UIC Law Review

Volume 47 | Issue 4 Article 15

Summer 2014

Balancing Security and Privacy in 21st Century America: A Framework for FISA Court Reform, 47 J. Marshall L. Rev. 1453 (2014)

Daniel Cetina

BALANCING SECURITY AND PRIVACY IN 21ST CENTURY AMERICA: A FRAMEWORK FOR FISA COURT REFORM

DANIEL K. CETINA*

I. INTRODUCTION

A. Snowden's Sudden Scandal

"I think it is important to recognize that you can't have 100% security and then also have 100% privacy and zero inconvenience . . . . [w]e are going to have to make some choices as a society."[1]

So said President Barack Obama in the wake of former intelligence contractor Edward Snowden's disquieting disclosure of clandestine governmental surveillance of American citizens.[2]

*The author would like to thank his family, his staff editors, and the Law Review Editorial Board for their help and support throughout the writing process.

[1] Michael Pearson, *Obama: No One Listening To Your Calls*, CNN (June 9, 2013), *available at* http://www.cnn.com/2013/06/07/politics/nsa-data-mining/index.html (quoting President Barack Obama).

[2] *See* James Ball, *Edward Snowden NSA Files: Secret Surveillance and Our Revelations So Far*, THE GUARDIAN (Aug. 21, 2013), *available at* http://www.theguardian.com/world/2013/aug/21/edward-snowden-nsa-files-revelations (summarizing Edward Snowden's revelations eleven weeks after his initial bombshell disclosures; specifically, that the U.S. government continued previously-disclosed warrantless wiretapping and that it operated secret surveillance programs designed to compile and scrutinize telephone and email records in concert with some of the world's most powerful technology

Snowden publicized that surveillance, which is conducted largely through the National Security Agency (NSA),[3] one of the United States' internal intelligence organizations, thereby reigniting debate regarding the legality and desirability of the federal government's data-gathering programs.[4]

This Comment discusses myriad issues regarding governmental surveillance.[5] Part II provides background information germane to surveillance. Part II.A defines surveillance and summarizes the breadth and extent of existing surveillance practices. Part II.B provides an overview of relevant federal legislation granting the executive branch enhanced law enforcement and surveillance powers. And Part II.C discusses cases involving challenges to federal surveillance powers.

Part III presents this Comment's principal arguments. Part III.A argues that, while certain surveillance measures are necessary, particularly during wartime, the extent of current surveillance is overly broad and the existing putative oversight measures are ineffectual. Part III.B lists and describes various remedial proposals and their limitations.

Part IV provides a two-pronged proposal. Parts IV.A and IV.B describe that proposal, which incorporates both structural and interpretive components, including strengthening concrete oversight measures and introducing a judicial test that weighs

---

companies, including Google, Apple, Microsoft, and Yahoo).

[3] *See* JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 1-4, 94-96 (2008) (describing how the 9/11 terrorist attacks precipitated a massive recalibration of NSA procedures and resources, historically directed at foreign threats and established persons of interest, towards domestic surveillance as well).

[4] John Cassidy, *Snowden's Legacy: A Public Debate About Online Privacy*, THE NEW YORKER (Aug. 20, 2013), *available at* http://www.newyorker.com/online/blogs/johncassidy/2013/08/snowdens-legacy-public-debate-about-online-privacy.html.

[5] *See* National Research Council, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 44-47 (National Academy of Sciences 2008) (outlining detailed proposals for 21st century U.S. surveillance with the dual goals of mitigating governmental surveillance's debilitating effects on liberty interests and remedying various ambiguities and inefficiencies in existing programs); *see also* RICHARD A. POSNER, NOT A SUICIDE PACT: THE CONSTITUTION IN A TIME OF NATIONAL EMERGENCY 30-32 (2006) (arguing for flexibility with civil liberties during wartime); Richard A. Posner, *The Truth About Our Liberties*, *in* RIGHTS VS. PUBLIC SAFETY AFTER 9/11: AMERICA IN THE AGE OF TERRORISM 25-28 (Amitai Etzioni & Jason H. Marsh eds., 2003) (discussing the tension between civil liberties and state security and arguing that civil libertarians grossly exaggerate the threat to American values during wartime while deemphasizing legitimate national security concerns). *But see* David Cole, *Let's Fight Terrorism, Not the Constitution*, *in* RIGHTS VS. PUBLIC SAFETY AFTER 9/11: AMERICA IN THE AGE OF TERRORISM 35-42 (focusing specifically on the U.S. immigration system post-9/11, but otherwise arguing that modern surveillance/security measures, particularly the Patriot Act, are cumulatively enervating).

both security interests and privacy interests, respectively. Part IV.C addresses counterarguments to the two-pronged remedial model. Part V briefly concludes.

II. BACKGROUND

Modern surveillance controversies arose during the second Bush Administration with allegations of severe executive overreach and impropriety.[6] Recent disclosures of the Obama Administration's own dubious surveillance agenda only compounded these controversies.[7] Contemporarily, the value most at stake is the fundamental right to privacy.[8] However, it is difficult to persuasively argue that any measure of surveillance is impermissible or that existing policies do not advance compelling national interests.[9] The ultimate issue is determining the

---

[6] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), *available at* http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all; *see also* JAMES RISEN, STATE OF WAR: THE SECRET HISTORY OF THE CIA AND THE BUSH ADMINISTRATION 4-7, 10 (2006) (outlining various abuses of power former President George W. Bush perpetrated, while making a grander argument about disturbing bloated executive authority and its frequent unconstitutional overreach).

[7] Glenn Greenwald, *Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security*, THE GUARDIAN (Sept. 5, 2013), *available at* http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security.

[8] U.S. CONST. amend. XIV, § 1. It is worth noting that nowhere is privacy explicitly mentioned textually in the Constitution, yet courts have nevertheless identified an implied right to privacy through the broad concept of liberty embodied in the Due Process Clause of the Fourteenth Amendment. *See, e.g.*, Griswold v. Connecticut, 381 U.S. 479, 500-01 (1965) (Harlan, J., concurring) (determining that the right to privacy is located implicitly in the Due Process Clause of the Fourteenth Amendment, a position vindicated through subsequent application in such cases as *Eisenstadt v. Baird*, 405 U.S. 438 (1972) (involving the distribution of contraceptives to unmarried persons), and *Roe v. Wade*, 410 U.S. 113, 153 (1973) (upholding as constitutional a woman's right to choose to have an abortion)). Though *Griswold* and its progeny dealt primarily with reproductive/sexual privacy, those seminal cases clarified that many other Amendments contain inherent privacy implications. For example, the First, Third, Fourth, and Fifth Amendments each contain elements of decisional and/or spatial privacy, without which the explicitly codified rights in those same amendments would be weakened. *Griswold*, 381 U.S. at 484. *See generally* ALAN WESTIN, PRIVACY AND FREEDOM (1967) (arguing that the three policy values of dignity, autonomy, and intimacy together create the essential personhood of the individual and policies impinging on privacy, such as governmental surveillance, are damaging and only permissible in putative total institutions like jails and insane asylums). Interestingly, Westin – writing in the 1960's and therefore prior to the inception of the Internet – defines privacy as the "claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others." *Id.* at 7.

[9] Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934,

healthiest balance between security interests and privacy interests, both of which are crucial and necessary for civilized states.[10] Further, developing a cognizable framework to apply in discrete scenarios that considers both interests is critical.

Analyzing the current controversy first requires a basic understanding of the use of surveillance, the origins of governmental surveillance power, and the prior legal controversies regarding that power. Only after grasping these concepts can one posit a reasonable solution.

A. What is Surveillance?

Any legitimate attempt to discuss and critique United States surveillance tactics necessarily demands defining exactly what surveillance is and what it entails. Although discourse surrounding governments' intelligence and law enforcement techniques transcends any specific epoch or state,[11] modern communication technologies "have revolutionized our daily lives [and] have also created minutely detailed recordings of those lives,"[12] thereby making governmental surveillance simple, potentially ubiquitous, and susceptible to abuse.[13] Of course, recent surveillance programs were implemented for the noble purpose of conducting the War on Terrorism;[14] but the danger is that pursuing this purpose unchecked can undermine the central principles that both provide the Republic's foundation and differentiate it from the very enemies it combats.[15]

1936 (2013).

[10] Editorial Board, *FISA Needs to Balance Security and Liberty*, WASH. POST (Oct. 28, 2013), *available at* http://www.washingtonpost.com/opinions/fisa-needs-to-balance-security-and-liberty/2012/10/28/49cddec8-1fb6-11e2-afca-58c2f5789c5d_story.html.

