Toward Institutional Reform of Intelligence Surveillance: A Proposal to Amend the Foreign Intelligence Surveillance Act

*Tyler C. Anderson**

In the next year, reforming the manner in which intelligence agencies conduct surveillance will be a national priority. As recent events like the Boston Marathon bombing have shown, gathering effective intelligence to prevent national security threats remains a pressing goal for policymakers. Nevertheless, the current statutory framework, an expansive amendment to the Foreign Intelligence Surveillance Act passed by Congress in 2008 and renewed in late 2012, has been almost universally criticized by policymakers, legal academics, and members of the general public from across the political spectrum. Congress itself was deeply unsatisfied with the Act, including within it a narrow sunset provision with the intention of substantially revising the act at the end of 2012. Despite near-consensus on the need for reform outside the National Security Administration (NSA) itself, Congress renewed the act with minimal floor debate and a nearly unanimous vote. Now, because of the myriad problems associated with intelligence surveillance (many of which were recently disclosed by Edward Snowden and The Guardian newspaper), the Obama Administration has released a plan to overhaul the Foreign Intelligence Surveillance Act (FISA) surveillance law. While President Obama's "NSA speech" offers a helpful starting point, this paper argues that further reforms will be required to end the abusive NSA practices that began under President George W. Bush and continued under the current administration. In doing so, this paper summarizes current intelligence surveillance law and proposes legislative language that Congress should adopt in implementing reforms that protect the fundamental privacy of American citizens.

I. Introduction

"[T]he capacity to devise institutions and procedures adequate to its problems is perhaps the chief mark of a civilized society."
— Lon Fuller[1]

While Edward Snowden's recent disclosures have thrown many of the NSA's surveillance overreaches into public scrutiny and demonstrated the need for the amendments to the Foreign Intelligence Surveillance Act (FISA) proposed in this article,[2] to understand the current structure of intelligence surveillance law, it is important to contextualize it within the Bush-era scandal that gave it birth. On December 16, 2005, the *New York Times* ex-

* J.D Candidate, Harvard Law School, Class of 2014. The author gratefully acknowledges the helpful guidance and input provided by professors James Baker, Juan Zarate, Yochai Benkler, and Jack Goldsmith. The author would also like to thank Matt Nickel, Jean Ripley, and the members of the Harvard Law & Policy Review for their advice and editing assistance.

[1] Lon L. Fuller, The Morality of Law 181 (2d ed. 1969).

[2] *See, e.g.*, Mirren Gidda, *Edward Snowden and the NSA Files – Timeline*, The Guardian (July 25, 2013), http://www.guardian.co.uk/world/2013/jun/23/edward-snowden-nsa-files-timeline?INTCMP=SRCH; Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. Times (July 6, 2013), http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html?pagewanted=all&_r=0.

posed a shocking breach of the Fourth Amendment. According to government officials, in response to the national security emergency on September 11, 2001, "President Bush secretly authorized the National Security Agency [NSA] to eavesdrop on Americans and others inside the United States to search for evidence of terrorist activity without the court-approved warrants ordinarily required for domestic spying."[3] After *The New York Times* brought President Bush's warrantless wiretapping program to public attention, the program faced widespread criticism from pundits, law professors, and civil libertarians on the left and the right.[4] Attorney General Alberto Gonzales responded by arguing that because of the national security emergency triggered by 9/11, the government had a compelling reason to circumvent normal[5] Fourth Amendment procedures.[6] Because of the need for updated and expedited wiretapping procedures, Congress essentially adopted President Bush's wiretapping program,[7] while attaching to it minimal institutional safeguards.[8] To do so, Congress first passed the stopgap 2007 Protect

---

[3] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all.

[4] *See* Curtis A. Bradley et al., *A Response to the Justice Department from Law Professors and Former Government Officials* (Jan. 9, 2006), http://www.fas.org/irp/agency/doj/fisa/doj-response.pdf.

[5] In surveillance done for national security purposes, Congress and the Fourth Amendment typically require that the NSA go to a special Foreign Intelligence Surveillance Act Court (the FISC) in order to obtain a wiretapping warrant. *See* 50 U.S.C. §§ 1881a(i), 1881b(c), 1881c(c).

[6] The core of Gonzales' speech was that, "It is imperative for national security that we can detect [terrorist threats] RELIABLY, IMMEDIATELY, and WITHOUT DELAY. . . . Consistent with the wartime intelligence nature of this program, the optimal way to achieve the necessary speed and agility is to leave the decisions about particular intercepts to the judgment of professional intelligence officers." Alberto Gonzales, U.S. Att'y Gen., Prepared Remarks for Attorney General Alberto R. Gonzales at the Georgetown University Law Center (Jan. 24, 2006), *in* U.S. Dep't of Justice Archives, http://www.justice.gov/archive/ag/speeches/2006/ag_speech_0601241.html.

[7] *See* FISA Amendments Act (FAA), 50 U.S.C. §§ 1881a(I)(3)(A) (2012); STEPHEN DYCUS, ARTHUR L. BERNEY, WILLIAM C. BANKS, & PETER RAVEN-HANSEN, NATIONAL SECURITY LAW 620 (5th ed. 2011) ("After a FISC judge approves the program features, the Attorney General and DNI authorize the surveillance program —without the need to obtain judicial orders for individual targets"). As the FISA Court of Review held in *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, wiretaps under the Protect America Act (to which the FAA is substantially similar) do not need to specify targets with particularity, and do not need to be reviewed by FISA judges ex-ante. 551 F.3d 1004, 1014 (FISA Ct. Rev. 2008).

[8] *See* JACK GOLDSMITH, POWER AND CONSTRAINT: THE ACCOUNTABLE PRESIDENCY AFTER 9/11 16–17 (2012). It is probably more accurate to state that the Protect America Act (PAA) and then the FISA Amendment Act (FAA) formalized some of the institutional safeguards the President had already put in place. By the end of President Bush's warrantless wiretapping program, both Congress and the Judiciary already knew and had perhaps authorized the program, therefore it is unclear that the congressional oversight established under the PAA and then the FAA significantly modified the preexisting arrangement. *See, e.g.*, DYCUS ET AL., *supra* note 7, at 619 (arguing that at least one federal judge had approved the program); U.S. Dep't of Justice, Letter from William E. Moschella, Assistant Att'y Gen., to The Honorable Pat Roberts, Chairman, Senate Select Comm. on Intelligence, et al. (Dec. 22, 2005) *available at* http://www.fas.org/irp/agency/doj/fisa/doj122205.pdf ("Leaders of Congress were briefed on these activities more than a dozen times.").

America Act (PAA),[9] and then in 2008 passed the Foreign Intelligence Surveillance Act Amendments Act (FAA).[10] At the end of 2012, the FAA came before Congress for renewal. Despite widespread criticism of the act by many members of Congress and the public, Congress reauthorized the act without reassessing or limiting many of the act's more troubling provisions.[11] As we now know, the NSA has used these provisions to conduct extensive surveillance on the American people in pursuit of total informational awareness while deliberately misleading the public about the extent of NSA surveillance.[12]

This paper argues that Congress made a mistake—a mistake that ought to be redressed through a series of legislative amendments. As recent disclosures have made plain, FAA-governed intelligence surveillance is in need of reform, and the recent report commissioned by President Obama[13] and the pressure placed on the administration by the Snowden leaks create a perfect opportunity for progressive policymakers. Reform efforts failed despite near-universal consensus on the need for reform and broad agreement about the scope of reform outside the intelligence community.[14] These efforts failed because of limited public knowledge of NSA surveillance programs,[15]

---

[9] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552.

[10] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436, 2437-78 (codified 50 U.S.C. §§ 1801–12 (2012)).

[11] *See* FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat. 1631.

[12] *See, e.g.*, Dan Roberts & Spencer Ackerman, *Clapper Under Pressure Despite Apology for 'Erroneous' Statements to Congress*, THE GUARDIAN (July 1, 2013), http://www.theguardian.com/world/2013/jul/01/james-clapper-apology-congress-erroneous-response; Risen & Lichtblau, *supra* note 3.

[13] PRESIDENT'S REVIEW GRP. ON SURVEILLANCE & COMMC'N TECHNOLOGIES, LIBERTY AND SECURITY IN A CHANGING WORLD (2013), *available at* http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf [hereinafter PRESIDENT'S REVIEW GRP.].

