Maryland Law Review

Volume 79 | Issue 1 Article 7

Protecting First Amendment Rights in the Fight Against Disinformation: Lessons Learned from FISA

Jill I. Goldenziel

Manal Cheema

PROTECTING FIRST AMENDMENT RIGHTS IN THE FIGHT AGAINST DISINFORMATION: LESSONS LEARNED FROM FISA

JILL I. GOLDENZIEL* & MANAL CHEEMA**

I. INTRODUCTION

Protecting national security, especially in a time of crisis, can come at a cost to Americans' civil liberties. The U.S. government must make difficult choices between implementing the strongest possible protections from foreign threats and preserving Americans' constitutional freedoms at home. Irreparable violations to civil rights can and have occurred from striking the wrong balance.[1] In a time of indefinite war against unconventional adversaries, the balance between protecting national security and preserving civil liberties is of utmost importance.

As the new "endless war" shifts from the war on terror to the information domain,[2] Congress must enable the United States to fight enemy information warfare while protecting the rights to privacy and freedom of speech and information.[3] Congress has had some recent experience crafting legislation to balance national security with these constitutional rights: The Foreign Intelligence Surveillance Act ("FISA").[4] FISA, initially passed in

* Associate Professor of International Law and International Relations, Marine Corps University-Command and Staff College; Affiliated Senior Scholar, University of Pennsylvania Fox Leadership International Program. Thanks to Mark Graber and Michael Pine. Errors are our own. Views expressed in this Article are the authors' own and do not necessarily reflect the position of the Department of Defense or any other arm of the U.S. government.

** J.D. Candidate 2020, University of Virginia School of Law. I am thankful for the support and encouragement of my family and friends. Errors are our own.

1. *See, e.g.*, Korematsu v. United States, 319 U.S. 432, 435–36 (1943) (allowing Japanese Americans to be detained because they did not vacate their homes after being excluded by executive order).

2. President George W. Bush coined the term "War on Terror" shortly after September 11, 2001. Remarks on Arrival at the White House and an Exchange with Reporters, 2 PUB. PAPERS 1114–16 (Sept. 16, 2001). The term would come to be used to refer to U.S. military actions in Iraq and Afghanistan and to fight terrorism all over the world. As of this writing, American military presence in Iraq and Afghanistan is winding down. Focus has shifted to information warfare. For example, the U.S. Marine Corps established information as a warfighting function in January 2019. ROBERT B. NELLER, COMMANDANT OF THE MARINE CORPS, MARINE CORPS BULLETIN 5400 (Jan. 17, 2019), https://www.marines.mil/portals/1/Publications/MCBUL%205400.pdf?ver=2019-02-06-082807-103.

3. *See* U.S. CONST. amend. V and amend. IX (privacy); U.S. CONST. amend. I (free speech).

4. 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 (2001).

1978, was modified significantly after the 9/11 terrorist attacks. FISA provoked robust debate in the national security community, prompting several amendments to its provisions,[5] specifically those contained in the FISA Amendments Act of 2008 ("FAA")[6] and the FISA Amendments Reauthorization Act of 2017.[7]

Lessons learned from debates over FISA can inform legislation that would balance national security and First Amendment rights in the fight against information warfare. FISA is an example of Congress's attempt to thread the same needle that any response to foreign disinformation campaigns must: allowing surveillance of foreign agents without unduly infringing on the First Amendment rights of U.S. persons ("USPERs"). This Essay will argue that FISA can serve as a framework for balancing the government's need to access USPERs' First Amendment-protected information to combat information warfare with USPERs' constitutional rights.[8]

To preserve civil liberties, Congress must ensure that federal agencies access USPERs' First Amendment-protected information solely for narrowly tailored national security purposes.[9] Congress should mandate that government agencies use only open-source data on USPERs whenever sufficient open-source data is available and when time permits given the urgency of any particular national security concern.[10] If an agency cannot meet those two requirements without risking its goal(s), Congress should require the agency to obtain a court order or warrant to conduct prospective surveillance of USPERs' communications.[11]

FISA can serve as a framework for constitutional protections of U.S. civil liberties in the context of fighting information warfare. To sanction government surveillance under FISA, a judge must find probable cause that

5. *See, e.g.*, Chris Inglis & Jeff Kosseff, *In Defense of FAA Section 702: An Examination of Its Justification, Operational Employment, and Legal Underpinnings*, LAWFARE (Apr. 26, 2016, 7:31 AM), https://www.lawfareblog.com/defense-faa-section-702-examination-its-justification-operational-employment-and-legal-underpinnings (arguing in favor of § 702 of the FAA); Faiza Patel & Elizabeth Goitein, *Fixing the FISA Court by Fixing FISA: A Response to Carrie Cordero*, LAWFARE (Apr. 8, 2015, 12:18 PM), https://www.lawfareblog.com/fixing-fisa-court-fixing-fisa-response-carrie-cordero (arguing that "FISA became an existential threat to the Fourth Amendment's warrant requirement in ordinary criminal cases" when the FISC abandoned the "primary purpose test"); Benjamin Wittes, *Yeah, But Is It a Good Bill? Thoughts on the Leahy FISA Reform Proposal*, LAWFARE (July 30, 2014), https://www.lawfareblog.com/yeah-it-good-bill-thoughts-leahy-fisa-reform-proposal (considering whether proposed Senate reforms were "worth pursuing").

6. FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

7. FISA Amendments Reauthorization Act of 2017, Pub. L. No. 115-118, 132 Stat. 3 (2018) (codified at 50 U.S.C. § 1801) [hereinafter 2017 Amendments].

8. This Essay expands on our introduction of this argument in the article Jill I. Goldenziel & Manal Cheema, *The New Fighting Words?: How U.S. Law Hampers the Fight Against Information Warfare*, 22 U. PA. J. CONST. L. 81, 136–37 (2019).

9. *Id*. at 48.

10. *Id*.

11. *Id*.

the target is a foreign power or agent of a foreign power and/or probable cause that the target uses a particular facility.[12] The court cannot accept the government's assertion that someone is an agent of a foreign power based solely on their First Amendment activities.[13] Instead, "a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target."[14] However, under FISA Section 702,[15] when the government is surveilling foreign actors overseas, it may incidentally collect information about or communications of USPERs with whom potential foreign targets communicate.[16]

These First Amendment protections that FISA provides for USPERs can be a useful model for legislation to enable the United States to combat information warfare, combined with additional safeguards suggested by FISA's critics. Specifically, to protect the First Amendment, Congress should require procedures similar to FISA's when open-source information is unavailing. First, the government should obtain a court order or warrant under probable cause, based on something more than First Amendment activities. Second, where the government incidentally collects the information of USPERs, the government should adopt and follow minimization procedures to prevent the misuse and retention of that data. Any legislation relaxing surveillance restrictions on USPERs to combat information warfare should also be subject to extensive oversight from the Department of Justice, Congress, and the Foreign Intelligence Surveillance Court ("FISC"), similar to the oversight program in place for FISA Section 702.[17]

This Essay will proceed in the following parts. Part I will provide a brief overview of the challenges of responding to disinformation campaigns. Part II will provide background on the political and legal landscape that drove the development of FISA. Part III will explain how electronic surveillance orders are applied for and obtained under FISA and how FISA succeeds and fails in providing protections for civil liberties in traditional surveillance and Section 702 bulk data surveillance. Part IV then will discuss how a warrant requirement is critical for protecting First and Fourth Amendment interests in any surveillance operation. Finally, Part V will explain how lessons

12. 50 U.S.C. § 1805(a)–(b) (2012).

13. *Id*. § 1805(a)(2)(A); *see* United States v. Aziz, 228 F. Supp. 3d 363 (M.D. Pa. 2017); United States v. Rosen, 447 F. Supp. 2d 538, 548–51 (E.D. Va. 2006) (finding a judge can rely in part on these activities as long as there is probable cause that the target may be involved in unlawful clandestine activities).

14. 50 U.S.C. § 1805(b).

15. 50 U.S.C. § 1881a (2012 & Supp. V 2018).

16. The FISA definition of a USPER is broader than just a U.S. citizen. Under § 1801(i), a USPER is a citizen, a lawful permanent resident ("LPR"), an unincorporated association where a substantial number of members are citizens or LPRs, and so on. 50 U.S.C. § 1801(i) (2012).

17. 50 U.S.C. § 1881a (2012 & Supp. V 2018).

learned from FISA should inform legislation designed to address disinformation campaigns meant to influence the electoral process.

A. The Challenge of Responding to Disinformation Campaigns

In 2016, Russian actors and other non-USPERs used the informational and organizational capabilities of social media to influence the U.S. presidential election. According to the Intelligence Community Assessment of Russian actions, Russia's interference in the 2016 election was its "[b]oldest [y]et," aimed to "undermine public faith in the U[.]S[.] democratic process."[18] Russia is attempting to influence the 2020 election[19] with similar covert actions intended to "sow division in our society, undermine confidence in our democratic institutions, and otherwise affect political sentiment and public discourse to achieve strategic geopolitical objectives."[20]

Russian information campaigns utilized paid advertisements, false stories, and divisive propaganda to carry out their goals.[21] As many as 126 million Facebook users, representing almost forty percent of the U.S. population, were exposed to content promulgated by Russian actors.[22] Social media companies, regulatory agencies, Congress, and the general public continue to debate[23] how to curtail foreign interference in the democratic process, preserve the integrity of the political process, and retain critical civil liberties protections.