[11] *See* ALFRED W. MCCOY, POLICING AMERICA'S EMPIRE: THE UNITED STATES, THE PHILIPPINES, AND THE RISE OF THE SURVEILLANCE STATE 16 (2009) (elucidating that the United States' surveillance practices predate contemporary global conflicts, with historical roots at least as early as the end of the 19th century when the United States intervened in the Philippines, among other locations, during the overarching Spanish-American War).

[12] Richards, *supra* note 9, at 1936.

[13] *Id.*

[14] *See* LAWRENCE WRIGHT, THE LOOMING TOWER: AL-QAEDA AND THE ROAD TO 9/11 165–67, 185, 198–99 (2007) (detailing the origins of the War on Terrorism, including an overview of relevant international players in both government and various terrorist networks, with an especial analysis of the War on Terrorism's historical underpinnings). Wright emphasizes the former Soviet Union's abortive war in Afghanistan during the 1980s, which directly contributed to the radicalization of a new generation of *mujahideen*, including a young Osama bin Laden, who would later initiate the formal War on Terrorism by orchestrating the 9/11 terrorist attacks against the United States. *Id.* at 165.

[15] *See generally* Girardeau A. Spann, *Terror and Race*, 45 WASHBURN L.J. 89, 89–90 (2005) (arguing that terrorists' fundamental goal is not to

While the prospect of governmental surveillance seems to implicitly suggest a quasi-Orwellian dystopia,[16] fantastical science fiction mythologies,[17] abstruse philosophical concepts,[18] or documented repressive regimes,[19] the reality is both less foreboding and more nuanced. Although American society, ostensibly, is looking increasingly akin to such fiction, theory, and totalitarianism, surveillance as applied is not so disturbing. Surveillance involves and encompasses many topics and practices, both abstract and practical,[20] but it primarily involves power relationships.[21] Specifically, surveillance is "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction."[22] Surveillance can target a modern society's numerous communications networks,[23] which exist to send and receive information.[24] The

---

unremittingly create wanton destruction, but rather to undermine Western democratic values and civil liberties precisely through unspeakable acts of terror, so perpetuating an expansive and repressive War on Terrorism actually endangers domestic liberties and ironically furthers terrorists' objectives, albeit indirectly); *see also* Rosa Ehrenreich Brooks, *War Everywhere: Rights, National Security Law, and the Law of Armed Conflict in the Age of Terror*, 153 U. PA. L. REV. 675, 679 (2004) (arguing that contemporary warfare is fundamentally different from heretofore binary warfare and conventional understandings--war and peace, state versus state – of worldwide conflict and that the erosion of international law threatens both global populations and liberal democratic values). *But see* WILLIAM REHNQUIST, ALL THE LAWS BUT ONE: CIVIL LIBERTIES IN WARTIME 222–23 (1998) (advocating that when civil liberties and security interests conflict, the former should not necessarily eclipse the latter).

[16] *See generally* GEORGE ORWELL, 1984 (1950) (depicting a dystopia in which the government, referred to as "Big Brother," is constantly monitoring its citizens and in which even certain private musings are considered "thoughtcrimes").

[17] *See* MINORITY REPORT (20th Century Fox 2002) (chronicling a futuristic world where a triumvirate of prescient humans known as "precogs" assist the PreCrime law enforcement division by foreseeing murders before they actually occur).

[18] *See generally* JEREMY BENTHAM, THE PANOPTICON WRITINGS (Miran Bozovic ed., Verso 1995) (conceptualizing a prison model that permits almost total control over prisoners through forced self-discipline); MICHEL FOUCAULT, DISCIPLINE AND PUNISH: THE BIRTH OF THE PRISON (A. Sheridan trans., 2nd ed., Vintage 1995) (applying, in part, Bentham's Panopticon principles to an expansive analysis of Western criminal justice and punitive penitentiary systems).

[19] *See generally* RICHARD OVERY, THE DICTATORS: HITLER'S GERMANY, STALIN'S RUSSIA (2006) (comparing and contrasting two of the most recognizably evil and tyrannical regimes in history, both of which engaged in surveillance – and worse).

[20] DAVID LYON, SURVEILLANCE STUDIES: AN OVERVIEW 13–16 (2007).

[21] *Id.* at 15.

[22] *Id.* at 14.

[23] Orin S. Kerr, *Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 610 (2003).

[24] *Id.* at 611.

communications include both envelope information and content information, distinct categories that draw varying degrees of interest from the surveillance authority.[25]

But surveillance is not strictly the province of the federal government.[26] Indeed, state and local governments have their own surveillance practices,[27] as do private corporations, which routinely use surveillance data to determine purchasing trends and calibrate advertising, especially through such social media sites as Facebook.[28] Surveillance, therefore, transcends the boundary between the private sector and the public sector.[29]

The focus here, however, is on federal governmental surveillance. It is therefore critical to understand from where the federal government derives its authority to monitor and analyze communications networks.

B. Legislative Delegations of Power: A Slippery Slope

There is no one supreme legislative grant augmenting federal surveillance powers.[30] Surveillance authority grew over time and through various, often unrelated bills. There is no effective point of origin from which to begin analyzing legislative conferrals of surveillance authority. But the Foreign Intelligence Surveillance Act of 1978 ("FISA")[31] is perhaps the logical starting point because it established the Foreign Intelligence Surveillance Court ("FISA Court"),[32] which is currently under scrutiny for its centrality in

---

[25] *Id.* at 611. Envelope information is information about information, such as names and addresses on mail envelopes or routing information coded in emails. In contrast, content information is the substantive information contained within the metaphorical or actual envelope: a real letter within an envelope or the communicative/expressive text of an email. *Id.* at 611-12. Interestingly, email surveillance is actually a subcategory of packet surveillance, or surveillance of unique communications packets applicable only to the websphere, which contain individual parts of emails disassembled during transit. *Id.* at 614-15. Depending on the importance of the privacy at stake, the government will allegedly have to satisfy threshold showings ranging along a certain continuum for surveillance to be authorized. *Id.* at 619-20.

[26] Richards, *supra* note 9, at 1938.

[27] Matthew Waxman, *Ohio's Lessons: State Governments and Facial Recognition*, NEW REPUBLIC (Oct. 2, 2013), *available at* http://www.newrepublic.com/article/114957/states-cities-facial-recognition-law-enforcement-and-privacy.

[28] Richards, *supra* note 9, at 1938–39 (referencing the commercial phenomenon known as behavioral advertising, and indicating that e-readers like the Kindle can determine reading habits based on book purchases).

[29] *Id.* at 1941.

[30] *Infra* notes 31-36, 39-40, 44-49 and accompanying text (describing several relevant surveillance statutes).

[31] 50 U.S.C. § 36 (1978).

[32] *Id.*

President Obama's overall surveillance scheme.[33] Congress amended FISA numerous times, most importantly in 2001,[34] 2007,[35] and 2008.[36] The FISA Court is presently the body empowered to curb federal surveillance power: it considers governmental requests for surveillance warrants.[37] But, arguably, this deliberation is strictly nominal and an unsatisfying check on potentially unlimited governmental power in the surveillance realm.[38]

The Electronic Communications Privacy Act of 1986 ("ECPA")[39] is the second bill meriting discussion. Although the ECPA practically limits governmental surveillance authority by applying the rules for wiretapping telephones[40] to electronic – e.g. Internet – communications,[41] it remains glaringly inefficient. The government routinely circumvents this law by arguing that information voluntarily submitted to third parties, such as cell phone carriers and Internet servers, is beyond the scope of ECPA protection,[42] a phenomenon characterized as the disclosure principle.[43]

---

[33] Evan Perez, *Secret Court's Oversight Gets Scrutiny*, WALL ST. J. (June 9, 2013), *available at* http://online.wsj.com/article/SB10001424127887324904004578535670310514616.html.

[34] Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified at 50 U.S.C. § 1861).

[35] *See* Protect America Act (PAA), Pub. L. No. 110–55, 121 Stat. 552 (2007) (codified at 50 U.S.C. § 1801) (amending FISA and replacing the warrant requirement for wiretapping foreign subjects with internal NSA protocols); Responsible Electronic Surveillance That is Overseen, Reviewed, and Effective Act (RESTORE Act), H.R. 3773, 110th Cong. (2007) (reestablishing the FISA Court's authority to issue warrants for particularized surveillance).