[14] This consensus extends from institutional giants like Richard Posner and Jack Balkin to center-right law professors like David Kris and Robert Chesney. It also includes civil libertarians like Rand Paul and the ACLU plus institutional liberals like President Obama. *See, e.g.*, David Kris, *Thoughts on a Blue-Sky Overhaul of Surveillance Laws: Introduction*, LAWFARE (May 18, 2013, 11:00 AM), http://www.lawfareblog.com/2013/05/thoughts-on-a-blue-sky-overhaul-of-surveillance-laws-introduction/ ("[The FAA] resolved two difficult issues, at least for the short run."); Amy Schatz, *Paul Camp, Liberals Unite on Spy Bill*, WALL ST. J., June 26, 2008, http://online.wsj.com/news/articles/SB121443403835305037; Robert Chesney, *The Foreign/Domestic Divide and the Legal Architecture of "Domestic Intelligence,"* LAWFARE (Oct. 6 2010, 11:06 AM), http://www.lawfareblog.com/2010/10/the-foreigndomestic-divide-and-the-legal-architecture-of-domestic-intelligence/ ("Of course, now might also be a good time to pause to take stock of the legal architecture of domestic intelligence with respect even to wholly domestic threats."); GOLDSMITH, *supra* note 8, at 16; *see also infra* Part III (comparing academic proposals on modifying the FAA). *Compare* H.R. Rep. No. 112-645, at 10–11 (2012), http://www.gpo.gov/fdsys/pkg/CRPT-112hrpt645/html/CRPT-112hrpt645-pt1.htm, *with* Ellen Nakashima, *Senate Approves Measure to Renew Controversial Surveillance Authority*, WASH. POST, Dec. 28, 2012, http://www.washingtonpost.com/world/national-security/senate-approves-measure-to-renew-controversial-surveillance-authority/2012/12/28/4353905c-50fc-11e2-8b49-64675006147f_story.html (describing the broadly held view in the Senate that the FAA needs to be reformed).

[15] *See, e.g.*, Gidda, *supra* note 2; Risen & Lichtblau, *supra* note 3.

the shift to a Democratic administration,[16] and the focus on challenging the constitutionality of FISA[17] demobilized activists while media attention on the rise of drone warfare and legislative budget battles eclipsed smaller-scale, bipartisan reform efforts in Congress.[18] Fortunately, the effort to reform FISA has not ended, and the President has stated that he plans to accept many of the recent reform proposals.[19] Additionally, because of the disclo-

---

[16] For a sense of how civil liberties advocates bought into the notion that the election of Barack Obama itself would end civil-liberties abuses, *see* Dana Priest, *Bush's "War" on Terror Comes to a Sudden End*, WASH. POST (Jan. 23, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/01/22/AR2009012203929.html ("[President Obama] effectively declared an end to the 'war on terror,' as President George W. Bush had defined it, signaling to the world that the reach of the U.S. government in battling its enemies will not be limitless."). Nevertheless, President Obama has continued many of President Bush's surveillance policies. *See* GOLDSMITH, *supra* note 8, at 15–17; Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES (Sept. 27, 2010), http://www.nytimes.com/2010/09/27/us/27wiretap.html?pagewanted=all.

[17] *See, e.g.*, Eric Posner, *Why Amnesty Should Lose at the Supreme Court: It's Not the Job of Judges to Stop Warrantless Wiretapping*, SLATE (Oct. 26, 2012), http://www.slate.com/articles/news_and_politics/view_from_chicago/2012/10/amnesty_s_challenge_of_surveillance_at_the_supreme_court.html; *Clapper v. Amnesty Int'l*, 133 S. Ct. 1138 (2013); ACLU, *Establishing a New Normal: National Security, Civil Liberties, and Human Rights Under the Obama Administration: An 18-Month Review* at 16 (July 2010), *available at* https://www.aclu.org/national-security/establishing-new-normal; *cf.* Jack Goldsmith, *ACLU Opposes FISA-Like Judicial Review of Drone Strikes*, LAWFARE (Feb. 9, 2013, 11:42 AM), http://www.lawfareblog.com/2013/02/aclu-opposes-fisa-like-judicial-review-of-drone-strikes/ ("[describing problems relating to] what can happen when objections about the substance of a practice are articulated through lawsuits and arguments about legal foundations, separation of powers, and process").

[18] *See, e.g.*, Editorial, *The Power to Kill*, N.Y. TIMES (Mar. 11, 2012), http://www.nytimes.com/2012/03/11/opinion/sunday/the-power-to-kill.html; John B. Bellinger III, *Will Drone Strikes Become Obama's Guantanamo?*, WASH. POST (Oct. 2, 2011), http://www.washingtonpost.com/opinions/will-drone-strikes-become-obamas-guantanamo/2011/09/30/gIQA0ReIGL_story.html; Tara Mckelvey, *Inside the Killing Machine*, NEWSWEEK (Feb. 15, 2011), http://www.newsweek.com/inside-killing-machine-68771; *cf.* Harold Hongju Koh, U.S. Dep't of State Legal Advisor, The Obama Administration and International Law (Mar. 25, 2010), *in* U.S. Dep't of State Archives, http://www.state.gov/s/l/releases/remarks/139119.htm.

[19] Most importantly, President Obama has committed to warehousing NSA-collected data in a location not controlled by the NSA, adopting adversarial procedures within the FISA court (FISC), and limiting the scope of incidental data collection. *See* Barack Obama, U.S. President, Remarks on National Security Agency Data Collection Programs (Jan. 17, 2014), *available at Obama's Speech on N.S.A. Phone Surveillance*, N.Y. TIMES (Jan. 17, 2014), http://www.nytimes.com/2014/01/18/us/politics/obamas-speech-on-nsa-phone-surveillance.html. I conclude by evaluating some of Obama's proposals for reforming FISA and translating them into appropriate legislative language for congressional enactment. Within the White House, it has been clear even before the Snowden disclosures that something needed to be done to reform intelligence surveillance. *See, e.g.*, Charlie Savage, *U.S. Weighs Wide Overhaul of Wiretap Laws*, N.Y. TIMES (May 7, 2013), http://www.nytimes.com/2013/05/08/us/politics/obama-may-back-fbi-plan-to-wiretap-web-users.html?pagewanted=all; Kris, *supra* note 14. While these types of proposals have been circulating for some time, the recommendations of the Privacy and Civil Liberties Oversight Board and the Presidential Review Group give the President some additional political cover in making specific recommendations. *See, e.g.*, PRIVACY & CIVIL LIBERTIES OVERSIGHT BD., Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court 200 (2014), *available at* http://www.pclob.gov/SiteAssets/Pages/default/PCLOB-Report-on-the-Telephone-Records-Program.pdf (arguing for broader declassification) [hereinafter PCLOB Report]; PRESIDENT'S REVIEW GRP., *supra* note 13.

sures by *The Guardian* regarding actual NSA operation and procedure, Congress has begun to seriously consider several proposals for surveillance reform independent of those proposed by the President, including a prohibition on backdoor searches, reverse targeting, and the use of National Security Letters to bulk-collect information.[20]

Typically, critics of the FAA focus on the privacy-violating aspects of intelligence surveillance,[21] and the rule-of-law implications of the FAA.[22] Specifically, critics (including the Obama-appointed taskforce) argue that the FAA delegates too much surveillance authority to intelligence agencies and also overly reduces the role of the Foreign Intelligence Surveillance Court in supervising the exercise of this authority.[23] This paper provides an overview of current FAA law, summarizes some of the more prevalent criticisms of the FAA, proposes language Congress could use in amending the FAA to restrict the scope of the surveillance intelligence agencies can conduct, and addresses some of the counter-arguments to FAA reform. First, Congress should substantially clarify the FAA by more precisely defining the conduct that warrants targeting under the act. Second, Congress should mandate independent oversight of surveillance activity including adversarial hearings during the warrant-issuing process to ensure that intelligence agencies do not exceed the authority granted under the FAA. Third, Congress should codify the language President Obama issued in Presidential Policy Directive 28 promising not to use NSA-gathered intelligence to target domestic political dissidents.[24] Fourth, while the White House has a clear interest in restricting the public disclosure of surveillance targets (which would undermine critical surveillance operations), Congress should nevertheless mandate the periodic declassification of FISC opinions and NSA minimization procedures to ensure that the FAA is used only for its intended pur-

---

[20] *Compare* Senator Ron Wyden, *What Does the Intelligence Oversight and Surveillance Reform Act Do?* (2013), http://www.wyden.senate.gov/download/?id=4d1fb49b-3093-4c81-8060-6c2dc14da90f&download=1, *with* Obama, *supra* note 19; Spencer Ackerman, *U.S. House Bill Would Force Obama to Declassify FISA Court Decisions*, THE GUARDIAN (June 20, 2013), http://www.guardian.co.uk/world/2013/jun/20/house-obama-declassify-fisa-court.

[21] *See* ELIZABETH B. BAZAN, CONG. RESEARCH SERV., RL34566, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: A SKETCH OF SELECTED ISSUES (2008) (discussing the criticisms traditionally leveled at FISA); *see also* Lichtblau, *supra* note 2.

