Warrantless Wiretapping, FISA Reform, and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture

Paul M. Schwartz†

INTRODUCTION

The central metaphor of Stephen Holmes's Jorde Lecture[1] is a haunting one: it is of emergency room personnel taking time and care during a life-threatening situation to follow rules. These rules are ones of medical procedure that the staff carefully learns before the emergency and then faithfully follows during it. Rules should be followed during a crisis situation, Holmes tells us, because "psychologically flustering pressures" will provoke errors without such a behavior structure in place.[2]

Law should play a similar role for our leaders, and it is one that becomes more, and not less, important in responding to the terrorist threat to the United States. Holmes astutely builds on his analogy to the relatively rigid protocols upon which emergency room personnel rely.[3] He argues that rights embodied in law "demarcate provisional no-go zones into which government entry is prohibited unless and until an adequate justification can be given."[4] Thus, legal rights serve as "a trip-wire and a demand for government explanation."[5]

This mandatory process forces the Executive to explain her behavior and to confront other views. As Holmes warns, "If a government no longer has to provide plausible reasons for its actions . . . it is very likely, in the relative short

† Professor of Law, University of California, Berkeley, School of Law. For their helpful comments on this draft, I would like to thank Andrew Guzman and Daniel Solove.

1. Stephen Holmes, Keynote Address at the 11th Annual Thomas M. Jorde Symposium: In Case of Emergency: Misunderstanding Tradeoffs in the War on Terror (Nov. 5, 2007), *in* 97 CALIF. L. REV. 301 (2009).
2. *Id.* at 302.
3. *Id.*
4. *Id.* at 332.
5. *Id.*

term, to stop having plausible reasons for its actions."[6] Beyond its steadying function then, law can help the Executive "to make appropriate midstream adjustments in a timely fashion" and help everyone discover mistakes.[7] Legal rules help facilitate an "adaptation to reality."[8] In contrast, when executive behavior is shielded in secrecy, inordinate delays in correcting terrible mistakes may damage national security.

The Jorde Lecture by Holmes burns with the light of clear analysis and calm rationality. In this Essay, I wish to build on it by considering Holmes's model of "public liberty" in greater depth. Public liberty improves security by preventing policymakers from hiding errors under a veil of secrecy. It even opens up the process of debate within the executive branch itself. This Essay develops Holmes's model by discussing how private liberty, and information privacy in particular, is a precondition for public liberty. For Holmes, private liberty is largely a negative right—a right to be free from governmental interference. In contrast, my view is that privacy is also an element of public liberty. Participation in a democracy requires individuals to have an underlying capacity for self-determination, which requires some personal privacy.

This Essay then analyzes a number of Holmesian concepts through the lens of the recent process of the amendment of the Foreign Intelligence Surveillance Act (FISA).[9] Since information privacy stands at the intersection of private and public liberty, it is an ideal topic for evaluating Holmesian principles about the contribution of law during times of national emergency. This Essay considers, in particular, the Bush administration's policies toward FISA and Congress's amendment of this statute.

In Part I, I describe the background of FISA and the National Security Agency's (NSA) warrantless surveillance in violation of this statute. I also discuss the amendments to FISA in the Protect America Act of 2007—a short term statutory "fix" that has expired—and the FISA Amendments Act of 2008, which remains in effect.[10] In Part II, I turn to an analysis of the challenges to private and public liberty posed by the NSA's surveillance. I organize this Part around three topics: (1) past wisdom as codified in law; (2) the impact of secrecy on government behavior; and (3) institutional lessons. As we shall see, a Holmesian search for the wisdom previously collected in law proves quite difficult. FISA regulated some aspects of intelligence gathering and left the intelligence community entirely free to engage in others. Over time, moreover, technological innovations and altered national security concerns transformed

6. *Id.* at 329.
7. *Id.* at 307.
8. *Id.* at 334.
9. Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. §§ 1801-1812, 1821-29, 1841-46, 1861-63 (2000 & Supp. V 2005).
10. Protect America Act of 2007 (PAA), Pub. L. No. 110-55, 121 Stat. 552; FISA Amendments Act of 2008, Pub. L. No. 110-261, 122 Stat. 2436.

the implications of the past policy landscape. As a result, the toughest questions, which concern surveillance of foreign-to-domestic communications, do not receive an easy answer from the past.