[36] FISA Amendments Act (FAA), H.R. 6304, 110th Cong. (2008) (enacted) (amending the original FISA with provisions similar to the expiring PAA, including § 702, which authorizes dilatant surveillance programs).

[37] Glenn Greenwald, *Fisa Court Oversight: A Look Inside a Secret and Empty Process*, THE GUARDIAN (June 18, 2013), *available at* http://www.theguardian.com/commentisfree/2013/jun/19/fisa-court-oversight-process-secrecy.

[38] *See* Alex Seitz-Wald, *Despite Obama's Claim, FISA Court Rarely Much of a Check*, SALON (June 7, 2013), http://www.salon.com/2013/06/07/despite_obamas_claim_fisa_court_rarely_much_of_a_check/ (indicating that the FISA Court frequently acts merely as a rubber stamp on executive surveillance requests--a persuasive claim considering the FISA Court did not deny any of the government's 1,789 surveillance applications in 2012 and modified only 30).

[39] 18 U.S.C. §§ 2510-2522 (1986).

[40] *See* Omnibus Crime Control and Safe Streets Act, 42 U.S.C. § 3711 (1968) (including provisions limiting governmental wiretapping privileges).

[41] Kerr, *supra* note 23, at 662.

[42] *See* United States v. Graham, 846 F. Supp. 2d 384, 389-90 (D. Md. 2012) (holding that there is no realistic expectation of privacy for cell site location records); Smith v. Maryland, 442 U.S. 735, 745-46 (1979) (holding that warrants are not required prior to installing pen registers because they are not searches meriting Fourth Amendment protection).

[43] Kerr, *supra* note 23, at 627-28.

The third important act is the USA PATRIOT Act ("Patriot Act"),[44] passed in the wake of the September 11, 2001 terrorist attacks in New York City and Washington, D.C. The Patriot Act amended FISA and authorizes such surreptitious programs as PRISM[45] and BLARNEY.[46] By amending existing laws,[47] the Patriot Act affects multiple areas of federal power.[48] Significant to the augmentation of federal surveillance authority is Title II, which amended FISA and provides for various additional surveillance provisions.[49]

This confluence of legislation, passed reflexively to contend with exterior threats like al Qaeda post-9/11, collectively underpins contemporary United States surveillance authority.[50] Courts do hear surveillance challenges, but have done little thus far to clarify what are often ambiguous laws and intractable legal imbroglios.[51]

C. Case History: Disturbing Deference

Interestingly – and most problematically – there is not a seminal line of cases involving governmental surveillance akin to, for example, First Amendment jurisprudence[52] or civil rights jurisprudence,[53] both of which developed in relatively linear

---

[44] Pub. L. No. 107–56, 115 Stat. 272 (2001) (codified at 50 U.S.C. § 1861).

[45] *See* Glenn Greenwald & Ewen MacAskill, *NSA Prism Program Taps In To User Data of Apple, Google and Others*, THE GUARDIAN (June 6, 2013), *available at* http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data?guni=Article:in%20body%20link (describing PRISM, a secretive program enabling the government to access Google search history, online messaging, and email contents).

[46] *See* Siobhan Gorman & Jennifer Valentino-DeVries, *New Details Show Broader NSA Surveillance Reach*, WALL ST. J. (Aug. 20, 2013), *available at* http://online.wsj.com/article/SB10001424127887324108204579022874091732470.html (describing BLARNEY, among other secret programs, which collects and filters metadata).

[47] Kerr, *supra* note 23, at 608.

[48] *Id.* at 624-26.

[49] Pub. L. No. 107–46, § 215, 115 Stat. 272, §§ 201–02 (2001) (amending FISA and augmenting governmental surveillance power by expanding the availability of wiretaps, for example).

[50] However, this collection is by no means complete. There are many other laws that directly or indirectly permit governmental surveillance. *See, e.g.,* Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. § 1001 (2012), but an exhaustive analysis of every relevant federal law is beyond the scope of this Comment.

[51] *Infra* notes 59–65 and accompanying text (providing examples of surveillance cases).

[52] *See* ANTHONY LEWIS, MAKE NO LAW: THE SULLIVAN CASE AND THE FIRST AMENDMENT 84–89, 189–95 (1992) (documenting and analyzing the history and development of First Amendment jurisprudence through much of the 20th century).

[53] *Id.* at 19–20 (suggesting that *Brown v. Board of Education*, 347 U.S. 483 (1954), the capstone civil rights case, ushered remarkable social changes

fashions.[54] The dearth of major surveillance cases may be due to the veritable schizophrenia of salient legislation, which developed sporadically over several decades.[55]

Close examination of certain cases involving federal surveillance yields no discernable formula, test, or framework to apply in future surveillance controversies. However, two common trends emerge in surveillance cases: relying[56] on the state secrets privilege[57] and, relatedly, dismissing for non-justiciability,[58] specifically lack of standing.[59]

The state secrets privilege frequently emerges in modern

---

independent of the judiciary); *see also* RICHARD KLUGER, SIMPLE JUSTICE: THE HISTORY OF *BROWN V. BOARD OF EDUCATION* AND BLACK AMERICA'S STRUGGLE FOR EQUALITY 531-42 (2004) (documenting and analyzing the history and development of the Civil Rights Movement, including landmark Supreme Court decisions that clarified and protected civil rights for African Americans, and more contemporary cases involving affirmative action).

[54] Free speech law especially. For instance, libel law began developing with the Court's decision in the seminal free speech case *N.Y. Times Co. v. Sullivan*, 376 U.S. 254 (1964), otherwise known as the Sullivan Case.

[55] *Supra* notes 39-44 (discussing principal surveillance legislation).

[56] *See, e.g.*, United States v. Reynolds, 345 U.S. 1, 7–8 (1953) (applying the state secrets privilege for the first time, thus representing formal judicial recognition of the doctrine); *see also* Sterling v. Tenet, 416 F.3d 338, 347–48 (2005) (dismissing CIA agent plaintiff's racial discrimination case on application of the state secrets privilege); Terkel v. AT&T Corp., 441 F. Supp. 2d 899, 909–10 (N.D. Ill. 2006) (holding that the state secrets privilege prevented discovery to determine whether AT&T had disclosed private telephone records to the NSA).

[57] *See generally* Amanda Frost, *The State Secrets Privilege and Separation of Powers*, 75 FORD. L. REV. 1931, 1935-37, 1941 (2007) (providing, in part, an examination of the history of the state secrets privilege with especial emphasis on its common law and constitutional origins, as well as its gradual evolution and expansion, particularly post-9/11, when judicial decisions favorable to the executive applied the state secrets privilege in multiple scenarios, alternatingly involving extraordinary rendition and surveillance programs); Robert M. Chesney, *State Secrets and the Limits of National Security Litigation*, 75 GEO. WASH. L. REV. 1250, 1270-80, 1314-15 (2007) (supplying an exhaustive history of the state secrets privilege and concluding that the privilege tilts too strongly in favor of protecting security).

[58] An issue that is improper for judicial examination. *See* BLACK'S LAW DICTIONARY 882 (8th ed. 2004); *see also* CONSTITUTIONAL LAW: STRUCTURE AND RIGHTS IN OUR FEDERAL SYSTEM 245, 254, 262 (William C. Banks & Rodney A. Smolla eds., 6th ed. 2010) (outlining the various justiciability concepts, including political question doctrine, standing, ripeness, and mootness).

[59] *See, e.g.*, Ne. Fla. Chapter of the Associated Gen. Contractors of Am. v. City of Jacksonville, Fla., 508 U.S. 656, 663–64 (1993) (declaring that a party seeking federal jurisdiction must assert appropriate standing, which involves demonstrating (1) an injury in fact, or otherwise one that is "concrete and particularized and actual or imminent, not conjectural or hypothetical"; (2) a causal relationship between the alleged injury and the challenged state action; and (3) that the injury is capable of redress, or otherwise the ability of the court to issue a favorable ruling).

surveillance cases like *Hepting v. AT&T*.[60] When the government is permitted to assert the state secrets privilege[61] in the context of surveillance cases, the privilege allows the government to withhold information regarding the very security apparatuses and surveillance tactics from which plaintiffs seek relief.[62] This withholding leaves plaintiffs with the paradoxical task of demonstrating injuries that are, due in large part to the state secrets privilege, incapable of being proven in court.[63]

This is where the justiciability problem arises.[64] Courts often determine that plaintiffs fail to assert cognizable injuries. For example, in *Laird v. Tatum*,[65] the Court reasoned that the plaintiff's fear of future harm stemming from governmental surveillance was too attenuated[66] and therefore inappropriate for judicial rectification.[67]

Various federal laws and certain cases collectively constitute the general tableau for contemporary surveillance. Indisputably,

---

[60] 439 F. Supp. 2d 974, 1011 (N.D. Cal. 2006) (denying, in a rare victory for plaintiffs, the government's motion to dismiss based on the state secrets privilege). *But see* Al-Haramain Islamic Found. v. Bush, 507 F.3d 1190, 1197 (9th Cir. 2007) (applying the state secrets privilege, thereby preventing the plaintiffs from determining whether they were actually the subjects of surveillance); El-Masri v. United States, 479 F.3d 296, 303 (2006) (applying the state secrets privilege in a controversy involving extraordinary rendition for a German citizen in CIA custody).