[22] *See, e.g.*, Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 25 (2008) (describing the rule-of-law concerns surrounding the FAA); *Restoring the Rule of Law: Hearing Before the S. Subcomm. on the Constitution of the S. Comm. on the Judiciary*, 110th Cong. 14–15 (2008) (statement of Harold Hongju Koh, Dean and Gerard C. & Bernice Latrobe Smith Professor of International Law, Yale Law School); Risen & Lichtblau, *supra* note 3.

[23] PRESIDENT'S REVIEW GRP., *supra* note 13. *See also* Letter from I. Charles McCullough III, Inspector Gen. of Intelligence Cmty., to Sens. Ron Wyden & Mark Udall (June 15, 2012), *available at* WIRED MAG., http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf (last visited May 8, 2014) (seeking to assuage the rule-of-law concerns of Senators Wyden and Udall).

[24] Press Release, White House Press Office, Presidential Policy Directive—Signals Intelligence Activities (Jan. 17, 2014), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

pose.[25] Finally, this piece contextualizes the post-Snowden FAA critique within the existing debate on executive power in national security by addressing some of the prominent public choice arguments used to justify a legally unbound Executive, including damage to the President's party during elections and insubordination by officials tasked with carrying out surveillance.

II. An Overview of the Foreign Intelligence Surveillance Act Amendments Act

This section provides an overview of the content and application of the current FISA statute as well as its relevant legislative history. In brief, Congress enacted the FAA in order to grant executive branch agencies broader surveillance power than they had under the original FISA. The FAA accomplishes this while simultaneously limiting the judicial oversight provided by the Foreign Intelligence Surveillance Court (FISC). First, the FAA updates FISA by abolishing the methodological distinctions FISA placed on different types of electronic surveillance (e.g. the distinction between wiretapping phone lines and intercepting radio waves). In its place, the FAA establishes a uniform process for seeking judicial authorization of electronic surveillance regardless of the type of communication being monitored. Second, the FAA further creates a broad category of intelligence surveillance that is not subject to ex-ante judicial scrutiny and is only subject to limited *ex-post* judicial review.[26]

A. History and Purpose of the Foreign Intelligence Surveillance Act Amendments Act

It is impossible to understand the FAA without understanding the problem it was meant to solve. Congress passed the original FISA (the act that the FAA modifies) in order to help American intelligence agencies conduct surveillance in a pre-internet, pre-cellphone era.[27] More specifically, in 1978 Congress designed the original FISA to deal with landline communication in the age of corded telephones and radio. Congress wanted to give the intelligence agencies broad power to spy on non-U.S. citizens abroad, while protecting to the fullest extent possible the privacy of U.S. persons within the United States.[28] In order to achieve this objective, Congress limited the

---

[25] Professor William Banks and the National Research Council have proposed independent oversight committees along these lines. *See e.g.*, William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 Tex. L. Rev. 1633, 1661 (2010); *Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Program Assessment*, Nat'l Research Council 3–4 (2008), http://epic.org/misc/nrc_rept_100708.pdf.

[26] *See infra* Table 1.

[27] *See* H.R. Rep. No. 25-1283, pt. I, at 25 (1978); *see also* United States v. Duggan, 743 F.2d 59, 69–70 (2d. Cir. 1984) (interpreting FISA's legislative history).

[28] *Duggan*, 743 F.2d at 73–74.

President's power to spy based on both geographic territory and the type of communication a given intelligence agency planned on intercepting.[29] Congress drew a sharp distinction between eavesdropping on radio communications (which at that time were mostly domestic), and eavesdropping on wire communications (which were mostly international).[30] For radio surveillance, only communications with a "reasonable expectation of privacy" between non-U.S. persons where at least one party was within the United States required FISA warrants.[31] In contrast, all wire communications with at least one party within the United States required FISA warrants.[32] However, by the turn of the twenty-first century, increased access to the internet and cellular phones had significantly blurred the lines Congress had drawn between international/wired communication and domestic/radio communication.[33]

After the terrorist attacks on the World Trade Center and Pentagon on September 11, 2001, President Bush realized he possessed inadequate tools under FISA to conduct electronic surveillance on wireless international conversations taking place over cellphones and other forms of digital communication.[34] In response, he initiated a warrantless wiretapping program.[35] When the program came before the U.S. Department of Justice's Office of Legal Counsel (OLC), John Yoo (an aggressively pro-executive-power legal scholar who was also the only member of the OLC authorized to comment on, or even know about, the existence of the program)[36] wrote a memo justifying the program under the President's inherent wartime powers as Commander-in-Chief.[37] Once *The New York Times* published its story on the program, public outcry ensued and Congress initiated an investigation.[38]

One issue was that the Yoo Memo failed to cite the definitive case on presidential power: *Youngstown Sheet & Tube Co. v. Sawyer*.[39] According to Justice Jackson's concurring opinion (the now-canonical part of the Supreme

---

[29] 50 U.S.C. § 1801(f) (2012); *see also* United States v. Koyomejian, 946 F.2d 1450, 1456 (9th Cir. 1992).

[30] 50 U.S.C. § 1801(f).

[31] *Id.* § 1801(f)(3).

[32] *Id.* § 1801(f)(2).

[33] For a thorough and interesting account of this technological shift, see ANDREW BLUM, TUBES: A JOURNEY TO THE CENTER OF THE INTERNET (2012).

[34] *See* OFFICES OF INSPECTORS GEN. OF THE DEP'T OF DEF. ET AL., REPORT NO. 2009-0013-AS, UNCLASSIFIED REPORT ON THE PRESIDENT'S SURVEILLANCE PROGRAM 5 (2009), [hereinafter PSP REPORT], *available at* http://www.dodig.mil/Ir/reports/s0907.pdf.

[35] *Compare* 50 U.S.C. § 1801(f), *with* DYCUS ET AL., *supra* note 7, at 608–09 (illuminating the challenges the President faced conducting FISA surveillance of email); *see also* EDWARD C. LIU, CONG. RESEARCH SERV., R42725, REAUTHORIZATION OF THE FISA AMENDMENTS ACT 7 (2013) (discussing the changes FISA made to 50 U.S.C. § 1801(f)(2)).

[36] *See* PSP REPORT, *supra* note 34, at 10–18; *see also* MICHAEL C. DORF, THE TORTURE DEBATE IN AMERICA 248 (Karen J. Greenberg ed., 2005) ("OLC memos do not have the force of law in quite the way that opinions of the Supreme Court do, but neither are they mere opinion pieces . . . . OLC is often asked to address constitutional issues that will never [sic] make it to court—what lawyers call nonjusticiable political questions. In these circumstances, the formal advice of OLC may be the only sort of 'precedent' that exists.").

[37] *See* PSP REPORT, *supra* note 34, at 10–18.

[38] *See* DYCUS ET AL., *supra* note 7, at 608–09 (citing Risen & Lichtblau, *supra*) note 31.

[39] 343 U.S. 579 (1952).

Court opinion), the President has the most authority to act if Congress has directly delegated power to act to the President. The President may have some authority to act when Congress is silent on the issue in question. The President has the *least* power to act when he acts contrary to Congress's explicit or implied direction.[40] Here, the argument that the congressional investigation made under the Inspector General's Report on the President's Surveillance Program (PSP Report) is that since Congress had already authorized an analogous wiretapping program in FISA, the President should have gone through the FISA-authorized process in order to wiretap conversations under the PSP.[41]

Ultimately, Congress determined that the President's initial assessment of the threat was right: FISA alone did not grant the President sufficient authority to conduct twenty-first century electronic surveillance of email, cellphones, and mass electronic communication.[42] Due to this compelling need, Congress decided to pass a deeply controversial law that would authorize the type of surveillance conducted under the warrantless wiretapping program and chose to limit the law by including a narrow sunset provision.[43] The result was the FAA.

B. Summary of the Foreign Intelligence Surveillance Act Amendments Act

The FAA modifies the original FISA by creating "new separate procedures for targeting [for surveillance] non-U.S. persons and U.S. persons reasonably believed to be outside the United States."[44] The new procedure contains two steps: first, a federal agency determines the target of electronic surveillance and the method of surveillance, subject to approval by the Attorney General; second, the relevant agency submits an application for a FISA warrant to the Foreign Intelligence Surveillance Court (FISC), which reviews the agency's targeting procedures to determine their consistency with the FAA and the Fourth Amendment's search-and-seizure provisions.[45] This section discusses each of these steps in turn.

1. *The First Step: Determining the Target and Method of Surveillance*

When intelligence agencies use the FAA, they must first decide on a target and method of surveillance. The FAA supersedes the procedures out-

---

[40] *Id.* at 635–38.

[41] *See* PSP REPORT, *supra* note 34, at 13.

[42] *See id.* at 5; *compare* 50 U.S.C. § 1801(f), *with* DYCUS ET AL., *supra* note 7, at 608–09 (illuminating the challenges the President faced conducting surveillance of email under FISA); *see also* LIU, *supra* note 35, at 7 (discussing the changes the FAA made to 50 U.S.C. § 1801 (f)(2)).