The 2017 U.S. National Security Strategy characterizes the United States response to enemy information warfare as "tepid and fragmented."[24] One reason is that U.S. laws and jurisprudence protecting free speech and privacy do not reflect modern technological realities. First Amendment doctrine, the Privacy Act of 1974, and related laws hinder the U.S. response to information campaigns.[25] In particular, the Privacy Act and other Cold War-

18. OFFICE OF THE DIR. OF NAT'L INTELLIGENCE, INTELLIGENCE COMMUNITY ASSESSMENT: ASSESSING RUSSIAN ACTIVITIES AND INTENTIONS IN RECENT US ELECTIONS 1, 5 (2017), https://www.dni.gov/files/documents/ICA_2017_01.pdf.

19. Josh Gerstein, *U.S. Brings First Charge for Meddling in 2018 Midterm Elections*, POLITICO (Oct. 19, 2018, 4:43 PM), https://www.politico.com/story/2018/10/19/first-criminal-case-filed-over-russian-interference-in-2018-midterms-916787.

20. U.S. DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE 1 (July 2, 2018), https://www.justice.gov/ag/page/file/1076696/download; *see also* Goldenziel & Cheema, *supra* note 8, at 84.

21. Goldenziel & Cheema, *supra* note 8, at 87.

22. *Social Media Influence in the 2016 U.S. Election Before the S. Select Comm. on Intelligence*, 115th Cong. 13 (2017) (prepared statement of Colin Stretch, General Counsel, Facebook).

23. *Once Considered a Boon to Democracy, Social Media Have Started to Look Like Its Nemesis*, ECONOMIST (Nov. 4, 2017), https://www.economist.com/briefing/2017/11/04/once-considered-a-boon-to-democracy-social-media-have-started-to-look-like-its-nemesis.

24. WHITE HOUSE, NATIONAL SECURITY STRATEGY OF THE UNITED STATES OF AMERICA 35 (2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf.

25. Goldenziel & Cheema, *supra* note 8, at 84.

era surveillance laws do not allow the collection of USPERs' data that would adequately enable the government to assess the extent of information campaigns and fight them.

Laws restricting collection on USPERs need to be relaxed, while still maintaining appropriate safeguards for civil liberties, to allow the United States to combat enemy information warfare effectively.[26] Preserving the integrity of the electoral process is a national security interest that itself involves a First Amendment right. However, legislation must appropriately balance this national security interest with other civil liberties concerns.[27] One mechanism for achieving this balance is reforming surveillance laws to allow government agencies to surveil USPERs under a narrowly tailored national security exception with appropriate constitutional safeguards.[28] At the same time, legislation must remain flexible enough to allow agencies to move "quickly to fight rapid and constantly changing information threats."[29]

Lessons learned from FISA and its amendments, which represent the last major attempt to reform surveillance laws for national security purposes, are crucial to developing such legislation. We argue that new legislation seeking to combat information warfare must exceed FISA's protections for constitutional liberties to preserve constitutional rights when allowing government surveillance of USPERs.

B. Why FISA Came to Be

Congress enacted FISA in the wake of abuses by the U.S. intelligence community that threatened the constitutional rights of U.S. citizens. Two events provoked Congress to pass FISA in 1978:[30] (1) the Supreme Court's decision in *United States v. U.S. District Court* ("*Keith*"),[31] and (2) the Church Committee reports.[32] First, in *Keith*, the Supreme Court considered Fourth Amendment requirements in domestic surveillance cases targeting an internal threat.[33] "The *Keith* Court recognized the Executive's power to obtain intelligence information through electronic surveillance . . . under the

26. *Id*. at 168.

27. *Id*. at 122.

28. *Id*.

29. *Id*. at 135.

30. Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978).

31. 407 U.S. 297 (1972) [hereinafter *Keith*].

32. The U.S. Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities, formed in 1975, was chaired by Idaho Senator Frank Church and became known as the "Church Committee." U.S. Senate Historical Office, *Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, https://www.senate.gov/artandhistory/history/common/investigations/ChurchCommittee.htm (last visited Sept. 28, 2019). The committee investigated intelligence abuses by the CIA, FBI, IRS, and other agencies. *Id*.

33. 407 U.S. at 309.

Article II Oath Clause."[34] However, due to the "convergence of First and Fourth Amendment values,"[35] the Court found that "the Clause, alone, is hardly sufficient to support warrantless surveillance merely on the basis of the foreign origin of the threat."[36] It also asserted that "Congress may wish to consider protective standards for [domestic security surveillance] which differ from those already prescribed for specified crimes in Title III."[37] The *Keith* decision encouraged the Executive and Congress "to find a legislative solution to the problem of warrantless searches."[38]

Second, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (the "Church Committee") described the domestic intelligence abuses by intelligence agencies and the military, which the executive had rationalized merely as foreign intelligence gathering.[39] The Senate created the Committee in the aftermath of Watergate and the disclosure of the Central Intelligence Agency's ("CIA") domestic and covert operations.[40] Among other abuses, the Committee investigated the CIA's assassination plots,[41] plans by a White House associate counsel to increase intelligence-gathering on Vietnam War protestors and other dissidents,[42] covert operations in Angola and Chile,[43] President Nixon's 1969 warrantless wiretapping of several journals and government employees,[44] and the National Security Agency's ("NSA") SHAMROCK program.[45] In considering these events, "[t]he Church Committee found that the [Federal Bureau of Investigation's ("FBI")] internal security and domestic intelligence programs compiled massive files on activities protected by the First Amendment and the political opinions of Americans."[46] Between 1975 and 1976,

34. William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 AM. U. L. REV. 1, 74 (2000) (footnote omitted); *see Keith*, 407 U.S. at 310.

35. *Keith*, 407 U.S. at 313.

36. Banks & Bowman, *supra* note 34, at 74; *see Keith*, 407 U.S. at 319–20.

37. *Keith*, 407 U.S. at 322.

38. Banks & Bowman, *supra* note 34, at 75.

39. S. REP. NO. 94-755, bk. II, at 6–7 (1976).

40. Marc B. Langston, *Rediscovering Congressional Intelligence Oversight: Is Another Church Committee Possible Without Frank Church?*, 2 TEX. A&M L. REV. 433, 436 (2015) (noting specifically the 1974 reports by Seymour Hersh in *The New York Times*).

41. *Id*. at 458.

42. *Id*. at 461.

43. *Id*. at 463.

44. *Id*. at 464.

45. *Id*. at 466. The program involved various private companies providing the NSA with Americans' international telegrams from 1947 to 1975. *Id*. at 468.

46. 147 CONG. REC. 20,672 (2001); *see also* Langston, *supra* note 40, at 474 (describing FBI's 2370 actions between 1956 and 1971 to harass dissidents within the United States and the FBI's plot to blackmail Dr. Martin Luther King Jr.).

the Church Committee published fourteen reports on U.S. intelligence agencies and provided recommendations to address their abuses.[47] The reports emphasized the absence of explicit congressional or judicial standards in the field of surveillance.[48] The Church Committee's disclosures shocked Americans, causing them to view their own government with new suspicion.[49]

As a result of these findings, Congress passed FISA in 1978 to constrain and impose judicial review on executive branch surveillance programs.[50] FISA legislation also created the FISC to review FISA applications, allowing the government to obtain intelligence while still protecting privacy and individual rights.[51] FISA was meant to ensure that "electronic surveillance for foreign intelligence" comported with the Fourth Amendment.[52] The 1978 Senate Intelligence Report to FISA ("Senate Intelligence Report") declared that Congress did not intend FISA to permit surveillance of lawful activities of American citizens, even those activities that are "secret and conducted for a foreign power."[53] The Senate Intelligence Report emphasized that individuals retain two freedoms. First, they must be free to communicate with "representatives of foreign governments or with foreign groups."[54] Second, they must be free from a chilling effect, that is, "free from any fear that such contact might be the basis for probable cause to believe they are acting at the direction of a foreign power thus triggering the [g]overnment's power to conduct electronic surveillance."[55]

This legislative history produced by the Senate Intelligence Report, which is the most widely accepted interpretation of FISA, makes it clear that legal protection extends only to the "*lawful* exercise of [F]irst [A]mendment

47. *See* Assassination Archives & Research Ctr., *Church Committee Reports*, http://www.aarclibrary.org/publib/church/reports/contents.htm (last visited July 13, 2019) (providing links to all fourteen reports).

48. Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 806–07 (1989) (describing the Church Committee's investigation and finding that "warrantless electronic surveillance had been used against United States citizens who were not readily identifiable as reasonable sources of foreign intelligence information"); *see also* Sharon H. Rackow, *How the USA Patriot Act Will Permit Governmental Infringement upon the Privacy of Americans in the Name of "Intelligence" Investigations*, 150 U. PA. L. REV. 1651, 1666 (2002).

49. Langston, *supra* note 40, at 474.

50. 147 CONG. REC. 20,673 (statement of Sen. Leahy).

51. Caitlin Thistle, Comment, *A First Amendment Breach: The National Security Agency's Electronic Surveillance Program*, 38 SETON HALL L. REV. 1197, 1201–02 (2008); *see also* ACLU Found. of So. Cal. v. Barr, 952 F.2d 457, 461 (D.C. Cir. 1992) (quoting S. REP. NO. 95-604, pt. 1, at 15 (1977)).

52. United States v. Falvey, 540 F. Supp. 1306, 1311 (E.D.N.Y. 1982).

53. S. REP. NO. 95-701, at 29 (1978).

54. *Id*.