[61] See Chesney, *supra* note 57, at 1250, 1308 (arguing that, post-*Reynolds*, the state secrets privilege is pervasive in federal litigation, creates harsh results, and too often allows the government to dismiss and therefore thwart legitimate suits, which impairs democratic accountability and transparency).

[62] Richards, *supra* note 9, at 1943–44; *see also* Frost, *supra* note 57, at 1937 (indicating that the state secrets privilege operates in litigation in three distinct ways: (1) by functioning as a barrier to evidence submission, as in *Reynolds*; (2) by causing courts to grant summary judgment in favor of the defendant, if the state secrets privilege prevents information that might otherwise assist in forming a valid defense from entering; and (3) by resulting in automatic dismissal in favor of the defendant, if the essential nature of the action at bar is itself subject to the state secrets privilege, notwithstanding the plaintiff's capacity to introduce non-privileged evidence).

[63] Richards, *supra* note 9, at 1944; *see also Al-Haramain*, 507 F.3d at 1202 (applying the state secrets privilege).

[64] Manifestly, application of the state secrets privilege inevitably leads to issues of standing: when certain information is protected under the auspices of the privilege, especially information tending to support claimed injuries, it exponentially increases the difficulty of satisfying the distinct standing requirements. Richards, *supra* note 9, at 1944.

[65] 408 U.S. 1 (1972).

[66] *Laird*, 408 U.S. at 11-13; *see also* Clapper v. Amnesty Int'l, 133 S.Ct. 1138, 1148 (2013) (holding that respondents failed to satisfy the requisite standing elements and could not assert a challenge against the FAA); ACLU v. NSA, 493 F.3d 644, 662 (6th Cir. 2007) (holding, in a significant First Amendment controversy, that the plaintiffs had failed to prove standing because, among other reasons, their alleged injuries were too conjectural and speculative to merit redress).

[67] *Laird*, 408 U.S. at 13-14.

surveillance poses problems for mature democracy necessitating practical solutions that protect both the citizens' legitimate privacy interests and the state's ability to defend against foreign and domestic threats.[68]

III. ANALYSIS

Part III presents this Comment's primary arguments and analyses. It begins with a brief overview of existing oversight measures and proceeds to discussions of certain measures' weaknesses, various remedial proposals, and these proposals' drawbacks.

A. Existing Surveillance and Oversight Programs

Although instituted for laudable purposes,[69] United States surveillance tactics prove to be both overbroad and antithetical to fundamental United States principles.[70] The existing oversight procedures are inadequate at best and nominal at worst.[71] As discussed, "surveillance" is monolithic in neither substance nor practice;[72] indeed, just as surveillance authority developed over decades of crises and responses,[73] the government's actual surveillance mechanisms and countervailing oversight procedures are themselves numerous and emerged intermittently over history.[74]

Again, most units of United States government engage in

---

[68] *Infra* notes 99-111 and accompanying text (discussing the most promising proposals).

[69] *See generally* Mark Mazzetti and Scott Shane, *Threats Test Obama's Balancing Act on Surveillance*, N.Y. TIMES (Aug. 9, 2013), *available at* http://www.nytimes.com/2013/08/10/us/threats-test-obamas-balancing-act-on-surveillance.html (describing how President Obama, while also professing his hope that the War on Terrorism will eventually conclude, believes that surveillance tactics, along with certain controversial tools of warcraft like drones, help to successfully prosecute the war); Charlie Savage, *N.S.A. Chief Says Surveillance Has Stopped Dozens of Plots*, N.Y. TIMES (June 18, 2013), *available at* http://www.nytimes.com/2013/06/19/us/politics/nsa-chief-says-surveillance-has-stopped-dozens-of-plots.html (indicating that General Keith B. Alexander, then the head of the NSA, alleged at a House Intelligence Committee hearing regarding governmental surveillance that NSA surveillance tactics have helped thwart multiple terrorist threats against the United States).

[70] Spann, *supra* note 15, at 93.

[71] Seitz-Wald, *supra* note 38.

[72] Lyon, *supra* note 20, at 13-16.

[73] *See supra* notes 35-36, 39-40, 44 and accompanying text (discussing various surveillance statutes).

[74] *See* Greenwald, *supra* note 37 (detailing how the FISA Court operates); *see also infra* notes 78-88 and accompanying text (examining numerous surveillance tactics the U.S. government employs, including telephone wiretaps and Internet communications analyses).

surveillance,[75] as do many foreign governments.[76] But the focus here is on modern governmental surveillance, examples of which include wiretapping telephones and monitoring various forms of Internet communications, the latter of which increased exponentially as Internet use emerged and intensified in the late 20th and early 21st centuries.[77]

President George W. Bush's warrantless wiretapping program,[78] instituted at the height of wartime zealotry and hysteria, represents essentially the beginning of modern governmental surveillance. The exigencies of foreign warfare and a domestic ethos of perpetual fear and suspicion only perpetuated and empowered this program.[79] Indeed, the arguably illegal actions of the Bush Administration[80] vaulted executive authority and – and surveillance in particular – into the public consciousness. The government, operating under the auspices of inherent executive authority[81] and without receiving necessary

---

[75] Waxman, *supra* note 27.

[76] *See, e.g.*, Patrick Wintour & Nicholas Watt, *Prism: Security Services Operated Within Law, Says David Cameron*, THE GUARDIAN (June 11, 2013), *available at* http://www.theguardian.com/world/2013/jun/10/prism-british-security-law-david-cameron (describing the United Kingdom's own troubling surveillance practices); *see also* Hayes Brown, *France, Germany and Brazil Have Surveillance Agencies Too*, THINK PROGRESS (Oct. 21, 2013), http://thinkprogress.org/security/2013/10/21/2807751/france-germany-brazil-surveillance/ (indicating that those countries also engage in surveillance).

[77] *See* Kerr, *supra* note 23, at 635-36 (detailing how, beginning towards the end of the Clinton Administration, a growing understanding of the Internet inspired numerous administration officials, such as Chief of Staff John Podesta, to advocate for applying legislative protections governing telephone surveillance to the Internet, but with the outbreak of the War on Terrorism the emphasis shifted to updating antiquated laws to help the government combat belligerents).

[78] *See Bush Says He Signed NSA Wiretap Order*, CNN (Dec. 17, 2005), *available at* http://www.cnn.com/2005/POLITICS/12/17/bush.nsa/ (describing how former President Bush authorized and reauthorized warrantless wiretapping more than 30 times as part of the larger effort against foreign terrorists).

[79] *See* ELIZABETH HOLTZMAN & CYNTHIA COOPER, CHEATING JUSTICE: HOW BUSH AND CHENEY ATTACKED THE RULE OF LAW AND PLOTTED TO AVOID PROSECUTION – AND WHAT WE CAN DO ABOUT IT 2, 39-42, 76-78 (Beacon Press 2012) (detailing the Bush Administration's numerous malfeasances, including actively misleading the public to justify occupying Iraq, warrantless wiretapping, and utilizing "enhanced interrogation" techniques, i.e. torture); Risen & Lichtblau, *supra* note 6 (describing the Bush Administration's warrantless surveillance policies).

[80] RISEN, *supra* note 6, at 33. *But see infra* note 85 and accompanying text (indicating that, much to the chagrin of civil libertarians, U.S. surveillance procedures operate pursuant to valid legislation and are therefore perfectly legal); Richards, *supra* note 9, at 1942 (stating that "the general principle under which American law operates is that surveillance is legal unless forbidden").