[43] *See* Bazan, *supra* note 21, at 1–3.

[44] LIU, *supra* note 35.

[45] *See, e.g.*, 50 U.S.C. § 1881a(i); *id.* § 1881b(c); *id.* § 1881c(c).

Table 1: Summary of Surveillance Authorized Under Different Sections of the FAA.

Provision of the U.S. Code	Targets Authorized	Judicial Review by the FISC
50 U.S.C. § 1881a	Targets are non-U.S. persons reasonably believed to be outside the United States, but the targeting agency collects the target's data inside the United States.	Ex-post authorization. Review is based on category of targets.
50 U.S.C. § 1881b	Targets are U.S. persons outside the United States, but the targeting agency collects the target's data inside the United States.	Ex-ante authorization. Review is based on individual targets.
50 U.S.C. § 1881c	Targets are U.S. persons outside the United States and the targeting agency collects the target's data outside the United States.	Ex-ante authorization. Review is based on individual targets. Surveillance is not limited to data collection.

lined in the original FISA, relaxing the requirements regarding radio and wire communications.[46] Instead, the FAA allows a targeting agency to conduct electronic surveillance in three different scenarios regardless of the type of communication being monitored: (1) the targeting of non-U.S. persons overseas; (2) the targeting of U.S. persons overseas whose data the agency gathers inside the United States; and (3) the targeting of U.S. persons overseas whose data the agency gathers overseas.

Targeting Non-U.S. Persons Overseas: The first type of target the government can select for surveillance, governed by 50 U.S.C. § 1881a, is an overseas person or entity that is not a U.S. person. Here, the FAA gives the President broad power: "upon the issuance of an order . . . the Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to one year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[47] This provision of the FAA has perhaps the most sweeping rule-of-law implications. Because this section of the FAA drastically diminishes the FISC review of intelligence activity and instead grants broad power to the Director of National Intelligence and the Attorney General, and because this section only requires that the intelligence agency not "*intentionally* target a U.S. person," (and by implication, such a person may be a collateral target of data collection)[48] this provision, in combination with Section 215 of the PATRIOT Act (which

[46] *Compare* 50 U.S.C. §§ 1881a, 1881b, 1881c(a)(2), *with* 50 U.S.C. § 1801(f); *see also* LIU, *supra* note 35, at 7.

[47] 50 U.S.C. § 1881a(a).

[48] *Id.* § 1881a(b)(3) (emphasis added).

covers the method of collecting NSA-collected data)[49] has borne the brunt of the act's criticism.[50]

Acquisitions Inside the United States Targeting U.S. Persons Overseas: The second type of surveillance, governed by 50 U.S.C. § 1881b, covers situations where the target of the surveillance is overseas, but the surveillance itself involves gathering electronic communications or stored electronic communications acquired in the United States.[51] This type of data collection is much more common now than it was when Congress originally passed FISA since so much internet traffic flows through the United States, even when the parties communicating are all overseas.[52] Unlike 50 U.S.C. § 1881a, discussed above, 50 U.S.C. § 1881b still requires individual targeting and ex-ante review, much like the original FISA. However, unlike FISA, here the wire/radio distinction has been abolished.[53] In order to conduct surveillance, the targeting agency must submit a FISA warrant application, approved by the Attorney General, to the FISC.[54]

Acquisitions Targeting U.S. Persons Overseas: The third type of target, governed by 50 U.S.C. § 1881c, is a U.S. person outside the United States where data acquisition also occurs outside the United States.[55] This provision also allows action beyond electronic surveillance or the acquisition of stored communications or data (e.g. physical searches by intelligence personnel).[56] Interestingly, unlike the other provisions of the FAA (which are largely meant to streamline intelligence acquisition), 1881c actually strengthens privacy protection compared to the original FISA. This is because both pre-FAA sources of authority for electronic surveillance—FISA warrants and law enforcement warrants under Title III—"have been understood to apply only to interceptions [i.e. data collection] within the United States."[57] Essentially, before the FAA, data acquisitions overseas were unprotected.[58] Beyond the new application of FISA procedures to data acquisition overseas, Section 1881c is essentially the same as Section 1881b. In order to conduct surveillance, the targeting agency must submit a FISA warrant application, approved by the attorney general, to the FISC.[59] Additionally, 1881c authorizes data collection beyond electronic surveillance or the

---

[49] *See In re* Application of the FBI for an Order Requiring the Production of Tangible Things from [Redacted], No. BR 14-01 at 1–3 (FISA Ct. Jan. 3, 2014), http://www.uscourts.gov/uscourts/courts/fisc/br13-09-primary-order.pdf.

[50] *See* BAZAN, *supra* note 21 (discussing the criticisms leveled at the FAA).

[51] 50 U.S.C. § 1881b.

[52] *See* BLUM, *supra* note 33, at 27.

[53] 50 U.S.C. § 1881b(a)(1)–(2).

[54] *Id.* § 1881b(b).

[55] *Id.* § 1881c(a)(1)–(2).

[56] *See id.*

[57] GINA STEVENS & CHARLES DOYLE, CONG. RESEARCH SERV., 98–327, PRIVACY: AN ABBREVIATED OUTLINE OF FEDERAL STATUTES GOVERNING WIRETAPPING AND ELECTRONIC EAVESDROPPING 14 (2012).

[58] *See* 50 U.S.C. § 1801(c)(2)(C).

[59] *Id.* § 1881c(b).

acquisition of stored electronic information, such as physical searches and seizures.[60]

2. *The Second Step: Judicial Authorization for FAA Surveillance*

The second part of the FAA requires that a targeting agency submit its target specifications and methods to the FISC for review.[61] Sections 1881b and 1881c mandate FISC review that is both ex-ante and target specific, similar to the review under the original FISA.[62] By contrast, Section 1881a has drastically reduced the potential for FISC review (this provision is often attacked by civil libertarians); it requires neither ex-ante review nor target-specific review.[63]

Sections 1881b and 1881c: Under these two sections of the statute, judicial authorization begins either with the targeting agency presenting its targeting certification to the FISC for approval[64] or with a determination by the Attorney General that exigent circumstances warrant timely authorization prior to court approval.[65] In order to receive certification, the FISC must find that the Attorney General has approved the application, that the agency has probable cause to believe that the target is both a person reasonably believed to be located outside the United States and an agent of a foreign power, and that surveillance will follow the statutorily required minimization procedures and that those minimization procedures will be consistent with the Fourth Amendment.[66] After the FISC reviews the agency's application, the FISC issues a court order describing the identity of the target, the method of surveillance, nature of information sought, and duration of the order.[67] The FISC also immunizes communication service providers who assist with the surveillance.[68]

Section 1881a: Section 1881b, Section 1881c, and the original FISA all require FISC warrants for each individual act of surveillance.[69] In contrast, Section 1881a calls for minimal judicial scrutiny and surveillance authorization.[70] Under 1881a, agencies do not apply for individual FISA warrants.[71] Instead, the Attorney General and the Director of National Intelligence can make a much broader, non-individualized determination about the types of

---

[60] *Compare* 50 U.S.C. § 1881b(a)(1), *with* 50 U.S.C. § 1881c(a)(1).
[61] *See, e.g.*, 50 U.S.C. § 1881a(i); *id.* § 1881b(c); *id.* § 1881c(c).
[62] *Id.* § 1881b(c); *id.* § 1881c(c); *see* STEVENS & DOYLE, *supra* note 57, at 14.
[63] *See* 50 U.S.C. § 1881a(i).
[64] *See, e.g.*, *id.* § 1881b(c); *id.* § 1881c(c).
[65] 50 U.S.C. § 1881b(d); *id.* § 1881c(d).
[66] *See, e.g.*, 50 U.S.C. § 1881b(c)(1); *id.* § 1881c(c)(1); *see* STEVENS & DOYLE, *supra* note 57, at 13–14.
[67] *See, e.g.*, 50 U.S.C. § 1881b(c); *id.* § 1881c(c).
[68] 50 U.S.C. § 1881b(c)(5); *id.* § 1881c(c)(5); *see* STEVENS & DOYLE, *supra* note 57, at 13.
[69] *See, e.g.*, 50 U.S.C. § 1881b(1)(B); *id.* U.S.C. § 1881c(1)(B).
[70] *See* 50 U.S.C. § 1881a(a).
[71] *See* LIU, *supra* note 35, at 4–7.