55. *Id*.

rights of speech, petition, assembly, and association."[56] The Senate Intelligence Report stated that electronic surveillance might be appropriate if there is probable cause to believe that "foreign intelligence services [are] hid[ing] behind the cover of some person or organization in order to influence American political events and deceive Americans into believing that the opinions or influence are of domestic origin and initiative."[57] The Senate Intelligence Report predicted such deception would be "willfully maintained in violation of the Foreign Agents Registration Act," and could thus be prosecuted.[58] Thus, the Senate Intelligence Report contemplated that activities seeking to undermine or "influence American political events," such as elections, may be subject to surveillance, even if they implicate traditional First Amendment activities.[59]

II. THE FRAMEWORK OF FISA

FISA authorizes four investigative activities: (1) electronic surveillance;[60] (2) physical searches;[61] (3) pen register and trap and trace surveillance;[62] and (4) business records.[63] This Essay focuses on electronic surveillance, as defined in Section 1801(f), which is the primary method for surveillance to prevent and combat disinformation campaigns.

56. *Id*. (emphasis added). The 1978 Senate Judiciary Committee report and the House Intelligence Committee report on FISA seem to contradict the Senate Intelligence report. The Judiciary Committee report states that activities protected by the First Amendment may not "form *any part* of the basis" for identifying a FISA target. *See* S. REP. NO. 95-604, at 23 (1977) ("In no event may lawful political activity within the ambit of the protections afforded by the first amendment be the basis, or form any part of the basis, for finding that any individual is engaged in 'clandestine intelligence activities.'"). Likewise, the House Intelligence Committee Report emphasized that FISA "would not authorize surveillance of ethnic Americans who *lawfully* gather political information and perhaps even *lawfully* share it with the foreign government of their national origin." *See In re* Sealed Case, 310 F.3d 717, 739 (FISA Ct. Rev. 2002) (emphasis added) (quoting H. REP. NO. 95-1283, at 40 (1978)).

57. S. REP. NO. 95-701, at 29 (1978).

58. *Id*.

59. *Id*.

60. 50 U.S.C. §§ 1801–12 (2012); *see id*. § 1801(f)(1)–(4) (defining the four categories of electronic surveillance under FISA).

61. *Id*. §§ 1821–29. Congress amended FISA in 1994 to authorize physical searches of the "premises, property, information or material of a foreign power or agent of a foreign power" in the United States, conducted for the purpose of collecting "foreign intelligence information." Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, sec. 302(b), § 1882, 108 Stat. 3423, 3445 (1994) (codified as amended at 50 U.S.C. § 1822 (2012)).

62. 50 U.S.C. §§ 1842–46.

63. *Id*. §§ 1861–62. In 1998, Congress amended FISA to permit FBI use of pen registers and trap and trace devices and authorized FISA surveillance of business records. Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, sec 402, § 1842, 112 Stat. 2396, 2405 (1998) (codified as amended at 50 U.S.C. § 1842 (2012)).

A. Requesting and Obtaining Order

Section 1804(a)(1) through (9) describes the required contents of an application to conduct electronic surveillance under FISA. A federal officer must apply for a court order from the FISC, in writing and under oath, which must be approved by the Attorney General ("AG").[64] The application must identify or describe the specific target, and the AG must find that standard investigation cannot reasonably obtain the information.[65] In a FISA application, a federal officer must: (1) provide statements of facts and circumstances that justify the officer's belief that the person is a foreign power or an agent of a foreign power;[66] (2) list the facilities or places that the target is allegedly using;[67] and (3) describe the nature of the information and types of communication sought.[68]

At a minimum, the application must allow the FISC to find probable cause that the target is a "[f]oreign power"[69] or an "[a]gent of a foreign power."[70] The terms "[f]oreign power" and "[a]gent of a foreign power"

64. 50 U.S.C. § 1804(a).

65. *Id*.

66. *Id*. § 1804(a)(3)(A).

67. *Id*. § 1804(a)(3)(B).

68. *Id*. § 1804(a)(5).

69. *Id*. § 1801(a).

"Foreign power" means—

(1) a foreign government or any component thereof, whether or not recognized by the United States;

. . . .

(4) a group engaged in international terrorism or activities in preparation therefor;

(5) a foreign-based political organization, not substantially composed of [USPERs]; [or]

(6) an entity that is directed and controlled by a foreign government or governments . . . .

Id.

70. *Id*. § 1801(b).

"Agent of a foreign power" means—

(1) any person other than a [USPER], who—

(A) acts in the United States as an officer or employee of a foreign power . . .

(B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; [or]

. . . .

(2) any person who—

(A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States;

(B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of such

ensure the international nexus necessary to fall under FISA's jurisdiction. Within the definition of "[a]gent of a foreign power," there is a "knowingly" requirement when a USPER is the proposed target, thereby heightening the standard for finding that a USPER is an agent.[71] In other words, the government would have to prove that the USPER knowingly acted for or on behalf of a foreign power, whereas the government would not need to make a showing of mens rea for a non-USPER.

To receive a FISA order, the government must have the "significant purpose" to obtain foreign intelligence information ("FII") from the surveillance.[72] The definition of FII is broad, and the standard for FII collection further depends on whether the information concerns a USPER.[73] FII is information that relates to the ability of the United States to protect against actual or potential attack or other grave hostile acts;[74] sabotage or international terrorism, or the international proliferation of weapons of mass destruction;[75] or clandestine intelligence activities by or of a foreign power or an agent of a foreign power.[76] On the one hand, if the information sought does not concern a USPER, the information must only relate to these activities.[77] On the other hand, if the information involves a USPER, the information collected must be necessary to (a) the national defense or security of the United States[78] or (b) the conduct of the foreign affairs of the United States.[79] Russian disinformation is likely to fall into the catch-all language regarding security and foreign affairs.[80]

Fundamentally, the "significant purpose" requirement protects against abuse of FII collection. In other words, the "sole objective" in the collection

> foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; [or]
>
> (C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; . . . .

Id.

71. *Id*.; *see* United States v. Duggan, 743 F.2d 59, 75 (2d Cir. 1984) ("Section 1801(b), for example, makes a [USPER] an agent of a foreign power only if he 'knowingly' engaged in certain activities; the [S]ection contains no knowledge requirement with respect to non-[USPERs].").

72. 50 U.S.C. § 1804(a)(6)(B). The USA PATRIOT Act amended FISA to state that acquisition of FII need only be a significant purpose, rather than the primary purpose, of the surveillance. *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, sec. 218, 115 Stat. 272, 291 (codified at 50 U.S.C. §§ 1804(a)(6)(B), 1823(a)(6)(B) (2012)).

73. *Id*. § 1801(e).

74. *Id*. § 1801(e)(1)(A).

75. *Id*. § 1801(e)(1)(B).

76. *Id*. § 1801(e)(1)(C).

77. *Id*. § 1801(e)(1)–(2).

78. *Id*. § 1801(e)(2)(A).

79. *Id*. § 1801(e)(2)(B).

80. *Id*. § 1801(e)(2).

of FII may not be "merely to gain evidence of past criminal conduct" to punish the agent of a foreign power.[81] FISA requires a high-ranking executive branch official to certify that: (1) the information sought is FII; (2) a "significant purpose" of the surveillance or search is to obtain FII; and (3) normal investigative techniques cannot reasonably obtain such information.[82]

Membership in or activities in support of an organization—even one that advocates violence—are protected First Amendment activities.[83] Under FISA and the First Amendment, a proposed target's mere association with terrorist groups cannot justify surveillance. Instead, the government must establish probable cause that a prospective target intentionally acted to further terrorist activities.[84]

FISA's high standards for the collection of information on USPERs can serve as a model for creating legislation that would allow domestic surveillance of USPERs. Requiring an application for a court order from FISC, and heightened requirements for collection on USPERs, would preserve constitutional rights. As discussed below, requiring a warrant would better protect civil liberties.[85] However, a warrant requirement may not always be practical in light of urgent national security concerns.

B. FISA's Protections for Civil Liberties

Beyond certification, FISA places additional restrictions on surveillance that seek to balance national security and First Amendment rights, namely, minimization procedures and a prohibition on surveilling a USPER solely based on First Amendment activities. In particular, FISA imposes limitations on how non-public information regarding non-consenting USPERs may be used, requires a FISC judge to review the adequacy of proposed minimization procedures, and limits the use of First Amendment information of a proposed target.

First, to reduce the risk that surveillance might interfere with the rights of USPERs, FISA imposes limitations on the acquisition, retention, and dissemination of non-public information regarding non-consenting USPERs.[86]

81. *See In re* Sealed Case, 310 F.3d 717, 735 (FISA Ct. Rev. 2002). But to the extent that obtaining FII is in part influenced by law enforcement interests, FII collection and criminal prosecution functions may overlap. 50 U.S.C. §§ 1801(e), 1804, 1823(e).

82. 50 U.S.C. § 1804(a)(6).

83. *See* United States v. Megahey, 553 F. Supp. 1180, 1184 (E.D.N.Y. 1982) (acknowledging Senate report notes, which stated that the purpose of FISA was to strike a balance between the need for surveillance and the protection of civil liberties), *judgment aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1983) *and judgment aff'd on other grounds*, 743 F.2d 59 (2d Cir. 1984).

84. *See* S. REP. NO. 95-604, at 23, 27–28, 47 (1977) (clarifying that the probable cause standard is the same as in the traditional criminal context and that the Government must "establish[] probable cause that each and every element of [the status of agent of a foreign power] exists").

85. *See infra* Section II.D.