[81] David E. Sanger, *White House Begins New Effort to Defend Surveillance Program*, N.Y. TIMES (Jan. 23, 2006), *available at*

warrants from the FISA Court, monitored phone calls to persons outside the United States in a sweeping effort to locate and apprehend suspected terrorists.[82]

More recently, PRISM,[83] a data-mining program that collects private communications from the servers of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple,[84] has come under scrutiny. Although President Bush authorized PRISM in 2007,[85] President Obama, in marked and profound contrast to the civil libertarian stance he assumed during the 2008 presidential election,[86] not only authorized PRISM's continuation, but actually expanded governmental surveillance authority and prevented the public from learning of the program's full breadth and purpose.[87] Similarly, BLARNEY,[88] another data mining

---

http://www.nytimes.com/2006/01/23/politics/23cnd-wiretap.html; *see also* Hamdi v. Rumsfeld, 542 U.S. 507, 516 (2004) (referencing the notion of the unitary executive exercising "plenary authority" embodied in the Article II Vesting Clause as justification for detaining an enemy combatant). *Hamdi* embodies how this theory is used to justify executive authority for wiretapping and was directly cited by President Bush when defending his surveillance measures. 542 U.S. at 516, 533–34.

[82] Risen & Lichtblau, *supra* note 6.

[83] *See* Barton Gellman & Laura Poitras, *U.S., British Intelligence Mining Data From Nine U.S. Internet Companies In Broad Secret Program*, WASH. POST (June 7, 2013), *available at* http://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970ccb04497_story.html (providing in meticulous detail an overview of the PRISM program and its role in U.S. surveillance/counterterrorism methods under both President Bush and President Obama).

[84] Greenwald & MacAskill, *supra* note 45.

[85] Timothy B. Lee, *How Congress Unknowingly Legalized PRISM In 2007*, WASH. POST (June 6, 2013), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/06/how-congress-unknowingly-legalized-prism-in-2007/; Gellman and Poitras, *supra* note 83.

[86] *See, e.g.*, Julie Hirschfield Davis, *Obama Surveillance Defies Campaign Civil Liberty Pledge*, BLOOMBERG (June 7, 2013), http://www.bloomberg.com/news/2013-06-07/obama-surveillence-defies-campaign-civil-liberty-pledge.html (elucidating that President Obama hypocritically embraced many of the same security policies that he made a political career out of decrying, first as Senator and then as presidential candidate); *see also* 2008 Democratic Party Platform, *available at* http://www.presidency.ucsb.edu/ws/index.php?pid=78283#axzz2igu1shkM (last visited Feb. 3, 2014) (including a section entitled "Reclaiming Our Constitution and Our Liberties," which outlines the party's intent to reject many of the security policies the Bush Administration implemented); Jonathan Easley, *Obama Says His Is 'Most Transparent Administration' Ever*, THE HILL (Feb. 14, 2013), http://thehill.com/blogs/blog-briefing-room/news/283335-obama-this-is-the-most-transparent-administration-in-history (explaining how President Obama believes his administration is, as the title suggests, the most transparent presidential administration in history).

[87] Tom Cohen, *Snowden Claims Online Obama Expanded 'Abusive' Security Programs*, CNN (June 18, 2013), *available at*

program that collects and analyzes metadata, is part of the NSA's vast arsenal of surveillance programs.

In a democracy such as the United States, one expects pervasive surveillance programs to operate under strict checks in order to prevent unconstitutional overreach and ameliorate inefficiencies.[89] Not so. At the center of this amalgamation of executive power and operative surveillance stands a single supervisory committee: the FISA Court.[90] Created in 1978 and enhanced numerous times in the 21st century during the War on Terrorism,[91] this chief check on governmental surveillance authority is not operating meaningfully.[92] Because it is literally a court within the larger federal court system – it has been dubbed a "parallel Supreme Court"[93] – the FISA Court is doubly insulated from political pressure. Its twelve members deliberate the government's surveillance requests, invariably granting most of them.[94] Additionally, the FISA Court's functionality, independent

---

http://www.cnn.com/2013/06/17/politics/nsa-leaks/; *see also* Gianluca Mezzofiore, *NSA Whistleblower Edward Snowden: Washington Snoopers Are Criminals*, INT'L BUS. TIMES (June 17, 2013), *available at* http://www.ibtimes.co.uk/articles/479709/20130617/nsa-whistleblower-edward-snowden.html (discussing how Edward Snowden claims the extent of U.S. surveillance practices is entirely hypocritical in that they target civilian infrastructure – the very practice the U.S. ostensibly demonizes).

[88] Gorman & Valentino-DeVries, *supra* note 46 (describing in part that the BLARNEY program, while actually utilized prior to the 9/11 terrorist attacks, was, post-9/11, expanded to apply to numerous Internet networks in the U.S.).

[89] This simple assumption is one of the fundamental propositions upon which our system of government is predicated. *See* AKHIL REED AMAR, AMERICA'S CONSTITUTION: A BIOGRAPHY 62-63 (2005) (explaining how the Constitution created an elaborate governmental system characterized by separated powers that check and balance each other in order to avoid concentrating excessive power in any individual branch and also to "minimize the likelihood that an *arguably unconstitutional* federal law would pass and take effect").

[90] *Supra* notes 31-33 (involving the FISA Court's creation and contemporary attention).

[91] *Supra* notes 34-36 (discussing legislation altering the FISA Court).

[92] Carol D. Leonnig, *Court: Ability to Police U.S. Spying Program Limited*, WASH. POST (Aug. 15, 2013), *available at* http://www.washingtonpost.com/politics/court-ability-to-police-us-spying-program-limited/2013/08/15/4a8c8c44-05cd-11e3-a07f-49ddc7417125_story.html.

[93] Eric Lichtblau, *In Secret, Court Vastly Broadens Powers of N.S.A.*, N.Y. TIMES (July 6, 2013), *available at* http://www.nytimes.com/2013/07/07/us/in-secret-court-vastly-broadens-powers-of-nsa.html.

[94] Seitz-Wald, *supra* note 38. *But see* Mike Masnick, *FISA Court Argues to Senate That It's Not A Rubber Stamp*, TECHDIRT (Oct. 16, 2013), http://www.techdirt.com/articles/20131015/18154624888/fisa-court-argues-to-senate-that-its-not-rubber-stamp.shtml (documenting that the FISA Court, taking umbrage at its characterization as a rubber stamp, stated that its high approval rate is for "final applications" and that it often requests substantial alterations); Benjamin Wittes, *There's a Perfectly Good NSA Defense That the Obama Administration Isn't Making*, NEW REPUBLIC (Aug. 18, 2013),

of actual surveillance requests, is inadequate to guarantee objectivity. The Chief Justice of the United States is vested with sole appointment power.[95] This is problematic because the Chief Justice, though sequestered by design,[96] is given free reign to select like-minded judges without direct political or electoral accountability.[97] Finally, the aura of secrecy surrounding the FISA Court and the nature of secret surveillance militate against airing contrary opinions within or fostering robust debate between the coordinate branches of government and the American public.[98] Unsurprisingly, such defects inspire caustic criticism and myriad proposed remedies.

B. Proposals

Numerous scholars and public officials have proffered remedies or overhauls of existing oversight structures, particularly in the aftermath of the Snowden scandal.[99] Two proposals merit particular discussion.

1. Remedies

The two proposals discussed below involve substantially altering the FISA Court – a prospect that appears to have substantial bipartisan appeal.[100] One proposal requires making

---

available at http://www.newrepublic.com/article/114364/nsa-spying-defense-case-administration-isnt-making (arguing, in part, that the characterization of the FISA Court as a rubber stamp is unwarranted).

[95] Ezra Klein, *Did You Know John Roberts Is Also Chief Justice of the NSA's Surveillance State?*, WASH. POST (July 5, 2013), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/05/did-you-know-john-roberts-is-also-chief-justice-of-the-nsas-surveillance-state/.

[96] *Compare* THE FEDERALIST NO. 78 (Alexander Hamilton) (arguing that the judiciary is the least dangerous branch because, due to its lack of power over the metaphorical sword and purse, it possesses only the power to issue judgments) *with* ALEXANDER M. BICKEL, THE LEAST DANGEROUS BRANCH: THE SUPREME COURT AT THE BAR OF POLITICS 16-23 (2nd ed. 1986) (describing how, contrary to its supposed insulation from the other branches and from political pressure, the unelected judiciary's use of judicial review constitutes a certain counter-majoritarian difficulty).

[97] Klein, *supra* note 95.

