privacy and government overreach. Rather than haggle over another surveillance reauthorization bill, Congress should take meaningful action and empower would-be plaintiffs to hold the government to its constitutional promises.

CONCLUSION

Legal challenges to global surveillance are stymied at standing. Most plaintiffs lack standing because they cannot show that their communications were collected by secret surveillance programs. But courts are crucial partners in the fight against global surveillance because they check the political branches. This role is especially important to plaintiffs from minority communities that do not wield political power.

To enable more would-be plaintiffs with meritorious claims to survive the standing inquiry, Congress should create a private right of action that defines the injury and causation required for surveillance challenges. Returning to a "reasonable fear" standard for future threatened injuries would more accurately capture the dynamics of surveillance while limiting challenges to those based on acknowledged governmen-

193. *See, e.g.*, Alex Kimata, Note, *Section 702 Malfisance*, 16 COLO. TECH. L.J. 455 (2017); Deborah Samuel Sills, *Certified Question Jurisdiction: A Significant New Authority for the FISA Court and FISA Court of Review*, 5 NAT'L SEC. L.J. 1 (2016); Peter Margulies, *Dynamic Surveillance: Evolving Procedures in Metadata and Foreign Content Collection After Snowden*, 66 HASTINGS L.J. 1 (2014); Menno Goedman, *The Power to Appoint FISA Judges: Evaluating Legislative Proposals to Reform to U.S.C. § 1803 and Improve the Surveillance Court*, HARV. J. LEGIS. 365 (2014).

194. *See* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117 (2015); Donohue, *supra* note 41.

195. *See* Butler, *supra* note 12 at 83.

196. *See, e.g.*, Margo Schlanger, *Intelligence and Legalism and the National Security Agency's Civil Liberties Gap*, 6 HARV. NAT'L. SEC. J. 112 (2015).

197. *See, e.g.*, Nicole B. Casarez, *The Synergy of Privacy and Speech*, 18 UNIV. PENN. J. CONST. L. (2016) (arguing that while neither the First nor the Fourth Amendment alone offers sufficient protection against covert government surveillance programs, they mutually reinforce each other's protections); William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633 (2010) (arguing for rebuilding the FISA regime from the ground up).

tal activities. Under this standard, plaintiffs would be free to allege chilling effects as present, First Amendment injuries and future, Fourth Amendment injuries. The proposed private right of action would help force a more complete reckoning of the widespread surveillance abuses conducted under FISA and Executive Order 12,333 and spur reform to avoid future surveillance abuse.