people to be targeted. No court order is necessary ex-ante.[72] However, after the Attorney General and Director of National Intelligence have made a determination, they must submit a written certification and affidavit summarizing the targeting procedures to be used for surveillance to the FISC.[73] While the FISC can review and reject the certification,[74] the breadth of a Section 1881a warrant is much greater than the previous, individually targeted warrants under FISA.[75] Under Section 1881a, the FISC's review of the proposed surveillance is limited to ensuring that the proposed targeting procedures are confined to targeting persons reasonably believed to be located outside the United States, preventing the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States, and ensuring that the targeting agency follows the statutorily required minimization procedures and that those minimization procedures are consistent with the Fourth Amendment.[76]

3. *A Brief Summary of the Criticism of the FAA*

As detailed above, the FAA grants agencies conducting electronic surveillance broad power with relatively minimal oversight. For this reason, critics have attacked the bill since its first passage,[77] often asserting that it essentially normalizes President Bush's warrantless wiretapping program.[78] One of the most criticized sections, codified at 50 U.S.C. § 1881a (but often called Section 702 after the public law), allows agencies to conduct surveillance without applying for target-specific FISA warrants.[79] Instead, the Attorney General and the Director of National Intelligence can categorically declare that a specific type of surveillance against a particular type of target is necessary.[80] Additionally, under Section 1881a, the FISC's review of the proposed surveillance is substantially limited and only occurs after the surveillance has already begun.[81] The FAA also couples the expansion of agency authority generally with robust emergency provisions that tempora-

---

[72] *See* 50 U.S.C. § 1881a(b).
[73] *Id.* § 1881a(g).
[74] *Id.* § 1881a(i).
[75] *See* Banks, *supra* note 25, at 1654*; see also* STEVENS & DOYLE, *supra* note 57, at 11–14.
[76] *See* 50 U.S.C § 1881a(i)(2)(A)–(C).
[77] *See, e.g.*, Steve Vladeck, *More on Clapper and the Foreign Intelligence Surveillance Exception*, LAWFARE (May 23, 2012, 3:32 PM), http://www.lawfareblog.com/2012/05/more-on-clapper/ ("Congress in the FAA (building on the Protect America Act of 2007) specifically authorized programmatic warrantless foreign intelligence surveillance in a manner *almost guaranteed* to sweep up a substantial volume of communications involving U.S. persons.") (emphasis in original).
[78] *See* GOLDSMITH, *supra* note 8, at 16. ("In the summer of 2008, candidate Obama voted to put President Bush's unilateral warrantless wiretapping program, which he had opposed as an abuse of presidential power, on a legally more defensible statutory basis.").
[79] *See supra* Part II.
[80] *See supra* Part II.
[81] *See supra* Part II.

rily grant intelligence agencies even broader power. In these instances, the FAA explicitly provides the Attorney General with the power to determine exceptions to the already-flexible FAA warrant procedure.[82]

In addition to the troubling implications that arise from enhanced intelligence agency authority, critics have attacked the FAA because the surveillance program is too opaque for the public to understand how the law functions even when it functions well.[83] As the FISA Court of Review (the appellate court that oversees the FAA) reasoned in one of its foundational cases, *In re Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act*, the plaintiff's claim against the Protect America Act (PAA, the FAA's precursor, to which the FAA is in many ways identical) failed in part because the plaintiff, an unnamed telecommunications firm concerned with NSA interception of its clients' communications, did not understand how the law functions in practice.[84] The court called some of the plaintiff's assertions about the application of the law "overblown" and stated that the government does not engage in the abusive practices under the PAA that the plaintiff suspected.[85] Nevertheless, to the broader public, the heavily redacted opinion was largely construed as a vindication of the Bush-era wiretapping strategy that the PAA and later the FAA instantiated into law.[86] While the plaintiff's claims may have been overstated in *In re Directives* (and, of course, it is impossible to know as long as broad sections of the opinion remain classified), it is clear that the plaintiff had no way of knowing how overstated the claims were because the plaintiff did not have access to the classified information gathered during the government's investigation.[87] It is exactly because of opacity concerns surrounding electronic surveillance that the FISA Court of Review decided to release its opinion (albeit in redacted form), which would typically remain classified.[88]

Beyond the expansive authority the FAA grants surveillance agencies and the secret exercise of that authority by intelligence agencies, critics contend that FAA surveillance also lacks sufficient oversight by non-executive

---

[82] *See, e.g.*, 50 U.S.C. § 1881a(g); *id.* § 1881b(d); *id.* § 1881c(d). As far as the author can tell, no information on surveillance specifically authorized under these provisions has been declassified.

[83] *See*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245, 260 (2008).

[84] *In re* Directives Pursuant to Section 105B of Foreign Intelligence Surveillance Act, 551 F.3d 1004, 1015 (FISA Ct. Rev. 2008).

[85] *Id.*

[86] *See*, Del Quintin Wilber & R. Jeffrey Smith, *Intelligence Court Releases Ruling in Favor of Warrantless Wiretapping*, WASH. POST (Jan. 16, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2009/01/15/AR2009011502311.html?hpid=topnews.

[87] *In re* Directives, 551 F.3d at 1007, 1015.

[88] *See id.* at 1016–17. Following the leaks by Edward Snowden, the FISC has further declassified several of its opinions. *See, e.g.*, *In Re* Orders of This Court Interpreting Section 215 of the PATRIOT Act, No. Misc. 13-02 (FISA Ct. Sept. 13, 2013), https://www.aclu.org/sites/default/files/assets/fisc_opinion_on_sect_215_public_access_motion.pdf. The PCLOB has recently called on the Obama Administration to prepare for the broad declassification of FISC opinions. *See* PCLOB Report, *supra* note 19, at 200 (arguing for broader declassification).

branch personnel.[89] Neither Congress nor the FISC wields sufficient authority under the FAA to determine whether abuses of power have occurred.[90] Within the Judicial Branch, FISA courts are aware of surveillance that takes place and authorize warrants certifying such surveillance, but in Section 1881a cases they do not evaluate warrants against persons or places on an individual basis.[91] Additionally, even in Section 1881b and Section 1881c cases, the FISC offers little meaningful oversight. It is often pointed out that the FISC must manage a high volume of FISA warrants and essentially all FISA warrant requests are granted (although it is often facetiously stated that this has no significance because without evidence to the contrary, we should assume that spies are simply very conservative in making warrant requests).[92] According to the U.S. District Court for the Eastern District of Virginia (arguably the most important national security court in the country at the trial level due to the location of the Pentagon and Langley) the bar for granting a FISA warrant is incredibly low—if the government reasonably suspects that "the target of the electronic surveillance or physical search is a foreign power or an agent of a foreign power," a FISA warrant essentially *must* be granted.[93] Congress similarly wields an insufficient check over agency activity and receives only periodic briefings on the details of surveillance.[94] This problem is further compounded when Congress, concerned with the integrity of the NSA program, fails to probe deeply into NSA activity under the FAA.[95]

---

[89] *See infra* Part III.2.

[90] I do not mean to state that there is no oversight of FAA operations. The NSA and other targeting agencies do have in place several minimization procedures to help ensure that Fourth Amendment privacy rights remain unviolated. For example, the FISC, the Office of Legal Counsel and the Department of Justice exercise periodic review of FAA procedure. *See* Jack Goldsmith, *The Cyberthreat, Government Network Operations, and the Fourth Amendment*, at 14 (The Brookings Inst., The Future of the Constitution Ser. No. 3, 2010), http://www.brookings.edu/~/media/research/files/papers/2010/12/08%204th%20amendment%20goldsmith/1208_4th_amendment_goldsmith.

[91] *See* 50 U.S.C. § 1881a(I)(3)(A); *see also* DYCUS ET AL., *supra* note 7, at 620 ("After a FISC judge approves the program features, the Attorney General and DNI authorize the surveillance program—without the need to obtain judicial orders for individual targets . . . .").

[92] *See* U.S. DOJ, ANNUAL FISA REPORTS, http://www.fas.org/irp/agency/doj/fisa/#rept. To take 2010 as a case study, in that year the government made 1,579 FISA applications, the government withdrew five applications, and the FISC modified 14 applications. *See also* Letter from Ronald Weich, Assistant Att'y Gen., to Senator Harry Reid (Apr. 29, 2011), http://www.fas.org/irp/agency/doj/fisa/2010rept.pdf.

[93] *See* United States v. Rosen, 447 F. Supp. 2d 538, 543 (E.D. Va. 2006) (holding that probable cause existed to authorize wiretapping of AIPAC lobbyists even though lobbying is a First-Amendment-protected activity).

[94] The FAA merely requires that the President keep Congress periodically informed. *See* 50 U.S.C. § 1881(f).

[95] *See* Rep. Alan Grayson, *Congressional Oversight of the NSA is a Joke, I Should Know, I'm in Congress*, THE GUARDIAN (Oct. 25, 2013), http://www.theguardian.com/commentisfree/2013/oct/25/nsa-no-congress-oversight.