[98] Adam Serwer, *Does Obama Really 'Welcome Debate' on His National Security Policies?*, MSNBC (June 18, 2013), *available at* http://www.msnbc.com/msnbc/does-obama-really-welcome-debate-his-nat; *see also* Richards, *supra* note 9, at 1959–60 (arguing that secret surveillance is illegitimate because, as the sovereign in democracies, the people are entitled to know what their government is doing and, as a corollary, to express their support or opposition).

[99] Greg Sargent, *Reform of NSA Surveillance Is Probably Inevitable*, WASH. POST (July 25, 2013), *available at* http://www.washingtonpost.com/blogs/plum-line/wp/2013/07/25/reform-of-nsa-surveillance-is-probably-inevitable/.

[100] Andrea Peterson, *The House Is Divided Over Almost Everything. But FISA Court Reform Might Be Able to Unite It*, WASH. POST (Oct. 1, 2013),

the FISA Court procedure into a more adversarial process akin to conventional legal proceedings. The other involves granting Congress new powers to review and even directly affect FISA Court decisions and membership. Each proposal possesses significant potential and considerable limitations.

The first remedy involves appointing a privacy advocate whose sole duty would be to argue against the government's warrant requests, in essence acting as a quasi-public defender or guardian of privacy rights.[101] Such an idea is already percolating in the House of Representatives.[102] Retired Judge James Robertson, who formerly presided over the FISA Court, claims this is a necessary step[103] because the Court has frequently been merely a proverbial rubber stamp for surveillance requests.[104] Indeed, available literature suggests that the FISA Court grants over 90% of the government's requests.[105]

Introducing a privacy advocate would effectively force the FISA Court to consider individual requests from both perspectives: on the one hand, the government would present important security arguments, while the privacy advocate would focus on potential or actual dangers to cognizable privacy interests. This system would thereby promote equity in FISA Court proceedings and enable the public at large to have a representative promote privacy.

The second proposed remedy requires additional scrutiny of judges selected to serve on the FISA Court. The current Chief Justice of the United States, John Roberts, selects the other eleven FISA Court judges while also sitting at the head of that surreptitious body as its twelfth member.[106] A pending bill, the FISA Court Accountability Act ("FCAA"), would fundamentally alter FISA Court appointment and decisional procedures.[107] The FCAA would strip the Chief Justice of some appointment power and, instead, enable the four main congressional leaders – Senate majority leader and minority leader, House speaker and House

---

available at http://www.washingtonpost.com/blogs/the-switch/wp/2013/10/01/the-house-is-divided-over-almost-everything-but-fisa-court-reform-might-be-able-to-unite-it/.

[101] Matt Sledge, *Adam Schiff Prepares FISA Court Bill To Create Special Privacy Advocate*, HUFFINGTON POST (July 25, 2013), http://www.huffingtonpost.com/2013/07/25/adam-schiff-fisa-court_n_3653946.html.

[102] *Id.*

[103] *See* Dan Roberts, *US Must Fix Secret Fisa Courts, Says Top Judge Who Granted Surveillance Orders*, THE GUARDIAN (July 9, 2013), *available at* http://www.theguardian.com/law/2013/jul/09/fisa-courts-judge-nsa-surveillance (indicating that Judge James Robertson, who formerly sat on the FISA Court, believes it requires serious reformation).

[104] Seitz-Wald, *supra* note 38.

[105] *Id.*

[106] Klein, *supra* note 95.

[107] H.R. 2586, 113th Cong. (2013).

minority leader – to make some appointments.[108] The FCAA would also grant congressional authority over certain matters, including requiring a sixty–percent supermajority consensus on FISA Court rulings.[109] A similar proposal would subject FISA Court judges to additional senatorial confirmation proceedings.[110]

The FCAA and the related suggestion[111] requiring a second round of senatorial confirmation would insert an attractive balancing element that comports with the spirit of the United States government.[112] With Congress playing a more active role, the FISA Court would likely not acquiesce to every request from the executive. Enhancing Congress's role would also make the FISA Court indirectly accountable to public opinion and the consequences of intervallic democratic elections.

Ergo, the main proposals contain distinct and favorable attractions. However, they have multiple limitations, including such practical difficulties as the potential political gridlock and for constitutional violations.

2. Limitations

These good-faith proposals suffer from numerous flaws. Regarding the first proposal, the ideological composition of the FISA Court and the judiciary's historic deference to the executive in matters of foreign affairs[113] – especially as applied to domestic defense[114] – suggest that a privacy advocate would become a token figure without any influence. There is also the critical question of what role a public advocate would actually assume. Indeed, a "permanently constituted advocate seeking injunctive relief based

---

[108] *Id.*; *see also* Klein, *A Radical Plan For Shaking Up the FISA Court*, WASH. POST (July 9, 2013), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/07/09/a-radical-plan-for-shaking-up-the-fisa-court/ (discussing the FISA Court Accountability Act).

[109] H.R. 2586, 113th Cong. (2013).

[110] Tal Kopan, *Lawmaker Wants FISA Court Judges Confirmed in Senate*, POLITICO (July 17, 2013), http://www.politico.com/blogs/under-the-radar/2013/07/lawmaker-wants-fisa-court-judges-confirmed-in-senate-168576.html.

[111] *Id.*

[112] *See* Patrick M. Garry, *The Unannounced Revolution: How the Court Has Indirectly Effected a Shift in the Separation of Powers*, 57 ALA. L. REV. 689, 690 (2006) (describing the structure of the U.S. government, writing: "[federalism and separation of powers] pertain to structural provisions of the Constitution; both focus on allocating power to various government entities . . . and both act as a check on the power of the national government.").

[113] *See* Daniel R. Williams, *After the Gold Rush, Part I: Hamdi, 9/11, and the Dark Side of the Enlightenment*, 112 PENN ST. L. REV. 341, 365 (2007) (stating "[j]udicial deference to the Executive in matters of foreign affairs and warmaking indeed has a strong hold on our jurisprudential consciousness").

[114] *See, e.g.*, *Hamdi*, 542 U.S. at 518 (permitting the president to detain designated enemy combatants pursuant to the Authorization for Use of Military Force (AUMF)).

on a violation of law in the interest of the general public might be viewed as engaging in a government function," but "a private party appointed temporarily to litigate on behalf of the public might not be considered" a government agent.[115] This distinction could create Appointment Clause issues.[116] Also, the federal government may attempt to circumvent this agent by relying on the state secrets privilege.[117]

Likewise, the second proposal suffers from problems. First, the FISA Court judges are appointed from existing federal districts;[118] hence, Congress has already confirmed them. But since the FISA Court is not a traditional Article III court,[119] what role – if any – the Senate could have in potential confirmations is unclear at best. Second, requiring a supermajority consensus on FISA Court decisions is a manifestly unwise decision considering Congress's – and the country's – increasingly polarized nature.[120] Indeed, absent a supermajority by the sitting president's party, it is highly unlikely Congress could reach such a substantial threshold consensus on FISA Court surveillance decisions.[121] The polarization argument applies with equal force to the senatorial

---

[115] Jared P. Cole & Andrew Norman, Cong. Research Serv., R43451, *Reform of the Foreign Intelligence Surveillance Courts: A Brief Overview* 3 (2014).

[116] *Id.* at 3–4; *see also* U.S. CONST., art. II, § 2 (outlining the president's appointment powers).

[117] *See Reynolds*, 345 U.S. at 11 (discussing the state secrets privilege).

[118] Klein, *supra* note 108.

[119] *See* Jim Harper, *Ratifying NSA Spying, a Court Calls FISA 'Courts' Into Question*, CATO INSTITUTE (Dec. 27, 2013), *available at* http://www.cato.org/blog/ratifying-nsa-spying (discussing in part how the FISA Court is not a classical Article III court); *see also* U.S. CONST., art. III, §§ 1–2 (outlining the federal judiciary).

[120] Paul Rosenzweig, *The NSA Doesn't Need Wholesale Reform, Just Greater Oversight*, NEW REPUBLIC (Oct. 29, 2013), *available at* http://www.newrepublic.com/article/115392/nsa-reform-not-essential-congressional-oversight; *see also* RONALD M. PETERS, JR. & CINDY SIMON ROSENTHAL, SPEAKER NANCY PELOSI AND THE NEW AMERICAN POLITICS 6 (Oxford Univ. Press 2010) (discussing polarization trends); Neal Devins, *Party Polarization and Congressional Committee Consideration of Constitutional Questions*, 105 NW. U. L. REV. 737, 753–55 (2011) (indicating that party polarization rapidly accelerated around 1980, with moderates and political centrists largely disappearing).