Regarding the impact of secrecy on government behavior, the analysis is, at least initially, more straightforward. As Holmes discusses, the Bush administration was adept at keeping secrets not only from the public and other branches of government, but from itself. Even then-Attorney General John Ashcroft faced restrictions on his ability to receive legal advice within the Department of Justice about NSA activities, the legality of which he was required to oversee. It is also striking how little Congress knew about NSA activities while amending FISA. The larger lessons, however, prove more complicated: strong structural and political factors are likely to limit the involvement of Congress and courts in this area. This Essay concludes by confronting these institutional lessons and evaluating elements of a response that would improve the government's performance by crafting new informational and deliberative structures for it.

I
PUBLIC LIBERTY, INFORMATION PRIVACY, AND HOLMESIAN LESSONS

This Part first examines Holmes's concept of public liberty. It then turns to a discussion of Congress's amendment of FISA in the shadow of warrantless surveillance by the NSA. This process culminated recently with the enactment of the FISA Amendments Act of 2008.

A. Public Liberty: An Introduction

One of the great contributions of the Jorde Lecture is Holmes's elaboration of his concept of public liberty. Holmes draws an important distinction between "private liberty from government interference" and "[t]he public liberty to examine one's government, expose its mistakes, and throw it out of office."[11] Public liberty empowers citizens by allowing them to compel government to justify its action. It is a means for promoting "collective rationality" that functions through the "examination and criticism of government by alert citizens."[12] Through public liberty, governments are led to ponder alternatives and engage in self-critical thinking. An example of public liberty in action would be a government that listens to independent experts, that shows flexibility in processing new information, and that abandons false certainties.

In this fashion, public liberty plays a significant role in improving security by preventing policymakers from hiding their errors from the public and Congress behind a veil of secrecy. Holmes points out another reason why

11. *Id.* at 323.
12. *Id.*

excessive secrecy is problematic: "The executive branch cannot hide from Congress, the courts, the public, and the press, without hiding from itself as well."[13] When important executive branch officials conceal information from others with a need to know within their own branch of government, significant problems will arise. Indeed, as Holmes argues in *The Matador's Cape*, the Bush administration suffered at many junctures from a bad case of self-deception.[14] Its secrecy was accompanied not only by an eagerness to deceive others, but also a fervent belief in its own illusions.[15]

From this perspective, the so-called "unitary executive" proves not to be a single unit. Rather, a ruling clique within it can suppress information to limit the power of potential bureaucratic rivals as well as experts within the executive branch who might have dissenting views. In the next Part of this Essay, I will describe a specific example of such secrecy, which involves a restriction on then Attorney General Ashcroft's ability to seek legal advice from the Department of Justice regarding a secret intelligence gathering program.

Public liberty ultimately enhances collective rationality—it is a path to heightening our wisdom by increasing access to pertinent information and improving decision making. As Holmes notes, "all people, including politicians, are prone to error; all people, especially politicians, dislike admitting their blunders," but "all people relish disclosing the miscalculations and missteps of their bureaucratic or political rivals."[16] Because no one likes to admit mistakes, a real danger exists that an emphasis on secrecy and speed will impede this crucial source of error recognition and error correction and with it the government's ability to analyze new threats in a self-critical fashion. This danger proves quite critical because of the need for the government to engage in what Holmes terms "security-security tradeoffs."[17] As he observes, "There are no zero-risk options in the war on terror."[18] Due to scarce resources and opportunity costs, the government must make choices "of security along one dimension for security along another."[19]

The next Part of this Essay will assess public liberty and related ideas in the context of the Bush administration's policies toward FISA. This statute was enacted in 1978 in response to a history of governmental abuses of civil rights. It regulates intelligence agencies' use of electronic surveillance, physical searches, and other activities in gathering intelligence information. As David Kris and Douglas Wilson state, "There is a relatively recent and very extensive

13. *Id.* at 330.
14. STEPHEN HOLMES, THE MATADOR'S CAPE 307 (2007).
15. *Id.* at 320-23.
16. Holmes, *supra* note 1, at 324.
17. *Id.* at 318.
18. *Id.* at 319.
19. *Id.*

history of intelligence activities infringing on the rights of Americans."[20] FISA offers a fitting area for evaluating Holmesian principles because its core subject, information privacy, stands at the crossroads of both private and public liberty. FISA creates standards and processes for the government to meet before it can gather personal information as part of certain foreign intelligence activities.