III. Recommendations for Congress: A Proposed Amendment to the Foreign Intelligence Surveillance Act Amendments Act

If the above analysis is correct, then Congress should reassess intelligence surveillance and amend FISA. Fortunately, as Congress and the Obama Administration consider an overhaul of intelligence surveillance laws, a moment for such change presents itself.[96] In addressing concerns over the FAA, Congress should take two steps. First, Congress should narrow the scope of surveillance discretion granted to intelligence agencies. Second, Congress should strengthen the ability of courts, Congress, and the American public to check abuses in surveillance authority exercised by the executive branch. Drawing on the recent report issued by the President's Review Group on Intelligence and Communications Technologies,[97] this article proposes legislative language to do just that. Additionally, this article proposes that Congress codify some of the President's promises that offer to expand civil liberties protections, particularly the newly announced minimization procedures and the promise not to use the NSA to target domestic racial minorities or political dissidents.[98]

A. The First Step: Congress Should Narrow the Types of Conduct that Warrant Surveillance under the FAA

The first step Congress should take in reforming the FAA is to narrow and clarify what would give an intelligence agency authority to initiate electronic surveillance. Many have argued that one of the reasons the FAA has attracted so much negative attention is simply that the general public does not understand what type of behavior the act implicates.[99] This is not due to apathy, but rather to vagueness and secrecy because so much of the information surrounding FISA is classified.

Currently, the language of 50 U.S.C. § 1801 suggests that the FAA is construed incredibly broadly by intelligence agencies—an agency need only reasonably suspect that a target has committed or could commit *any* act "that would be a criminal violation if committed within the jurisdiction of the United States or any State" as long as a target was reasonably suspected of being an agent of a foreign power.[100] As the Snowden leaks demonstrate,

---

[96] *See, e.g.*, Savage, *supra* note 19; Kris, *supra* note 14; Ackerman, *supra* note 20.

[97] President's Review Grp., *supra* note 13.

[98] The White House, *Presidential Policy Directive 28: Signals Intelligence Activities, Section 1(b)* (Jan. 17, 2014), https://fas.org/irp/offdocs/ppd/ppd-28.pdf.

[99] *See* Posner, *supra* note 83, at 260 (stating that it is a good thing that FISA warrants are never denied, and that for the American people: "[t]he correct inference is that the Justice Department is too conservative in seeking warrants. The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport [8 hours early]."); *cf. In re* Directives, 551 F.3d at 1014 (addressing concerns regarding the secrecy of surveillance warrants).

[100] Interpreting 50 U.S.C. § 1801(b)(1)(C) in conjunction with § 1801(c)(1), both of which the FAA incorporates at 50 U.S.C. § 1861(a). This criticism of the act is well established. *See,*

this provision has in fact been used to conduct broad-ranging surveillance.[101] Moreover, the act gives no guidance as to what constitutes "reasonable suspicion" by an intelligence agency.[102] The most sweeping provision, Section 1881a, goes further by failing even to include such a requirement, requiring only that an intelligence agency not "intentionally target a U.S. person" in order to conduct surveillance activities.[103] By implication, such a person may be subject to surveillance if her data is knowingly, recklessly, or negligently collected.[104] As the American people discovered by the disclosures of Edward Snowden, this is exactly how the NSA and the FISA Court have interpreted this language.[105]

Congress should remedy the over-collection of data and clarify what behavior warrants surveillance by narrowing these provisions. In order to limit this expansive agency discretion, Congress could amend the FAA's most sweeping provision, Section 1881a, to require that intelligence agencies "reasonably suspect the surveillance targets of being agents of a foreign power" as defined in 50 U.S.C. § 1801. This requirement, as explained above, was incorporated by definition into the FAA in Sections 1881b and 1881c,[106] but not 1881a, and could be added after Section 1881a(g)(2)(A)(v), adopting the language "targets are reasonably believed to be a foreign power, an agent of a foreign power, or an officer or employee of a foreign power."[107] Furthermore, if Congress were to require that intelligence agencies swear to and demonstrate such reasonable suspicion when they apply for a FISC warrant, then much of the criticism of the Act's legal overbreadth would be alleviated, as 1881a could then only be used to target legally suspected terrorists.

Additionally, Congress should narrow the type of activity that constitutes reasonable suspicion by an intelligence agency that a U.S. person is an "agent of a foreign power" in Sections 1881b and 1881c, which it could

---

e.g., Steve Vladeck, *Why Clapper Matters: The Future of Programmatic Surveillance*, LAWFARE (May 22, 2012, 10:13 AM), http://www.lawfareblog.com/2012/05/clapper-and-the-future-of-surveillance/ ("'FISA warrants' are still predicated upon individualized suspicion, but suspicion to believe that the target is an agent of a foreign power, not that s/he is actively engaged in specific criminal activity."); Memorandum from the Cong. Research Serv. Am. Law Div., to Senate Select Comm. on Intelligence (Jan. 30, 2006), http://www.fas.org/sgp/crs/intel/m013006.pdf ("[FISA orders are based] upon the probability of a possibility; the probability to believe that the foreign target of the order may engage in spying, or the probability to believe that the American target of the order may engage in criminal spying activities.") (emphasis in original).

[101] For a summary of the early factual developments in the leak, *see* Klayman v. Obama, No. 13-0851, 2013 WL 6598728, at *2–4 (D.D.C. Dec. 16, 2013); Gidda, *supra* note 2; Lichtblau, *supra* note 2.

[102] *See* 50 U.S.C. § 1881(a).

[103] 50 U.S.C. § 1881a.

[104] *Id.* In the context of the FAA, this is often referred to as "dragnet surveillance." *See* Editorial, *Surveillance and Accountability*, N.Y. TIMES (Oct. 28, 2012), http://www.nytimes.com/2012/10/29/opinion/surveillance-and-accountability.html.

[105] *See* Gidda, *supra* note 102; Risen & Lichtblau, *supra* note 3.

[106] 50 U.S.C. §§ 1881b(b)(1)(C)(ii), 1881c(b)(3)(B).

[107] *Cf.* 50 U.S.C. §§ 1881b(b)(1)(C)(ii), 1881c(b)(3)(B).

accomplish by narrowing the definition of "international terrorism."[108] One version of this proposal has already been put forth by Seventh Circuit Judge Richard Posner.[109] In Judge Posner's proposal, the FAA would add an additional targeting requirement such that intelligence agencies would need to reasonably suspect that targets are threats to national security. Specifically, he would define "threat to national security" to implicate only "threats involving a potential for mass deaths or catastrophic damage to property or to the economy," and leave to traditional law enforcement the surveillance of acts that include "ecoterrorism, animal-rights terrorism, and other political violence that, though criminal, does not threaten catastrophic harm."[110]

Although Posner's proposal succeeds in narrowing intelligence agency discretion in interpreting the term "reasonably suspicious," his analysis fundamentally misreads the FAA since such behavior is already excluded.[111] However, Posner does validly argue that NSA surveillance techniques should not be used to target nonviolent political dissidents—a position that President Obama has publicly endorsed in his recent Presidential Policy Directive.[112] Congress could accomplish Posner's more thoughtful emendations and codify President Obama's recent directive if, instead of modifying the language of Sections 1881a, 1881b, and 1881c as Posner suggests, Congress altered the definition of terrorist activity itself. The new text would change the definition of terrorism from any act "that would be a criminal violation if committed within the jurisdiction of the United States or any State" to any act "that *threatens national security* and would be a criminal violation if committed within the jurisdiction of the United States or and State."[113] Of course, as is often the case in law governing executive power, particularly in national security, any particular tightening of legal language must be accompanied by oversight and enforcement to ensure that surveillance is only truly directed at national security threats.[114]

Third, Congress should modify Section 1881a so that it explicitly states that any collateral data on U.S. persons collected by intelligence agencies cannot be used for intelligence purposes without specific FISC authorization.[115] Here, Congress could insert a new requirement below Section

---

[108] 50 U.S.C. § 1801(b) (incorporated by reference in the FAA under 50 U.S.C. § 1861(a)).

[109] Posner, *supra* note 83, at 258.

[110] Posner, *supra* note 83, at 258.

[111] Recall that under FAA Sections 1881b and 1881c an agency must reasonably suspect that a target is the agent of a foreign power. *See supra* Part II. For this reason, the sorts of ecoterrorism and animal-rights terrorism Judge Posner envisions are actually already excluded from at least wiretaps under that part of the statute. *See* Posner, *supra* note 83, at 258.

[112] Presidential Policy Directive 28*, supra* note 98.

[113] *Cf.* 50 U.S.C. § 1801(b)(1)(C) and *id.* § 1801(c)(1), both of which the FAA incorporates at 50 U.S.C. § 1861(a).

[114] *See generally infra* Part IV.