[121] *See, e.g.*, Ezra Klein, *14 Reasons Why This Is the Worst Congress Ever*, WASH. POST (July 13, 2012), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2012/07/13/13-reasons-why-this-is-the-worst-congress-ever/ (noting how, among other things, Congress is simply failing to pass laws); Brad Plumer, *The House Farm Bill Unexpectedly Failed. So What Happens Next?*, WASH. POST (June 20, 2013), *available at* http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/20/the-house-farm-bill-unexpectedly-fails-195-234-so-what-happens-next/ (reporting how the House initially failed to pass a farm bill, which historically tend to pass Congress quite easily).

confirmation suggestion; such hypothetical confirmation proceedings would arguably be even more rancorous and partisan than regular federal judgeship confirmations[122] given the controversial nature of the FISA Court and the parties' mutual obstreperousness.[123]

In short, although the two highlighted proposals present promising prospects, their deficiencies severely blunt their effectiveness. And while some of the proposed remedies may mitigate the established system's problems from a practical perspective, more is needed to realize true reform. The FISA Court, along with lower federal courts considering individual surveillance challenges, requires an articulable substantive remedy that will fairly protect both security interests and privacy interests while also providing judicial stability and a semblance of decisional uniformity.

IV. PROPOSAL

Part IV proposes a two-pronged solution, which includes both a structural component and an interpretive component. Additionally, it discusses relevant counterarguments to the proposal.

A. Structural Prong

Despite suggested structural proposals' substantial limitations,[124] much of what has been suggested thus far could be effective if modestly modified. Requiring the Senate to reconfirm non-Article III FISA Court judges is a patently inadequate option because of the considerable constitutional problems it raises.[125] However, designating the four main congressional leaders with some appointment powers, instead of vesting this enormous responsibility exclusively in the chief justice,[126] is an intriguing approach. Furthermore, Congress should review FISA Court decisions, but only require a simple majority to approve them.[127]

---

[122] *See* David Leonhardt, *The Endless Battle Over Judicial Nominees*, N.Y. TIMES (June 22, 2013), *available at* http://www.nytimes.com/2013/06/23/opinion/sunday/the-endless-battle-over-judicial-nominees.html (describing the current trend of scuttling judicial nominees).

[123] Klein, *supra* note 121.

[124] *See supra* notes 113–123 (describing problems with the myriad solutions posed by politicians and judges for remedying FISA Court proceedings and composition).

[125] Harper, *supra* note 119.

[126] *See* FISA Court Accountability Act, H.R. 2586, 113th Cong. (2013) (proposing to alter FISA Court appointment authority and require a 60% supermajority confirmation vote).

[127] Congressional approval of FISA Court decisions via simple majority, i.e. a 51-vote threshold, is the major way this Comment's proposal differs from the FISA Court Accountability Act and other prominent suggestions. The reasons

This would avoid the infeasible supermajority threshold.[128] It would also give Congress a stake in these decisions, thereby making them politically accountable to the people, that sovereign body for whom Congress is directly responsible and to whom Congress is directly beholden, unlike the sequestered, electorally unaccountable federal judiciary.[129] In other words, the system would become more transparent – a virtue missing from the current security apparatus.[130] Finally, FISA Court proceedings must incontrovertibly become adversarial in accord with the great American tradition.

Additionally, courts – namely, the FISA Court – require a distinct framework for addressing challenges to governmental surveillance. Thus, in addition to applying these structural changes, introducing a judicial interpretive remedy is critical.

B. Interpretive Prong

Relying on the state secrets doctrine or routinely acquiescing to the government's demands cannot replace reasoned determinations of surveillance's practical effects on legitimate privacy interests or its potential overbreadth. Thus, courts should adopt a new approach that addresses both security interests and privacy interests.

Considering the relative dearth of effective judicial tests and

---

for requiring only a simple majority are rooted in pragmatism: Congress is growing increasingly polarized. *See* PETERS & ROSENTHAL, *supra* note 120, at 5-6 (discussing how Congress is more ideological and polarized than at any time in history). Thus, it would be unwise to entrust a body that is arguably paralyzed to approve important surveillance decisions by such a high margin. *See* Klein, *supra* note 121 (discussing how Congress is not even legislating efficiently).

[128] Necessitating a supermajority, i.e. 60-vote, consensus on FISA Court decisions is highly impractical and would likely produce insurmountable gridlock on an issue meriting a modicum of efficiency given the potentially profound national security interests at stake.

[129] And the FISA Court currently is doubly insulated: it is an unelected court comprising members appointed by the unelected Chief Justice alone. Klein, *supra* note 95.

[130] Criticisms about the FISA Court's lack of transparency in large part persuaded it to release a limited sampling of its prior surveillance decisions. Brian Fung, *The FISA Court Will Release More Opinions Because of Snowden*, WASH. POST (Sept. 13, 2013), *available at* http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/13/the-fisa-court-will-release-more-opinions-because-of-snowden/; *see also* LEWIS, *supra* note 52, at 243 (stating "[t]he one area of First Amendment law that most needs attention is the exception that the courts have implicitly created for *anything arguably related to the national security*") (*emphasis added*). Lewis proceeds to argue that the Court needs to rediscover the "courage of its First Amendment convictions." *Id.* The same logic applies with equal power to courts' jurisprudence in security-privacy controversies.

precedent in surveillance cases,[131] which again are generally decided pursuant to the state secrets privilege – and therefore in favor of the government[132] – a good approach is to analogize to an existing test. The best doctrinal underpinning for a new test is First Amendment law, more specifically, the various tests for defamation.[133]

Defamation cases,[134] such as libel and slander, present a dichotomy between two critical interests somewhat akin to surveillance cases: free speech and reputation.[135] In *New York Times Co. v. Sullivan*, the Supreme Court extended First Amendment protection to libel for the first time in our nation's history.[136] However, recognizing that personal reputation is as important to citizens as free speech rights, the Court subsequently carved out numerous exceptions when confronted with novel scenarios.[137] The specific test created for libel against public officials or public figures requires the plaintiff to show with convincing clarity that the defendant propagated made the defamatory statement with actual malice or with knowledge or reckless disregard of its falsehood.[138]

---

[131] *See* Jennifer Hoezler, *What You Should Know About the Foreign Intelligence Surveillance Court (FISC)*, HUFFINGTON POST (June 6, 2013), http://www.huffingtonpost.com/jennifer-hoelzer/what-you-should-know-abou_1_b_3399584.html (describing the FISA Court at length). Hoezler indicates that FISA Court judges are not necessarily well versed in surveillance law and therefore have limited ability to issue effective decisions. Plus, the judges must rely on strained interpretations of existing statutory surveillance authority. *Id.*

[132] *See Al-Haramain*, 507 F.3d at 1197 (applying the state secrets privilege, thereby preventing the plaintiffs from determining whether they were actually being monitored).

[133] *See* LEWIS, *supra* note 52, at 196 (describing three distinct tests: one for private individuals entirely outside of the public sphere, one for private individuals attacked on an issue of public interest, and one for public officials/public figures). *See also* Gertz v. Welch, 418 U.S. 323, 351-52 (1974) (addressing the surprisingly blurry distinction between public figures and private figures for defamation purposes).

[134] For a classic defamation case, see *Curtis Publishing Co. v. Butts*, 388 U.S. 130, 142-43 (1967) (involving allegedly libelous statements implicating University of Georgia athletic director Wally Butts in a bribery scandal).

[135] Of particular import for this speech/reputation dichotomy is the underlying distinction between public figures and private individuals and what degree of protection to afford both classes. *See* LEWIS, *supra* note 52, at 186 (writing that a key question in an early speech case, *Time, Inc. v. Hill*, 385 U.S. 374 (1964), was "whether that burden was justified to protect the privacy – or in a libel case the reputation – of a private person, one who had not volunteered for the rough-and-tumble of public life").

[136] 376 U.S. at 271.

[137] *See supra* note 133 (discussing how the Court has crafted several judicial tests for application depending on the identity of the allegedly defamed plaintiff).

[138] *Sullivan*, 376 U.S. at 279-80. For a more contemporary case, see *Hustler Magazine v. Falwell*, 485 U.S. 46 (1988), involving conservative evangelist Jerry Falwell's suit against *Hustler* for publishing a satirical parody

This test provides a good general framework that the judiciary should appropriate for surveillance cases. The government, bringing a surveillance request before the FISA Court, would have the same burden as public officials in defamation situations: convincing clarity.[139] Currently, the standard is probable cause[140] – far too loose when it comes to citizens' privacy. With this in mind, the government would be required to satisfy a threshold evidentiary standard by showing a substantial need for limited surveillance (the knowing or reckless falsehood prong) that is causally connected to preventing definite threats (the actual malice prong).