86. 50 U.S.C. § 1806 (allowing the use of information acquired from electronic surveillance concerning USPERs where certain minimization procedures are followed, (e.g., notification to the

Non-public information concerning a USPER may be disseminated without that person's consent only if the person's "identity is necessary to understand the [FII] or assess its importance."[87] Specifically, the AG must promulgate "minimization procedures" that are "reasonably designed" to minimize acquisition and retention and prohibit dissemination to avoid over-collection and misuse.[88]

Minimization procedures vary depending on the context: the type of intelligence collection at issue, the agencies involved, and the nature of the target.[89] For traditional FISA electronic surveillance, minimization occurs at the retention and dissemination stages.[90] If information is neither FII nor evidence of a crime, the reviewing agent will minimize information collection by discarding, erasing, or omitting the information in the indexing log.[91] And, before dissemination, the reviewing agent must redact all USPERs' names and personal identifiers, except when "such person's identity is necessary to understand [FII] or assess its importance" or is evidence of a crime.[92]

Minimization procedures for bulk data collections under Section 702 are more stringent.[93] The procedures place limits on who may access Section 702-acquired information and on the use of "sensitive information," such as "religious[,] academic, political, or highly personal" information and medical information.[94] For upstream collection, or collection of communications from fiber cables and infrastructure,[95] the FISC imposes additional procedures, such as "restrict[ing] access to databases most likely to contain wholly domestic communications," requiring the information to be purged from the

aggrieved person, permitting motions to suppress, and requiring the destruction of unintentionally acquired information, with exceptions)).

87. *Id*. § 1801(h)(2).

88. *Id*. § 1801(h)(1).

89. Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 72 (2018).

90. *Id*. at 73. Retention is where the information is decoded, translated, or otherwise made readable. *Id*.

91. *In re* All Matters Submitted to FISA, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002), *abrogated on other grounds by In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

92. 50 U.S.C. §§ 1801(h)(2), 1821(4)(B); *In re All Matters*, 218 F. Supp. 2d at 618.

93. Berman, *supra* note 89, at 75.

94. *Id*. at 76; *see also* LORETTA E. LYNCH, U.S. DEP'T OF JUSTICE, MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2016), https://www.dni.gov/files/documents/icotr/51117/2016_FBI_Section_702_Minimization_Procedures_Sep_26_2016_part_1_and_part_2_merged.pdf (enumerating the limitations on the FBI's acquisition of communications in line with Section 702(b)).

95. James Bamford, *They Know Much More Than You Think*, N.Y. REV. BOOKS (Aug. 15, 2013), https://www.nybooks.com/articles/2013/08/15/nsa-they-know-much-more-you-think/.

system, permanently tagging the information as "upstream" to alert its sensitive nature, and limiting retention to two years.[96]

Second, a FISC judge must sign off on proposed minimization procedures and deem them consistent with the need to obtain, produce, and disseminate FII.[97] Every FISC order incorporates these minimization procedures. FISC may also require supplemental procedures in certain circumstances,[98] and the government may request modifications to the procedures.[99] FISA also contemplates that minimization can occur later in the process of reviewing the communications.[100]

Third, and finally, the FISC cannot accept the government's assertion that a USPER is an agent of a foreign power "solely" based on activities protected by the First Amendment.[101] Instead, the judge "may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target."[102] However, if the government has probable cause to believe the target may also be involved with or knowingly aiding or abetting unlawful clandestine activities, the FISC may authorize surveillance even if the target is engaged in First Amendment activities.[103] As a federal district court ruled, a target's involvement in protected First Amendment activities does not bar electronic surveillance under FISA.[104]

96. Berman, *supra* note 89, at 76–77. For an explanation on how the NSA's upstream collection program obtains wholly domestic communications and the FISC's consideration of how NSA's targeting and minimizing procedures comport with the Fourth Amendment, see generally [REDACTED], No. PR/TT [REDACTED], 2011 WL 10945618, at *1, *15–17, *23–28 (FISA Ct. Oct. 3, 2011) (discussing NSA's targeting procedures and how NSA's upstream collection program collects wholly domestic communications, the minimization framework does not meet FISA, and the minimization and targeting procedures do not satisfy the Fourth Amendment).

97. *See* 50 U.S.C. § 1801(h) (outlining required minimization procedures).

98. *See, e.g.*, *In re* All Matters Submitted to FISA, 218 F. Supp. 2d 611, 618–19 (FISA Ct. 2002) (noting the legislative history that suggests a FISC judge has "*discretionary power to modify* the order").

99. *Id*. at 619 (describing how the Attorney General and Deputy Attorney General "augmented" and "expanded" procedures governing contacts between FBI and Department of Justice ("DOJ") attorneys during FISA surveillance).

100. Inherent in the concept of retention, an agency can obtain raw FISA-acquired information that needs to be evaluated for whether it contains FII, information necessary to understand or assess FII, or evidence of a crime. *See* LYNCH, *supra* note 94, at 5. The FBI then conducts minimization procedures, such as striking personal identifiers, from the raw FISA-acquired information. *Id*. at 9. Raw FISA-acquired information, that is, information the FBI obtained but must still review, can only be held for five years, unless the agency determines an extension is necessary. *Id*. at 22.

101. United States v. Rosen, 447 F. Supp. 2d 538, 548 (E.D. Va. 2006) (explaining a judge can rely in part on these activities as long as there is probable cause that the target may be involved in unlawful clandestine activities).

102. 50 U.S.C. § 1805(b).

103. *Rosen*, 447 F. Supp. at 549–50.

104. *Id*.

C. Court Orders and Section 702 Surveillance

Alongside the procedural and substantive requirements embedded in FISA, the Fourth Amendment, specifically the warrant requirement, also protects USPERs from improper surveillance under FISA. If surveillance intentionally targets a USPER, even if they are reasonably believed to be abroad, the traditional probable cause and warrant analyses are required.[105] However, with the FISA Amendments Act of 2008 ("FAA"), Congress distinguished procedures for targeting non-USPERs outside the United States,[106] collecting FII inside the United States targeting USPERs outside the United States,[107] and collecting FII by targeting USPERs outside the United States.[108] The enactment of the FAA affected how the probable cause and warrant analyses would apply, if at all, to the three categories.

The FAA had two primary goals. First, "Congress wanted to provide a sound statutory framework, consistent with the Constitution" that would enable the targeting of those abroad and, at the same time, afford additional protections to USPERs "whose communications are targeted for collection or collected incidentally."[109] For example, the FAA prevents the government from targeting USPERs overseas without an individualized warrant, as had been possible before.[110] Second, Congress "wanted to provide civil immunity" for service providers who assisted the intelligence community.[111]

The FAA preserves the principle of relying on the location of the potential target of surveillance and their USPER status as a basis for regulating intelligence collection. But unlike the practice with traditional FISA applications, the FAA does not require the government to obtain a FISC order identifying the facilities, telephone lines, e-mail addresses, places, or property where any surveillance will be directed. For programmatic surveillance, the FAA eliminated the requirement for the government to show probable cause that the target of surveillance was a foreign power or an agent of a foreign power.

Sections 702, 703, and 704 of the FAA cover collection on USPERs and non-USPERs outside the United States. First, Section 702 provides procedures for targeting non-USPERs abroad.[112] The AG and the Director of National Intelligence ("DNI") may authorize, for up to one year, targeting of

105. 50 U.S.C. §§ 1881b(c)(1)(B), 1881c(c)(1)(B).

106. *Id*. § 1881a.

107. *Id*. § 1881b.

108. *Id*. § 1881c.

109. OFFICE OF THE INSPECTOR GENERAL, DEP'T OF JUSTICE, A REVIEW OF THE FEDERAL BUREAU OF INVESTIGATION'S ACTIVITIES UNDER SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT AMENDMENTS ACT OF 2008 14 (2012) [hereinafter OIG REPORT], https://oig.justice.gov/reports/2015/o1501.pdf.

110. *Id*. at 14–15.

111. *Id*. at 15.

112. 50 U.S.C. § 1881a.

non-USPERs reasonably believed to be located outside the United States, subject to approved targeting and minimization procedures.[113] Section 702 is limited to determining whether targeting and minimization procedures comply with the statute and the Fourth Amendment.[114] It establishes a system with oversight for U.S. internet service providers to respond to government requests for information on foreign people believed to be located overseas and associated with foreign intelligence topics. Section 702 does not permit the intelligence community to target a USPER anywhere in the world[115] but permits incidental collection on USPERs, subject to minimization and use rules.[116]

Next, Section 703 regulates collection inside the United States that targets USPERs outside the United States.[117] It applies when the assistance of a provider is required to target the USPER.[118] Applications made to the FISC must describe the techniques used,[119] but do not have to specify the targeted facilities.[120] Additionally, a USPER overseas may be targeted under this Section if they meet the description of an agent of a foreign power in Title 50, section 1801(b)(2) of the United States Code *or* if they are officers or employees of a foreign power.[121] Section 703 contains a seven-day emergency provision.[122] Specifically, if an applicant can obtain an order under normal circumstances, but "an emergency situation exists" that requires the acquisition of FII, the AG can authorize the acquisition if a judge is informed at the time of authorization and an application is made to the FISC within seven days.[123]

Finally, Section 704 describes acquisitions targeting USPERs outside the United States.[124] It provides for FISC jurisdiction over the targeting of

113. *Id*. § 1805(d)(1).

114. *Id*. § 1881a (among other subsections, subsection (b) provides limitations on acquisitions, subsection (d) explains targeting procedures, subsection (e) provides minimization procedures, subsection (f) requires the Attorney General to adopt guidelines "consistent with the [F]ourth [A]mendment" and limits FBI access to certain communications, subsection (g) explains the Attorney General's certification requirements, and subsections (h), (i), and (j) provide for judicial review).

115. *Id*. § 1881a(b)(3).

116. *In re* Directives [Redacted] Pursuant to Section 105b of FISA, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008) (noting that "incidental collections occurring as a result of constitutionally permissible acquisitions do not render those acquisitions unlawful").

117. 50 U.S.C. § 1881b.