[115] *See supra* Part II.B.3, canvassing the criticisms of Section 1881a. Current internal procedures (periodically reviewed by the FISC) prohibit such use as long as the data does not contain intelligence information or evidence of a crime. *Minimization Procedures Used By the National Security Agency in Connection With Acquisitions of Foreign Intelligence Information Pursuant to Section 702 of the Foreign Intelligence Surveillance Act of 1978, as Amended*,

1881a(d)(1)(B) of the act, stating that any incidental data pertaining to U.S. persons and collected by intelligence agencies cannot be used without first obtaining a FISC warrant under Section 1881b or 1881c of the act or through normal Title III electronic surveillance procedures for criminal investigations. This proposal would remedy much of the criticism generated by the programs and methods recently reported by *The Guardian*.[116] While Congress need not adopt such a proposal wholesale, clarifying and narrowing the types of activity that give rise to FAA surveillance would help strengthen the rule-of-law principles our system of governance embodies.

B. The Second Step: Increase Oversight by Independent Parties

The second step Congress should take to improve the FAA is to heighten the independent oversight of surveillance activity under the act. To do so, Congress could establish a publicly accountable, independent watchdog agency to supervise the operation of the FAA and ensure that the law be used only for its intended purpose. Alternatively, Congress could strengthen the existing Privacy and Civil Liberties Oversight Board to achieve the same goal. Critically, Congress would have to ensure that the executive branch could not simply classify away the information that the watchdog agency would need to conduct its supervision.[117] Congress could accomplish this either by ensuring that agency members have high-level security clearances or by mandating specific, non-redacted disclosure by adding a disclosure provision to the text of the FAA as recommended by the Presidential Review Group on Intelligence and Communication Technologies.[118]

Many critics of the act have already suggested a watchdog agency. For example, Jack Balkin has argued that new legislative and judicial oversight based on "prior disclosure and explanation and subsequent regular reporting

---

NSA, Section 3(b)(4) (Oct. 31, 2011), http://www.dni.gov/files/documents/Minimization%20Procedures%20used%20by%20NSA%20in%20Connection%20with%20FISA%20SECT%20702.pdf. The release of these minimization procedures was part of the general executive branch response to the leaks by Edward Snowden and was no doubt strongly resisted within the NSA. *See* James Clapper, *Cover Letter Accompanying Classified Document Release*, http://www.dni.gov/files/documents/DNI%20Clapper%20Section%20702%20Declassification%20Cover%20Letter.pdf (last visited Apr. 6, 2014).

[116] *See* Ackerman, *supra* note 20.

[117] National security personnel have historically over-classified intelligence surveillance information in order to deny Congress and government watchdogs access to wiretapping operations. For example, when the DOJ Office of Professional Responsibility tried to investigate the initial warrantless wiretapping by President Bush, Alberto Gonzales denied the DOJ attorneys investigating the program the security clearances necessary to conduct the investigation. *See* Kathleen Clark, *The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program*, 2010 BYU L. REV. 357, 402 (2010). This same phenomenon occurred again recently when a high-ranking official stated that by opening specific instances of FAA wiretapping to review by the Inspector General, this "would itself violate the privacy of U.S. persons." Letter from I. Charles McCullough, Inspector Gen. of the Intelligence Cmty., to Senators Ron Wyden & Mark Udall, (June 15, 2012), http://www.wired.com/images_blogs/dangerroom/2012/06/IC-IG-Letter.pdf.

[118] PRESIDENT'S REVIEW GRP., *supra* note 13, at 128–29.

and minimization"[119] should be coupled with the creation of a new, independent agency charged with oversight.[120] Balkin describes such an agency as "a cadre of informational ombudsmen within the executive branch—with the highest security clearances—whose job is to ensure that the government deploys information collection techniques legally and nonarbitrarily."[121] This would heighten independent oversight and ensure congruence between the spirit and letter of the FAA and the FAA's application. Congress designed the Privacy and Civil Liberties Oversight Board (PCLOB) to perform just such a function following public outcry surrounding the passage of the PATRIOT Act, and later granted it independent status; however, as of today the PCLOB still has little teeth (for reasons including its historical lack of funding).[122] In fact, the PCLOB itself recently suggested that it requires more access to information to adequately perform its job.[123] Even before the Snowden disclosures, several critics of FISA had already suggested the PCLOB be strengthened so that it could effectively monitor intelligence surveillance activities.[124]

Moreover, this alteration in oversight should be coupled with an expansion of the actual review process before the FISC, which should have the benefit of robust adversarial proceedings. As the Presidential Review Group proposed, either Congress, the FISC, or the PCLOB should be obligated to appoint an attorney to contest some of the more contentious FISA warrants including those authorized under Section 1881a.[125]

IV. A Brief Response to the Opponents of Surveillance Reform in Favor of Presidential Discretion

While congressional leaders largely agreed that the FAA would need significant future revision and therefore enacted the statute with a narrow sunset provision,[126] within legal academia some skeptics, informed largely by a public choice theory approach to national security, have argued that the

---

[119] Balkin, *supra* note 22, at 22.

[120] *Id.* at 24.

[121] *Id.* Judge Posner argues that the NSA should be required to submit the names of every person being surveilled and a brief description of why they are being surveilled to a national intelligence steering committee and an independent watchdog agency modeled on the U.S. Government Accountability Office. *See* Posner, *supra* note 83, at 257 (such a committee would be composed of "the attorney general, the director of national intelligence, the secretary of homeland security, and a retired federal judge or justice appointed by the chief justice of the Supreme Court").

[122] *See, e.g.*, Garrett Hatch, Cong. Research Serv., RL34385, Privacy and Civil Liberties Oversight Board: New Independent Agency Status (2012); President's Review Grp., *supra* note 13, at 196–200.

[123] *See* PCLOB Report, *supra* note 19, at 20.

[124] *See* Letter from Sen. Joe Lieberman, Sen. Susan Collins, & Sen. Daniel Akaka, to President Barack Obama (Apr. 8, 2011), http://homeland.cq.com/hs/flatfiles/temporaryItems/20110412privacy-letter.pdf; *see also* President's Review Grp., *supra* note 13, at 35.

[125] *See* President's Review Grp., *supra* note 13, at 203–05.

[126] *See* Emily Berman, *The Paradox of Counter Terrorism Sunset Provisions*, 81 Fordham L. Rev. 1777, 1779–80 (2013).

expansion of executive surveillance power generally and the FAA in particular needs no significant check because intelligence agencies' power to conduct surveillance is constrained by agencies' internal guidelines, executive branch politics, and electoral forces.[127] In this section, I address these potential constraints and demonstrate why, as a matter of political theory, they are unsatisfying as a check on intelligence agencies' behavior. Instead of relying on public choice theory and politics to constrain the implementation of the FAA, Congress should adopt this article's legislative proposals.

A. A Summary of the Political Constraints on Intelligence Surveillance

Public choice theorists argue that restricting executive power is unnecessary because intelligence agency personnel are sometimes unwilling to conduct overly broad surveillance, even when directly instructed to do so.[128] Beyond the ordinary public choice theory literature, whose theoretical foundation lies largely in marginalist economics,[129] national security public choice theorists also draw on a fairly robust legal literature from administrative law, which holds that the President's power to fire subordinates ("the removal power") is fairly limited, and therefore bureaucrats have the ability to defy the President's will and act as they see best in a given policy area.[130] While the President may have some power to fire the heads of many executive branch agencies,[131] the Supreme Court has long held that he cannot directly control the day-to-day activities of executive-branch employees.[132] Accordingly, if the critique of rule-of-law skeptics is right, and the President necessarily needs power to act outside the constraint of law, presidential subordinates can still effectively limit any potential abuse of that authority by refusing to conduct surveillance on targets even if the FAA's broad language allows such surveillance.[133]

Perhaps the best historical support for this proposition comes from the experiences of Assistant Attorney General James Comey. During the Bush-era scandal over warrantless wiretapping, James Comey, then-Acting Attorney General, and Robert Mueller, then-Director of the FBI, refused to authorize the continuation of the President's wiretapping program after the

---

[127] *See* ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 113 (2011).

[128] *See* James B. Comey, *Intelligence Under the Law*, 10 GREEN BAG 2D 439 (2007).

[129] *See generally* Daniel Shaviro, *Beyond Public Choice and Public Interest: A Study of the Legislative Process as Illustrated by Tax Legislation in the 1980s*, 139 U. PA. L. REV. 1 (1990).

[130] *See, e.g.*, Steven G. Calabresi & Kevin H. Rhodes, *The Structural Constitution: Unitary Executive, Plural Judiciary*, 105 HARV. L. REV. 1153, 1166–67 n.57 (1992); Lawrence Lessig & Cass R. Sunstein, *The President and the Administration*, 94 COLUM. L. REV. 1, 23–24 (1994); A. Michael Froomkin, *The Imperial Presidency's New Vestments*, 88 NW. U. L. REV. 1346, 1348 (1994).