Of course, like any judicial test, these subjective phrases require specificity. To satisfy the "substantial need" requirement, the government would have to articulate what it intends to do with information gathered from limited surveillance.[141] As a corollary, this substantial need would have to outweigh the competing need for privacy, and it would necessarily be contingent on the government to overcome this barrier with convincing clarity.

To satisfy the "definite threat" requirement, the government would be compelled to demonstrate how desired information would help prevent an articulable threat to American interests.[142] In considering this element, the court would examine the threat on a sliding scale that considers both magnitude and probability. At one extreme would be a putative ticking time bomb scenario,

---

advertisement that suggested Falwell engaged in an incestuous relationship with his mother. The *Hustler* case is discussed at length in *Make No Law: The Sullivan Case and the First Amendment*. *See* LEWIS, *supra* note 52, at 231-33 (describing the case and concluding that it was greatly important for defamation law: it reaffirmed the validity of *Sullivan* in an era ostensibly less sensitive to civil liberties, including freedom of speech).

[139] *Sullivan*, 376 U.S. at 285-86. Convincing clarity, sometimes called clear and convincing evidence, is a more difficult standard than the typical civil suit burden of preponderance of the evidence. *Gertz*, 418 U.S. at 366. However, convincing clarity is obviously a less stringent threshold than the beyond a reasonable doubt standard in criminal cases. Anderson v. Liberty Lobby, Inc., 477 U.S. 242, 272 (1986).

[140] *See* Greenwald, *supra* note 37 (discussing in part how, while the government requires no individualized warrants to monitor domestic online communications, it must simply show probable cause to obtain surveillance warrants for domestic phone calls).

[141] Currently, the government's various surveillance programs collect and store a wide variety of communications data without accompanying explanations for how such information is utilized or why it is needed. *See supra* notes 83-88 (discussing the government's massive data-mining programs PRISM and BLARNEY). This is in part a consequence of the very liberal FISA Court alterations in 2008. Greenwald, *supra* note 37.

[142] Such a direct threat would obviously include suspected terrorist attacks but need not be that acute; for instance, if persons of interest are suspected of harboring, assisting, or communicating with terrorist cells, limited surveillance could be approved.

where the government shows surveillance is necessary to counter an identified threat that is actually at risk of transpiring; in such a situation judicial deference slides towards the government. The other extreme is a mere hypothetical threat,[143] for which surveillance is only required in the abstract; in this situation judicial deference slides towards privacy. Between these extremes are numerous situations of varying severity, and the balance may tip either way depending on the strength of the government's case.

Ideally, the FISA Court would apply the security-privacy test in an adversarial proceeding. Thus, as the government attempts to fulfill these stringent requirements, the privacy advocate would counter with evidence of the requested surveillance's effect or effects on privacy.[144] The burden, however, would always remain with the government as the entity seeking to circumvent privacy rights. And, assuming all of the structural remedies are adopted, Congress would then have to approve the surveillance decision via majority vote. These changes, however, would inevitably inspire multiple critiques.

C. Counterarguments

There are numerous counterarguments to the two-pronged proposal. First, government proponents would argue that introducing additional oversight procedures could hamper federal objectives, especially as they relate to identifying threats and apprehending suspected terrorists,[145] and create unwanted burdens. This argument is not without some import. The 2013 Boston Marathon bombing[146] is a persuasive indicator[147] that not

---

[143] Articulating definite threats is entirely the opposite of what the government currently does: showing probable cause for monitoring domestic phone calls while, shockingly, requiring no cognizable cause for online surveillance requests. Greenwald, *supra* note 37.

[144] *See* Sledge, *supra* note 101 (discussing in part the proposed privacy advocate, who would argue before the FISA Court in order to provide more balance to what is presently an entirely one-sided, and therefore biased, process).

[145] For instance, New Jersey Governor Chris Christie has stridently criticized attempts to curtail governmental surveillance, arguing that such measures will disenable the government from prosecuting the War on Terrorism and dishonor the memory of 9/11 victims. Erik Schelzig, *Rand Paul Hits Back At Chris Christie Over Surveillance*, HUFFINGTON POST (Sept. 28, 2013), http://www.huffingtonpost.com/2013/07/28/rand-paul-chris-christie_n_3668411.html. Rep. Peter King of New York also voiced similar themes. Sean Sullivan, *Rand Paul, Peter King Clash Over NSA Surveillance*, WASH POST (Aug. 18, 2013), *available at* http://www.washingtonpost.com/blogs/post-politics/wp/2013/08/18/rand-paul-peter-king-clash-over-nsa-surveillance/.

[146] *See* John Eligon & Michael Cooper, *Blasts at Boston Marathon Kill 3 and Injure 100*, N.Y. TIMES (April 15, 2013), *available at* http://www.nytimes.com/2013/04/16/us/explosions-reported-at-site-of-boston-marathon.html?_r=0 (detailing the heinous terrorist assault during the spring

only is the War on Terrorism an enduring conflict but also that enemies can emerge internally, necessitating continued monitoring of both foreign and domestic threats.

Second, there is no guarantee that a bright-line judicial test can withstand additional successful applications of the state secrets privilege.[148] Indeed, the interpretive component does not contemplate eradicating the state secrets privilege from the government's repertoire, and it may effectively become a failsafe for borderline cases, particularly at lower federal courts considering privacy claims.

However, the two-pronged proposal should quiet such criticisms. Governmental efficiency may be affected, but the system was designed not for unrestricted freedom to perpetuate controversial programs but rather for debate and contemplation,[149] those hallmarks of democracy. Furthermore, the new judicial test's substantial need and definite threat requirements should, absent the most extraordinary circumstances, overshadow the state secrets privilege.

V. CONCLUSION

Anthony Lewis wrote that the "accommodation of conflicting interests is always complicated. It requires judges to draw nice lines, it requires lawyers to argue, it requires academics to reflect."[150] Though he was speaking about libel law, Lewis's reflections apply with equal force to the security/privacy dynamic at the nucleus of surveillance law. Justice Souter clearly agrees that many legal controversies involve the "tension of competing values, each constitutionally respectable, but none open to

---

Boston Marathon).

[147] Mohamed Elibiary, *Boston Bombings and the Radicalized Homegrown Terrorist*, WASH. POST (April 30, 2013), *available at* http://www.washingtonpost.com/blogs/on-faith/wp/2013/04/30/boston-bombings-and-the-radicalized-homegrown-terrorist/. *But see* Jason Burke, *Is Terrorism Now International or Domestic?*, THE GUARDIAN (April 22, 2013), *available at* http://www.theguardian.com/world/2013/apr/22/is-terrorism-international-or-domestic (indicating that the Boston Marathon attack complicated the way in which governments view and understand terrorism, and arguing that the conventional distinction between international terrorists and domestic terrorists is both artificial and arbitrary).

[148] *See Al-Haramain*, 507 F.3d at 1197 (applying the state secrets privilege, thereby preventing the plaintiffs from determining whether the government was conducting surveillance). Ideally the new judicial test, applied in the augmented adversarial – albeit secret – FISA Court proceedings, would nullify the necessity for the government to assert this privilege, but that is uncertain.

[149] *See* AMAR, *supra* note 89, at 102 (stating that the U.S. legislature was designed to be a vigorous forum for debate); Richards, *supra* note 9, at 1965 (writing that American institutions presuppose "freedom of the mind").

[150] LEWIS, *supra* note 52, at 244.

realization to the logical limit."[151]

The government's interest in protecting the country is praiseworthy, but the right to privacy[152] is also respectable and constitutionally protected. Neither of these crucial values should be marginalized or abandoned; indeed, a strong democracy is capable of accommodating both. The proposed structural and interpretive remedies to United States surveillance tactics are important steps to realizing a more effective security apparatus that, far from dangerously impinging on cherished liberty, thoughtfully balances security and privacy in 21st century America.

---

[151] McCreary Cnty. v. ACLU of KY, 545 U.S. 844, 875 (2005).

[152] Again, the privacy concept is enormously broad. *See supra* text accompanying note 8 (describing the Constitution's textual privacy indicators). *See also* AMAR, *supra* note 89, at 326-27, 385-86 (discussing the Fourth Amendment's assurance of security in the home, papers, and effects, which includes an implied privacy component, and the Fourteenth Amendment's implied right to privacy).