118. *Id*. § 1881b(c)(5)(B).

119. *Id*. § 1881b(b)(1)(G).

120. *Id*. § 1881b(b)(1)(H).

121. *Id*. § 1881b(c)(1)(B)–(C).

122. *Id*. § 1881b(d)(1).

123. *Id*. § 1881b(d)(1)(A).

124. *Id*. § 1881c.

USPERs reasonably believed to be located overseas when the collection occurs *outside* the United States.[125] Applications need not specify the techniques or targeted facilities.[126] A USPER overseas may be targeted under this Section if they meet the description of an agent of a foreign power in section 1801(b)(2) *or* if they are officers or employees of a foreign power.[127] Like Section 703, it contains a seven-day emergency provision.[128]

FISA authority for electronic surveillance of USPERs may not exceed ninety days.[129] The government must obtain approval from the FISC for an additional authorization, not to exceed ninety days.[130] For non-USPERs, the surveillance authority may be granted for up to 120 days and up to one year upon renewal of the application if the FISC has probable cause to believe that no communications of any individual USPER will be acquired during the renewal period.[131] Renewals are unlimited so long as the government can continue to show the FISC that the government has probable cause to believe the target is a foreign power or an agent of a foreign power, and the target still uses or is about to use the targeted facilities.[132]

The FAA represents improved protections for constitutional liberties when conducting surveillance. With the Act, Congress made clear that USPERs require additional protections that are not necessary for non-USPERs and clarified other protections required for USPERs. In particular, the seven-day emergency requirement in Sections 703 and 704 creates a balance between the flexibility needed to address urgent national security concerns with safeguards for constitutional rights.

D. Protections on Bulk Data Collection

The FAA and the FISA Amendments Reauthorization Act of 2017 ("2017 Amendments") also limit surveillance authorities, especially under Section 702. FISA primarily structures limitations on surveillance around what is known at the time of acquisition.[133] First, surveillance "may not intentionally target any person known . . . to be located in the United States."[134] Second, surveillance "may not intentionally target a person reasonably believed to be located outside the United States if the purpose . . . is to target

125. *Id*. § 1881c(a).

126. *Id*. § 1881c(b) (omitting mention of needing to specify techniques or targeted facilities in the application).

127. *Id*. § 1881c(b)(3)(B).

128. *Id*. § 1881c(d)(1).

129. *Id*. § 1805(d)(1).

130. *Id*.

131. *Id*.

132. *Id*. § 1805(d)(2).

133. *Id*. § 1881a(b).

134. *Id*. § 1881a(b)(1).

a . . . person reasonably believed to be in the United States."[135] Third, surveillance "may not intentionally target a [USPER] reasonably believed to be located outside the United States."[136] That said, under the 2017 Amendments, surveillance may target a person to gather foreign intelligence without a separate FISC order if the AG has authorized "the emergency employment of electronic surveillance or a physical search."[137] Fourth, the surveillance "may not intentionally acquire any communication as to which the sender and all intended recipients are known . . . to be located in the United States."[138] Finally, all surveillance must be "consistent with the [F]ourth [A]mendment."[139] In addition to these limitations, the FBI cannot access the contents of Section 702-acquired communications without a court order.[140] To be precise, the FBI cannot retrieve information obtained "pursuant to a query made using a [USPER] query term" if its query "was not designed to find and extract [FII]" but instead is performed "in connection with a predicated criminal investigation" unrelated to national security.[141]

The FBI and NSA are the only agencies authorized to acquire FII under Section 702.[142] The FBI may only use USPERs' information collected under Section 702 as evidence in a criminal proceeding if the agency obtains a court order or if the criminal proceeding involves one of the items on an enumerated list of conduct.[143] The FBI must also review the sufficiency of the NSA's explanation for its reasonable belief that the account's user is outside of the United States.[144] Finally, the FBI must review and evaluate the sufficiency of the NSA-provided information that the person to be targeted is a non-USPER.[145]

Although collections under Section 702 do not require warrants, Section 702 includes many protections for constitutional liberties. Congress clarifies restrictions on collection on USPERs. The amendments to FISA also impose important certification requirements for these modes of surveillance to protect constitutional liberties.[146] First, the AG and DNI must certify to the FISC

135. *Id*. § 1881a(b)(2).

136. *Id*. § 1881a(b)(3).

137. 2017 Amendments, supra note 7, at 132 Stat. 13. Under this emergency exception, the Attorney General may authorize electronic surveillance where they "reasonably determine[]" that surveillance is required "to obtain [FII] before an order authorizing such surveillance can with due diligence can be obtained." 50 U.S.C. § 1805(e)(1)(A).

138. 50 U.S.C. § 1881a(b)(4).

139. *Id*. § 1881a(b)(5).

140. 2017 Amendments, *supra* note 7, at sec. 101, 132 Stat. 4.

141. *Id*.

142. OIG REPORT, *supra* note 109, at xiii. For the CIA to participate, it must submit its targeting request to the NSA. *Id*.

143. *See id*.

144. *Id*.

145. *Id*. at xv.

146. 2017 Amendments, *supra* note 7137, at sec. 101, 132 Stat. 4.

that acquisitions under the program will meet the targeting objectives and limitations under section 1881a.[147] Second, they must certify that the acquisitions will satisfy traditional FISA minimization procedures.[148] Finally, the certification must reflect that the AG adopted guidelines that meet the statutory procedures, the targeting and minimization procedures and guidelines do not violate the Fourth Amendment, and that a significant purpose of the programmatic collection is to obtain FII.[149]

Finally, and importantly, the 2017 Amendments require the release of information on the breakdown of U.S. and non-USPER targets of electronic surveillance. The FBI must also disclose to the public the number of instances it opened "an investigation of a [USPER] (who is not considered a threat to national security) based wholly or in part on an acquisition" of the information under Section 702.[150] The DNI and AG must annually release a declassified version of the minimization procedures that apply to the handling of USPER information collected under Section 702.[151] The AG must also report the number of subjects targeted either under an order or under an emergency authorization, and the number of those targeted who are USPERs.[152] This report must be unclassified "to the extent consistent with national security" and publicly available.[153] Section 702 surveillance is subject to regular review by the Justice Department, the Office of the Director of National Intelligence ("ODNI"), Congress, and FISC.[154] NSA employees also receive extensive training on Section 702 to minimize abuses.[155]

To summarize, the Section 702 program is highly valuable but also highly constrained and monitored. The Fourth Amendment is a fundamental limitation on collections of USPERs' data, whether intentional or incidental. In particular, the warrant requirement, minimization procedures, and reporting requirements that promote transparency—as adopted at various levels

147. 50 U.S.C. § 1881a(g) (2012).

148. *Id*.

149. *Id*.

150. 2017 Amendments, *supra* note 7137, at sec 102, 132 Stat. at 9.

151. *Id*. at sec. 104, 132 Stat. 13.

152. *Id*. at sec. 102, 132 Stat. 9. According to the DOJ, during 2018, the government filed 1081 applications for authority to conduct electronic surveillance. Letter from Stephen E. Boyd, Assistant Attorney General, Office of Legislative Affairs, U.S. Dep't of Justice, to The Honorable James C. Duff, Director, Admin. Office of the U.S. Courts, (May 3, 2019) (on file with authors). The FISC approved 1079 applications. According to the Administrative Office of the United States Courts, which reports the number of proposed applications, the government filed 1142 applications and 830 were granted, 245 were modified, 40 were denied in part, and 27 were denied in full. The total number of persons targeted for electronic surveillance was between 1500 and 1999 and the aggregate number of USPERs targeted was between 0 and 499. *Id*.

153. 2017 Amendments, *supra* note 7137, at sec. 107, 132 Stat. at 14.

154. CHRIS INGLIS & JEFF KOSSEFF, IN DEFENSE OF FAA SECTION 702, 15–19 (2016), www.hoover.org/sites/default/files/research/docs/ingliskosseff_defenseof702_final_v3_digital.pdf.

155. *Id*. at 16–17.

throughout FISA—protect civil liberties, including the First Amendment. Again, these provisions could serve as a model for creating legislation that would allow surveillance to combat disinformation campaigns designed to influence the electoral process. Similar warrant requirements, minimization procedures, and reporting requirements would protect Fourth and First Amendment rights.

III. FISA AND THE FIRST AMENDMENT

Surveillance will always implicate the First Amendment because of its potential to create a chilling effect on speech or impose associational burdens. FISA surveillance, in particular, has faced many First Amendment challenges, and Congress has reformed it to assuage these concerns.[156] Generally, if a warrant names accounts of foreign powers or agents disseminating or engaging in disinformation, a FISC may authorize the collection of their communications metadata.[157] That the government can intercept communications of foreign nationals believed to be outside the United States buttresses this point.[158] For example, an acquisition order could, in theory, seek all telephone and e-mail communications to and from countries of foreign policy interest, like Russia. That could include communications to and from USPERs.

However, if the government is surveilling for Russian disinformation, critics might raise concerns that the government could pretextually target a USPER for an expressed political view that aligns with disinformation tactics. Thus, a person may be chilled from stating their actual beliefs for fear of government intervention.[159] This section analyzes how FISA and the debate surrounding it can provide lessons learned for legislation to combat information warfare.

A. First Amendment Rights

Generally, to justify interference with First Amendment rights, the government must have a compelling state interest, narrowly tailored to achieve

156. *See, e.g.*, United States v. Falvey, 540 F. Supp. 1306 (E.D.N.Y. 1982) (holding that surveillance of U.S. citizens engaged in terrorist activities does not violate the First Amendment); United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982), *judgment aff'd without opinion*, 729 F.2d 1444 (2d Cir. 1983).