[131] *See* Myers v. United States, 272 U.S. 52, 136, 176 (1926).

[132] *See* Kendall v. United States, 37 U.S. 524, 612–13 (1838) (stating that the postmaster is beyond presidential control when he performs a "purely ministerial" task).

[133] *See* 50 U.S.C. § 1881a(i).

Department of Justice refused to reauthorize it.[134] Moreover, Mueller and Comey maintained this position despite powerful people like Vice President Dick Cheney and then-OLC Director Alberto Gonzales insisting that "thousands" of people would die if Mueller and Comey did not conduct the warrantless surveillance.[135] This confrontation culminated in a race to the hospital bed of John Ashcroft to try to prevent/coerce Ashcroft from/into reauthorizing the President's wiretapping program.[136] This example suggests that in instances where subordinates feel concretely empowered to do the right thing, insubordination can effectively check an intelligence overreach.

Public choice theorists also contend that the President's ability to unilaterally conduct surveillance on broad swaths of the American public is constrained by electoral responses to presidential overreach. While elections are certainly complex phenomena, and people vote for bundles of goods for not-entirely-rational reasons,[137] the American people and Congress have consistently punished the President for overreaching in his use of discretionary authority. For example, when the Court struck down New Deal legislation, President Franklin D. Roosevelt responded by submitting a Court-packing plan to Congress.[138] Even though responding to Supreme Court rulings by trying to change the composition of the Court was not illegal per se, Congress refused to ratify Roosevelt's plan because it appeared to violate the nationally-held sentiment that separation of powers principles are important.[139] The Watergate scandal provides another, more modern example. During the Watergate scandal, President Nixon's actions appalled the American people, who soundly rejected the by-then-incumbent President Gerald Ford during the next election.[140] Public choice theorists, according to this narrative, would argue that in both of these cases, popular opinion helped moderate or punish presidents who overextended their executive authority.[141]

In the national security context, President George W. Bush's invasion of Iraq, wiretapping and waterboarding programs can be viewed in the same light. Even though Bush still won re-election in 2004, he lost the enormous popular support he enjoyed in 2001–02, in part because the American people

---

[134] *See* PSP REPORT, *supra* note 34, at 27–29.

[135] *See id.* at 23.

[136] Dan Eggen and Paul Kane, *Gonzales Hospital Episode Detailed*, WASH. POST (May 16, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/15/AR2007051500864.html.

[137] *See* Shaviro, *supra* note 129, at 76–78.

[138] *See* NOAH FELDMAN, SCORPIONS: THE BATTLES AND TRIUMPHS OF FDR'S GREAT SUPREME COURT JUSTICES 103 (2010).

[139] *Id.* at 108.

[140] For a discussion of the loss of public faith in the executive branch caused by Watergate, *see* S. Select Comm. to Study Governmental Operations, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities of the United States Senate, S. Rep. No. 94-755, 16 (1976) [hereinafter Church Committee Report].

[141] *Cf.* POSNER & VERMEULE, *supra* note 127, at 48, 69 (describing the effect Watergate had on Nixon's presidential power vis-à-vis other branches of government).

viewed some of President Bush's policies as illegal.[142] Moreover, Obama won a sweeping victory in 2008, in part by promising a radical departure from Bush's national security policies.[143]

B. A Defense of a Legislative Solution

While it may be true that elections and insubordination (among other mechanisms) can constrain the President's power to authorize broad surveillance of American communications, neither of these answers will satisfy critics or prevent the abuses disclosed by Edward Snowden. First, insubordination is unreliable. As famously illustrated by Yale psychology professor Stanley Milgram (before the ethics of human psychological testing was seriously questioned), human beings follow orders even if asked to do incredibly immoral things. In Milgram's experiments, he demonstrated that a majority of people will shock innocent participants to death if given an order to do so.[144] This phenomenon is not limited to the halls of the Yale Psychology Department. In the context of U.S. national security law, during the Iran-Contra Affair, Lieutenant Colonel Oliver North abnegated responsibility for violating Congress' explicit refusal to authorize arms sales to the Nicaraguan Contras, declaring that he was just "following orders."[145] Lieutenant North's behavior is unsurprising; in cases of national security, it might actually be *more* likely that presidential subordinates will err in favor of following orders, since decisions by the President and government agencies presumptively directly affect the safety and wellbeing of American citizens. If we analogize to intelligence surveillance, it is entirely likely that intelligence agencies will defer to their superiors and conduct surveillance even if they themselves think that it is unlawful.

Electoral constraints, while perhaps more reliable than insubordination, are similarly unsatisfying, in part because even broad consensus on the need for reform has so far failed to materialize into a concrete FAA amendment.[146] Even when the American public does respond strongly to perceived presidential overreach, as in the case of Watergate and the 2006 and 2010 elections (against Bush's counter-terrorism strategy and Obama's healthcare

---

[142] *See generally* GOLDSMITH *supra* note 8, at 16 (arguing that Obama won in part by running against Bush's national security record before largely adopting Bush's approach to national security issues).

[143] *Id.*; *see also* Charlie Savage, *Closing Guantanamo Fades as a Priority*, N.Y. TIMES (June 26, 2010), http://www.nytimes.com/2010/06/26/us/politics/26gitmo.html?_r=0 (describing Obama's campaign promise to close Guantanamo Bay).

[144] *See* Stanley Milgram, *Behavioral Study of Obedience*, 67 J. ABNORMAL PSYCH. 371 (1963). This phenomenon, in explaining the behavior of German Nazis during World War II, has been labeled "the 'Nuremburg' Defense." *See, e.g.*, United States v. North, 910 F.2d 843, 881 (D.C. Cir. 1990); Jay v. United States, 865 F.2d 1175, 1177 (10th Cir. 1989).

[145] *See* North, 910 F.2d at 881. Similarly, during the Watergate scandal, for example, President Nixon's staff and CIA Agents engaged in a cover-up at the direction of the President. *See* Church Committee Report, *supra* note 140, at 28, 607–08.

[146] *See* Berman, *supra* note 126, at 1777 (describing the failure of Congress to reconsider and amend statutes that were perceived at the time of enactment to be short-term patches).

plan, respectively), electoral control exerts itself only post-overreach, and sometimes only distantly so.[147] Additionally, unless the overreach is particularly egregious, the people and Congress may not react at all.[148] This problem is compounded by the fact that intelligence surveillance takes place in secret, and the behavior of intelligence agencies is often classified. The American people cannot vote to reject something that they do not know is happening.

In short, if intelligence agencies or the President try to conduct broad, warrantless surveillance under the FAA, both insubordination and electoral outrage are unlikely to effectively constrain their behavior. This is because insubordination is unreliable and the surveillance process is too secretive to provoke a reaction from the American public. Given these problems with constraints, America would be better served by relying on legal mechanisms for reducing possible executive branch overreach. Most importantly, the amendments to the FAA that this article proposes will effectively restrict intelligence agencies in a way that electoral politics and insubordination do not.

V. Conclusion

Intelligence surveillance, as governed by the Foreign Intelligence Surveillance Amendments Act, is in need of reform. Congress passed the original Foreign Intelligence Surveillance Act in order to help American intelligence agencies conduct surveillance in a pre-internet, pre-cellphone era, wanting to give the executive branch broad power to spy on non-U.S. citizens abroad, while protecting to the fullest extent possible the privacy of U.S. persons within the United States. In the years following September 11, 2001, Congress enacted the Foreign Intelligence Surveillance Amendments Act in order to grant executive branch agencies broader surveillance power than the agencies had under the original FISA. First, the FAA established a uniform process for seeking judicial authorization of electronic surveillance. Second, the FAA created a broad category of intelligence surveillance that would not be subject to ex-ante judicial scrutiny and would only be granted limited ex-post judicial review. The near-consensus on the issue is that the FAA overly delegates broad surveillance authority to intelligence agencies and minimizes the level of judicial and congressional oversight exercised over these agencies. Moreover, outside the executive branch, there is no substantial political coalition opposing FISA reform efforts. Instead, the current system is largely a product of congressional gridlock and inertia. Despite such inaction, these problems cannot be ignored. Congress should

---

[147] *See generally* Shaviro, *supra* note 129.

[148] For a classic and particularly dismal take on Congress' ability to solve problems, *see* Morris Fiorina, Congress—Keystone of the Washington Establishment 71–81 (1977). For more on the general difficulty voters have policing Congress, *see generally* Ilya Somin, Democracy and Political Ignorance (2013).

amend the FAA to reduce the scope of surveillance authority granted to intelligence agencies. Congress should do this by more precisely defining the conduct that would warrant intelligence surveillance targeting. Additionally, Congress should expand the oversight of intelligence surveillance by both Congress and the courts to ensure that the government does not exceed the authority granted under the FAA.