157. *See, e.g.*, United States v. Aldawsari, 740 F.3d 1015 (5th Cir. 2014); United States v. Squillacote, 221 F.3d 542 (4th Cir. 2000) (holding that the defendant was an agent of a foreign power and electronic surveillance was legal). *But see* United States v. Missick, 875 F.2d 1294 (7th Cir. 1989) (finding that the defendant was not an agent of a foreign power such that FISA would apply).

158. *See* 50 U.S.C. § 1881a (2012).

159. *Cf.* Susan M. Akram & Kevin R. Johnson, *Race, Civil Rights, and Immigration Law After September 11, 2001: The Targeting of Arabs and Muslims*, 58 N.Y.U. ANN. SURV. AM. L. 295, 299–300 (2002).

its stated purpose. Some have questioned whether combatting efforts designed to undermine the electoral process is a clear enough national security interest to justify infringing on USPERs' First Amendment rights.[160] As the *Keith* Court stated, freedom of speech is placed in danger "where the [g]overnment attempts to act under so vague a concept as the power to protect 'domestic security.'"[161] Justifying surveillance on a so-called "national security interest" would be similarly vague without careful elaboration.

B. The Success of First Amendment Claims Under FISA

It is hard for an individual to make a successful claim that surveillance authorized by FISA violated their First Amendment rights. High potential for the abuse of First Amendment rights may exist when the executive branch alone makes national security surveillance decisions.[162] The FISC tends to reject any First Amendment objections or fails to mention them.[163] Arguments raised in other federal courts that challenge surveillance programs under the First Amendment also tend to fail.[164]

First, where surveillance, under FISA, does not directly target a USPER, courts have held that USPERs have no legal claim or concern under the First Amendment caveat, which prohibits probable cause determinations from being made solely on a proposed target's First Amendment activities,[165] as the First Amendment caveat does not apply to non-USPERs.[166] In *ACLU Foundation of Southern California v. Barr*,[167] the United States Court of Appeals for the District of Columbia affirmed a district court order upholding the legality of surveillance of nonresident aliens (non-USPERs), except for the district court's dismissal of the plaintiffs' First Amendment claim.[168] According to the court, only two of the eight alien plaintiffs were permanent resident aliens that would qualify as USPERs.[169] Thus, the First Amendment caveat

160. *See* Goldenziel & Cheema, *supra* note 8, at 95–96.

161. 407 U.S. 297, 314 (1972).

162. Thistle, *supra* note 51, at 1218.

163. *See, e.g.*, [Redacted], No. PR/TT [Redacted], at 66–69 (FISA Ct. [Redacted]) (Kollar-Kotelly, J.), https://www.odni.gov/files/documents/1118/CLEANEDPRTT%201.pdf (holding that NSA bulk collection of email and Internet metadata under Section 214 of the Patriot Act did not violate the First Amendment).

164. *See, e.g.*, ACLU v. Clapper, 785 F.3d 787, 821 n.12 (2d Cir. 2015) (deciding the cases without reaching the First Amendment issue); United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 WL 2866749, at *30–32 (D. Or. June 24, 2014) (holding that surveillance under Section 702 of FISA did not violate the First Amendment since the Fourth Amendment was satisfied).

165. 50 U.S.C. § 1805(a)(2)(A) (2012).

166. United States v. Megahey, 553 F. Supp. 1180 (E.D.N.Y. 1982) (asserting no USPER was the target of the surveillance pursuant to FISA, the First Amendment caveat was not implicated).

167. 952 F.2d 457, 472 (D.C. Cir. 1991).

168. *Id*.

169. *Id*. at 464.

only applied to those two plaintiffs.[170] However, the court noted "the government may be violating the First Amendment when it investigates someone because it dislikes the person's political views,"[171] and because the First Amendment does apply to non-resident aliens to some extent, that may be a basis for constitutional concern regarding all the plaintiffs, including non-USPERs.[172] Thus, if the target of the surveillance is a USPER or the target's activities are protected by the First Amendment, a wiretap will violate FISA if the target is labeled as a foreign power based solely on the target's First Amendment activities.[173]

Second, the government is allowed to rely in part on First Amendment activities in its application requesting surveillance, and the FISC is allowed to rely in part on First Amendment activities in permitting surveillance. In *United States v. Rahim*,[174] the defendant argued that "the FISA evidence was obtained solely on the basis of his protected First Amendment activities."[175] The court looked to precedent from other districts[176] to determine that "while Rahim may have been engaged in some protected First Amendment activities, these activities were not the sole basis underlying that determination."[177] Because the FISC judge could find probable cause that the target of the surveillance was an agent of a foreign power through considering other non-speech or association activities, the court found Rahim's argument to be meritless.[178] Extending *Rahim*, in *United States v. Kokayi*,[179] the court found that a target's First Amendment activities may contribute to a probable cause determination if the target engaged in otherwise prohibited activities. In *Kokayi*, the defendants alleged that "the FISA applications may have been improperly predicated on protected First Amendment activities."[180] The court, however, disagreed.[181] Instead, it asserted, "the probable cause determina-

170. *Id*. ("Although one would hardly know it from the Complaint, § 1805(a)(3)(A) turns out to be irrelevant to twenty-two of the twenty-four plaintiffs in this case.").

171. *Id*. at 471.

172. *Id*. at 467.

173. *See* United States v. Sattar, No. 02 CR. 395 JGK, 2003 WL 22137012, at *1 (S.D.N.Y. Sept. 15, 2003).

174. No. 3:17-CR-0169-B, 2019 WL 1595682, at *1 (N.D. Tex. Apr. 15, 2019).

175. *Id*. at *1–3.

176. United States v. Aziz, 228 F. Supp. 3d 363, 377 (M.D. Pa. 2017) (upholding FISA applications "grounded in conduct which plainly exceeds the bounds of the First Amendment's protective sphere"); United States v. Elshinawy, No. ELH-16-0009, 2017 WL 1048210, at *11 (D. Md. Mar. 20, 2017) (noting the government can use statements made in furtherance of a conspiracy to show a participant's criminal intent); United States v. Rosen, 447 F. Supp. 2d 538, 548–49 (E.D. Va. 2006) (noting the court can rely in part on First Amendment activities).

177. *Rahim*, 2019 WL 1595682, at *2.

178. *Id*.

179. 1:18-cr-410 (LMB), 2019 WL 1186846, at *1 (E.D. Va. March 13, 2019).

180. *Id*. at *4.

181. *Id*.

tion may rely in part on activities protected by the First Amendment, provided the determination also relies on activities not protected by the First Amendment."[182] Thus, a court may consider an individual's protected First Amendment activities so long as additional evidence of prohibited activities exists.[183]

Finally, First Amendment claims often fail under FISA because defendants do not always allege a proper First Amendment violation, such as a chilling effect. For the First Amendment to invalidate a practice, the government's action must harm a person because of their protected speech.[184] The mere assertion that speech or association will potentially be chilled is not sufficient to support a First Amendment claim.[185] An unconstitutional chilling effect exists where the government's actions are "regulatory, proscriptive, or compulsory in nature."[186] Three cases, *Laird v. Tatum*,[187] *Clapper v. Amnesty International USA*,[188] and *United States v. Falvey*,[189] provide the parameters of success for chilling effect claims under FISA. Because FISA forces the government to meet specific standards before an order based on an individual's First Amendment activities can be issued, courts have yet to find FISA's provisions so overly broad that they chill an individual's First Amendment rights.[190]

In *Laird v. Tatum*, the Court found the plaintiff's claim non-justiciable as the "allegations of a subjective 'chill' are not an adequate substitute for a claim of specific present objective harm or a threat of specific future harm."[191] The plaintiffs did not present evidence of illegal surveillance practices.[192] Similarly, in *Clapper v. Amnesty International USA*, the Court denied standing to plaintiffs who alleged actual and threatened harm from surveillance conducted under Section 702.[193] However, the plaintiffs did not show a realistic threat of imminent injury.[194] Under Section 702, the govern-

182. *Id*. at *4 (quoting United States v. Rosen, 447 F. Supp. 2d 538, 548 (E.D. Va. 2006)).
183. *Id*. at *13–14.
184. Laird v. Tatum, 408 U.S. 1, 11 (1972).
185. *See* Younger v. Harris, 401 U.S. 37, 50 (1971).
186. *Laird*, 408 U.S. at 11.
187. 408 U.S. 1 (1972).
188. 568 U.S. 398 (2013).
189. 540 F. Supp. 1306 (E.D.N.Y. 1982).
190. *See id*. at 1313 (asserting that because the judge, not the executive branch, makes the finding that the target is truly an agent of a foreign power, and that FISA admonishes that no USPER can be considered an agent solely based on her First Amendment activities, FISA is not overbroad); *see also* ACLU Found. of So. Cal. v. Barr, 952 F.2d 457 (D.C. Cir. 1992).
191. *Laird*, 408 U.S. at 13–14.
192. *Id*.
193. 568 U.S. at 402.
194. *Id*. at 405–22.

ment can monitor foreign communications without a showing of individualized suspicion, even if that program incidentally collects communications of USPERs.[195]

In *United States v. Falvey*, the defendants, accused of supporting the Irish Republican Army ("IRA"), claimed FISA violated the First Amendment by allowing the government to engage in politically motivated surveillance.[196] Further, the defendants asserted that surveillance would create a chilling effect where people would be afraid to express their sympathies for certain groups because the government would then invade their privacy under FISA.[197] However, the court held that FISA, on its face, is neither overbroad nor unconstitutional on First Amendment grounds, as it did not create a chilling effect.[198] The Court found it important that the FISC—and not the executive branch—made the finding that a target is an agent of a foreign power. The Court reasoned that a judicial determination, rather than an executive one, protects against abusive political surveillance.[199] Further, the Court noted that FISA prevents the executive from determining that someone is an agent of a foreign power solely based on protected First Amendment activities.[200] The court went on to assert that the First Amendment does not protect the IRA's acts of intimidating and coercing the civilian population and government, but more importantly, that these actions are "legitimately encompassed by FISA."[201] Accordingly, "the defendants' First Amendment rights were not violated."[202]

To summarize, plaintiffs must assert an actual chilling effect on their speech, not a potential one, to claim a First Amendment violation under FISA. This requirement by courts is consistent with the longstanding principle of actual harm required for standing. No First Amendment challenge to FISA has yet succeeded. However, a plaintiff alleging injury-in-fact to her constitutional rights due to FISA may very well succeed. To preserve constitutional liberties, any legislation allowing surveillance to combat information warfare should similarly allow lawsuits to challenge it based on injury-in-fact.

C. The Link Between the First and Fourth Amendment

A remaining question is whether FISA-like protections embedded in the legislation enabling surveillance to combat disinformation campaigns would

195. 50 U.S.C. § 1881a(a)–(b) (2012).
196. 540 F. Supp. 1306, 1307 (E.D.N.Y. 1982).
197. *Id.* at 1314.
198. *Id.* at 1314–15.
199. *Id.*
200. *Id.* at 1315; *see also* United States v. Aziz, 228 F. Supp. 3d 363 (M.D. Pa. 2017).
201. *Falvey*, 540 F. Supp. at 1315 (citing 50 U.S.C. § 1801(c)(2)).
202. *Id.*

be sufficient to address First Amendment concerns. Courts will likely hold that Fourth Amendment protections are adequate to protect First Amendment rights, as they have determined with regard to FISA.[203] However, we argue that Fourth Amendment protections are insufficient to protect the First Amendment rights implicated in any surveillance necessary to combat disinformation campaigns.

The First and Fourth Amendments both play an essential role in protecting the civil liberties of USPERs. Courts generally evaluate surveillance under the Fourth Amendment, not the First Amendment.[204] As a result, courts have found repeatedly that the satisfaction of Fourth Amendment requirements is sufficient to protect First Amendment rights in surveillance cases.[205] For example, in the 1978 case of *Zurcher v. Stanford Daily*,[206] the Supreme Court held that procedural safeguards are unnecessary to protect First Amendment Rights in the context of search and seizure as long as Fourth Amendment requirements are satisfied.[207] In *Zurcher*, a student newspaper alleged that a police search violated its First, Fourth, and Fourteenth Amendment rights because the warrant's scope was overly broad and the publication should not have been subject to a third-party search.[208] Officers searched the newspaper's office to retrieve photos it published about a violent protest in which none of the newspaper's members were involved.[209] The Court found that "[n]either the Fourth Amendment nor the cases requiring consideration of First Amendment values in issuing search warrants, however, call for imposing the regime ordered by the [d]istrict [c]ourt."[210] It held that First Amendment rights are protected where searches are subjected to a test of reasonableness and a warrant issued by a neutral magistrate.[211] Thus, according to the Court, where government action meets the Fourth Amendment requirements, an individual's First Amendment rights are adequately protected, and no further safeguards are needed.[212]

203. *See, e.g.*, United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 U.S. Dist. LEXIS 85452, at *38 (D. Or. June 24, 2014).

204. Nicole B. Casarez, *The Synergy of Privacy and Speech*, 18 U. PA. J. CONST. L. 813, 817 (2016).

205. ACLU v. NSA, 493 F.3d 644, 688 (6th Cir. 2007) (Smith Gibbons, J., concurring) (noting that the plaintiffs did not have standing to allege a complaint under the First Amendment); *see also* Gordon v. Warren Consol. Bd. of Educ., 706 F.2d 778, 781 n.3 (6th Cir. 1983) (finding surveillance, which falls under the Fourth Amendment "does not violate First Amendment rights, even though it may be directed at communicative or associative activities").

206. 436 U.S. 547 (1978).

207. *Id*. at 565–67.

208. *Id*. at 551–52.

209. *Id*. at 551.

210. *Id*. at 565.

211. *Id*.

212. *Id*. at 565–67.

Surveillance to combat disinformation campaigns, however, is fundamentally different from a physical search of a newspaper's offices. First Amendment rights will be chilled if Americans believe their government can obtain a warrant to surveil their communications based only on probable cause. If the government can obtain a warrant based on such a low standard, Americans will likely believe that the government will do so frequently. This belief would make Americans more likely to self-censor their communications and to protest government actions. The outcry after the surfacing of the National Security Agency's haystack program illustrates this point.[213] If Americans strongly opposed the idea of the National Security Agency collecting their metadata in a haystack, then they would protest the concept of the government's ability to easily surveil their online communications. Because of the high potential for chilling of speech, expression, and association, legislation regarding surveillance to combat disinformation campaigns must include additional protections for First Amendment rights. Courts must decouple the First Amendment analysis from the Fourth Amendment analysis, and legislation must create additional safeguards for the First Amendment itself in this context.

1. The Warrant Requirement

The government can meet both Fourth Amendment and First Amendment requirements by obtaining a warrant to conduct surveillance to combat disinformation campaigns. To do so, the government would follow requirements similar to those outlined in FISA. Obtaining a warrant is the easiest way for the government to show that it has a compelling state interest in conducting the requested surveillance and that the means of achieving that interest are narrowly tailored. A warrant request would require the government to state the target of the surveillance and provide evidence of a reasonable belief that the target presents a threat to national security.[214] Thus, by complying with FISA-like procedures—allowing prior judicial review of surveillance for reasonableness and minimization procedures—the government will not violate the First Amendment.[215] Prior judicial adjudication is exactly what the Supreme Court contemplated as adequate First Amendment protection: applying the Fourth Amendment with "scrupulous exactitude."[216] FISA

213. *See, e.g.*, John Mueller & Mark G. Stewart, *Secret Without Reason and Costly Without Accomplishment: Questioning the National Security Agency's Metadata Program*, 10 I/S: J.L. & POL'Y INFO. SOC'Y 407, 409 (2014) (discussing the secrecy, effectiveness, and "civil liberties and privacy implications of the NSA's massive surveillance efforts").

214. Thistle, *supra* note 51, at 1227.

215. *Id*. at 1226.

216. *See* Stanford v. Texas, 379 U.S. 476, 485 (1965); *see also* A Quantity of Copies of Books v. Kansas, 378 U.S. 205, 208 (1964); Marcus v. Search Warrant, 367 U.S. 717, 731–32, 738 (1961).

provides a model for new domestic surveillance laws that would require similarly stringent application of Fourth Amendment requirements.[217] The procedures and protections outlined in FISA are not sufficient, however. Legislation combatting disinformation should require additional safeguards given the First Amendment interests at stake.

2. Imposing New Warrant Requirements

While Section 702 of FISA currently does not require a warrant for each collection in bulk data collections, especially for incidental collections, a modified warrant process for bulk data collections to combat information warfare would mitigate some of the criticism of Section 702 and better protect constitutional rights.[218]

Section 702 of FISA has been criticized in the courts. In *United States v. Mohamud*,[219] the defendant, a USPER, argued that Section 702 violated the First and Fourth Amendment.[220] The defendant's "communications were collected incidentally during intelligence collection targeted at" non-USPERs outside the United States.[221] The defendant specifically challenged the breadth and vagueness of Section 702 surveillance, asserting it "chill[ed] Americans' exercise of their *First Amendment* rights, causing many to change their habits in using the Internet and telephones."[222] The Ninth Circuit held, however, that the "district court correctly rejected [the defendant's] First Amendment challenge, as motions to suppress based on First Amendment violations are analyzed under the Fourth Amendment."[223] Though the Ninth Circuit used the Fourth Amendment to analyze the alleged violation, it applied the "scrupulous exactitude" standards as ordained for First Amendment concerns that arise in Fourth Amendment searches and surveillance.[224] To be precise, the Oregon federal district court judge held that Section 702 FISA surveillance does not trigger the Warrant Clause because of prior case

217. *See supra* notes 112–116 and accompanying text (discussing the protections for civil liberties within § 702).

218. 50 U.S.C. § 1881(a) (2012).

219. 843 F.3d 420 (9th Cir. 2016).

220. *Id*. at 431.

221. United States v. Mohamud, No. 3:10-CR-00475-KI-1, 2014 U.S. Dist. LEXIS 85452, at *38 (D. Or. June 24, 2014) (emphasis added).

222. *Id*. at *30.

223. *Mohamud*, 843 F.3d at 444 n.28; *see Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *31; *see also* United States v. Mayer, 503 F.3d 740, 747–48 (9th Cir. 2007).

224. *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *32; *see also* Zurcher v. Stanford Daily, 436 U.S. 547, 564 (1978); *see also Mayer*, 503 F.3d at 750.

law on foreign intelligence gathering.[225] In the alternative, even if the Warrant Clause is triggered, Section 702 falls within the foreign intelligence exception.[226]

The analysis used in *Mohamud* is illuminating and provides lessons for new legislation to combat information warfare. First, the defendant in *Mohamud* contended that "the reasoning in *Keith* applies equally well to foreign national security surveillance, especially because of the *First Amendment* implications in the seizure of phone calls and emails."[227] However, the Supreme Court stated that a special needs exception to the warrant requirement exists where, "beyond the normal need for law enforcement, . . . the warrant and probable-cause requirement [become] impracticable."[228] Among other Circuits, the Second, Third, and Fourth Circuits recognized a foreign intelligence exception on the basis that "the important national interest in foreign intelligence gathering justifies electronic surveillance without prior judicial review."[229] The FISC also held that the foreign intelligence exception applies to Section 702 surveillance.[230] With this background, the Oregon federal district court in *Mohamud* concluded that in "balanc[ing] the intrusion on the individual's interest in privacy, namely the incidental collection of [USPERs'] communications, against these special needs when the government targets a non-[USPER] believed to be outside the United States . . . the foreign intelligence exception applies and no warrant is required."[231]

After finding that the foreign intelligence exception applies to Section 702, the *Mohamud* court turned to whether the government action is reasonable under the Fourth Amendment.[232] The district court applied a totality of the circumstances test,[233] weighing "the promotion of legitimate governmental interests against the degree to which [the search] intrudes upon an individual's privacy."[234] The court did "not find the lack of procedures associated with warrants ma[d]e [Section] 702 searches unreasonable under the

225. *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *44.

226. *Id*. at *42.

227. *Id*. at *43.

228. Griffin v. Wisconsin, 483 U.S. 868, 873 (1987) (quoting New Jersey v. T.L.O., 469 U.S. 325, 351 (1985) (Blackmun, J., concurring in judgment)).

229. United States v. Duka, 671 F.3d 329, 341 (3d Cir. 2011); *see* United States v. Duggan, 743 F.2d 59, 72 (2d Cir. 1984); United States v. Truong Dinh Hung, 629 F.2d 908, 914 (4th Cir. 1980).

230. [REDACTED], No. PR/TT [REDACTED], 2011 WL 10945618, at *24 (FISA Ct. Oct. 3, 2011).

231. *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *50.

232. *Id*. at *51; *see In re* Directives [Redacted] Pursuant to Section 105B of FISA, 551 F.3d 1004, 1016 (FISA Ct. Rev. 2008).

233. *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *51 (citing Samson v. California, 547 U.S. 843, 848 (2006)).

234. *Id*. (alteration in original) (quoting Maryland v. King, 569 U.S. 435, 448 (2013)).

Fourth Amendment."[235] Rather, "the minimization procedures contribute to the reasonableness of [Section] 702 under the *Fourth Amendment*."[236]

Thus, the *Mohamud* court went through a two-step process in determining that FISA adequately protects First Amendment concerns by considering those concerns through a Fourth Amendment framework. That is the court found, first, the foreign intelligence exception applies to FISA Section 702,[237] and, second, the government's action under that exception was reasonable.[238]

However, bulk collection without a warrant leaves First Amendment values vulnerable.[239] Fourth Amendment protections are weakened where no warrant is required.[240] Without these Fourth Amendment safeguards, a separate First Amendment analysis becomes crucial to protect freedoms of speech, expression, and association.[241] Any legislation to combat information warfare should incorporate such an analysis.

IV. LESSONS LEARNED FROM FISA

FISA's particular First Amendment protections for USPERs can be a useful model for allowing the United States to surveil foreign agents without unduly infringing on the civil liberties of USPERs. In particular, the statutory protections within FISA can, with some tailoring, properly address concerns about surveillance and potential intrusion on USPERs' privacy, especially those engaging in disinformation campaigns intended to undermine the electoral process. Legislation should draw upon critiques of FISA to improve protections for constitutional liberties when developing programs or collecting information to combat information warfare.

At the outset, to protect the First Amendment, Congress should require procedures similar to FISA's if open-source information is unavailing. New legislation should maintain FISA's high standards for allowing the collection of information on USPERs. First, the government must obtain a court order or warrant. Probable cause must not be based solely on a proposed target's First Amendment activities.[242] Second, the government must adopt and follow minimization procedures to prevent misuse and retention of any USPERs' data that they have incidentally collected.[243] New legislation that relaxes surveillance restrictions on USPERs for the specific national security purpose of combatting information warfare must have regular and rigorous

235. *Id*. at *60.
236. *Id*. at *64.
237. *See supra* note 231 and accompanying text.
238. *Mohamud*, 2014 U.S. Dist. LEXIS 85452, at *60.
239. Thistle, *supra* note 51, at 1227.
240. *Id*.
241. *Id*. at 1228.
242. *See supra* note 13 and accompanying text.
243. *See supra* note 88 and accompanying text.

oversight by the Department of Justice, Congress, and the FISC, much like the oversight structure for FISA Section 702.

In addition, case law involving FISA, discussed above, suggests further safeguards that Congress should incorporate into future legislation. The surveillance required to combat disinformation campaigns may meet the foreign intelligence exception but cannot rely on it entirely. Any legislation to combat information warfare through domestic surveillance should also contain a warrant requirement as additional protection for First Amendment rights. While the Fourth Amendment is necessary to protect First Amendment rights,[244] compliance with the procedural requirements of the Fourth Amendment is insufficient to protect First Amendment expressive and associational rights of individuals subject to surveillance. The First Amendment inquiry should thus be conducted separately from any Fourth Amendment requirements. Because of the high potential for violation of First Amendment rights and a chilling effect on speech, the government should be required to put forward a compelling state interest that is narrowly tailored to surveil a particular individual as to justify any intrusion on First Amendment rights. An all-encompassing interest in national security would be too broad. The government should be required to articulate a specific national security interest that would require surveillance of a particular individual. This would help avoid over-surveillance of Americans at large.

A warrant is the simplest way for the government to show that it has a compelling state interest that would justify infringement on a First Amendment right and that its proposed surveillance is narrowly tailored.[245] The government can then allow a court to decide whether surveillance is reasonable and whether the government has met FISA's requirements or other criteria. A warrant would satisfy the Fourth Amendment requirement and provide additional protections for First Amendment activity as well.

Some might argue that obtaining a warrant would be too burdensome and restrictive on surveillance. However, where First Amendment interests, as here, are incredibly implicated, requiring this level of judicial oversight is necessary for five reasons. First, as with FISA, the government should be able to surveil for urgent national security purposes so long as it obtains an application for a warrant within seven days. In this case, the government should follow minimization procedures to protect First Amendment rights. The government should still make a showing of a compelling state interest to conduct such surveillance that is narrowly tailored to achieve the specific national security objective. The government would ideally present this showing before a committee or a special branch of the FISC that could provide expedited review.[246]

244. *See supra* Section III.C.

245. *See supra* Section III.C.1.

246. *See* Thistle, *supra* note 51, at 1203.

Second, the analysis in *Keith* contemplates the balance between the government's interest in national security and the privacy interests of USPERs.[247] The court in *Keith* held that a neutral magistrate should issue a warrant instead of giving the executive branch sole discretion over domestic surveillance.[248] Similar competing interests must be balanced when justifying foreign surveillance.[249] Since the fight against enemy information warfare will require both domestic and foreign surveillance, a warrant is necessary to protect the Fourth and First Amendment rights of USPERs in either case.

Third, USPERs' First Amendment data should only be accessible for this specific national security purpose of fighting information warfare under this framework.[250] Only particular agencies, such as Homeland Security, State, and Justice, should be able to collect USPERs' information, and legislation must create a specified process for the steps an agency must take to access that information. This process would be similar to the certification process agencies currently undertake to obtain FISA orders.[251]

Fourth, courts should emphasize minimization procedures that prioritize discarding and/or redacting USPER information except where "such person's identity is necessary to understand" the information campaign.[252] This information, like upstream information, should be tagged, so agencies are alerted of its sensitive, First Amendment nature. Further, the government should not retain any information collected to assess and thwart information campaigns designed to influence the electoral process beyond the electoral cycle at hand. After the electoral cycle is over, agencies may summarize their findings, but all USPERs' data should be deleted or discarded within the shortest time possible, unless the agency can make a clear showing in a judicial body that it or another agency requires the data for an ongoing national security investigation.[253]

Finally, to improve transparency and oversight, private companies should be permitted to disclose the number and type of government requests they receive. The government should also report annually how it queries and

247. 407 U.S. 297, 299 (1972).

248. *Id*. at 317.

249. Goldenziel & Cheema, *supra* note 8, at 120.

250. *Cf.* Berman, *supra* note 89, at 76; *see also* LORETTA E. LYNCH, U.S. DEP'T OF JUSTICE, EXHIBIT B: MINIMIZATION PROCEDURES USED BY THE FEDERAL BUREAU OF INVESTIGATION IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978, AS AMENDED 4 (2016), https://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf.

251. 50 U.S.C. § 1881a(h) (2012).

252. *Id*. §§ 1801(h)(2), 1821(4)(B); *In re* All Matters Submitted to FISA, 218 F. Supp. 2d 611, 618 (FISA Ct. 2002).

253. *Cf.* Berman, *supra* note 89, at 77; [REDACTED], No. PR/TT [REDACTED], 2011 WL 10945618, at *1, *21 (FISA Ct. Oct. 3, 2011).

uses USPERs' communications. Congress and the courts must not abdicate their responsibility for providing oversight over electronic surveillance programs. As the ease of surveillance grows and its use becomes more prevalent, safeguarding constitutional liberties becomes increasingly essential.

V. CONCLUSION

In the fight against foreign information operations, the United States must reform its laws to ensure the integrity of the electoral process, while at the same time protecting civil liberties. The current framework and protections of FISA are a product of several rounds of congressional amendment and national debate about how to balance critical national security interests and civil liberties. While imperfect, FISA is a suitable reference and starting point for the development of any legislation countering information campaigns: the warrant requirement, minimization procedures, certification process, and transparency-creating measures all should characterize that legislation in order to protect civil liberties. The United States must combat information warfare that challenges the foundations of American democracy. However, this fight cannot compromise the constitutional rights of USPERs.