Here, one can build on an aspect of Holmes's analysis in his Jorde Lecture. Private liberty, as Holmes explains it, is merely equivalent to a negative right—a right to be free from government interference.[21] Yet, privacy is a personal interest that also plays an important role in preserving public rights. To relate this line of inquiry back to Holmes's idea of public liberty, examination and criticism of government behavior requires individuals to have an underlying capacity for self-determination, and this ability in turn requires some level of personal privacy. Holmes also shares this view. He notes that "democracy depends on maintaining a certain balance between the secrecy of government and the privacy of citizens."[22] He also warns, "At a certain point, we must worry that an under-scrutinized government ruling an over-scrutinized society will lose its essentially democratic character."[23]

In particular, perfected surveillance of naked thought's expression, especially in a digital age, will short-circuit the individual's decision making process. As I have argued elsewhere, the role of information privacy is to set limits on access to information that will have an impact on the extent to which certain actions or expressions of identity are encouraged or discouraged.[24] Privacy is in this sense a constitutive element of personal and community identity alike. Like public liberty, private liberty, bolstered by laws that safeguard information privacy, is a way to bolster collective rationality.

B. FISA, NSA Warrantless Wiretapping, and the FISA Amendments Act

Enacted first in 1978 and subsequently amended on numerous occasions, FISA establishes standards and procedures for use of electronic surveillance to collect "foreign intelligence."[25] Its rules differ from those of the legal regime that governs electronic surveillance for domestic law enforcement purposes, the Electronic Communications Privacy Act (ECPA).[26] ECPA concerns traditional criminal investigations; for instance, it can be used to authorize the FBI to

20. DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 2:2 at 2-3 (2007).

21. Holmes, *supra* note 1, at 323.

22. *Id.* at 327.

23. *Id.*

24. Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658-62 (1999).

25. 50 U.S.C. § 1801(e).

26. Electronic Communications Privacy Act, 18 U.S.C.A. §§ 1367, 2521, 2701-2711, 3117, 3121-3127.

engage in electronic surveillance of a crime family. FISA concerns the gathering of intelligence in the United States about a foreign power, an agent of a foreign power, terroristic organizations, or "a lone wolf" terrorist. For example, a United States intelligence agency would use its authority under FISA to gather foreign intelligence when investigating an al-Qaeda cell in the United States.

In December 2005, a front page article in the *New York Times* first revealed that the NSA was intercepting communications where one party was located outside the United States and the other party inside the United States, and it was doing so without gaining warrants from the Foreign Intelligence Surveillance Court (FISC).[27] This activity proved enormously controversial; the NSA did not follow the procedures that FISA established for such surveillance. Rather than seek to amend FISA to gain new kinds of investigative authority pursuant to law, the Bush administration had the NSA carry out this activity secretly for years.

Established in 1952, the NSA collects and analyzes foreign signals intelligence information. As Frederick Schwarz Jr. and Aziz Huq explain, "The NSA collects signals intelligence from telegrams, telephones, faxes, e-mails, and other electronic communications, and then disseminates this information among other agencies of the executive branch."[28] The NSA itself is no stranger to controversy. The enactment of FISA in 1978 was preceded by Senate and House investigations that had revealed abuses by the NSA, FBI, and other government agencies and officials. For example, the NSA had engaged in activities such as collecting millions of international telegrams sent from the United States, while the FBI maintained watch lists of U.S. citizens involved in political protests.[29] The Church Committee, which was the Senate investigatory committee, reported:

> Too many people have been spied upon by too many Government agencies and [too] much information has been collected. The Government has often undertaken the secret surveillance of citizens on the basis of their political beliefs, even when those beliefs posed no threat of violence or illegal acts on behalf of a hostile foreign power.[30]

Congressional investigations from 1975-1976 found that "the NSA had not

27. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16. 2005, at A1.

28. FREDERICK A.O. SCHWARZ JR. & AZIZ Z. HUQ, UNCHECKED AND UNBALANCED: PRESIDENTIAL POWER IN A TIME OF TERROR 127 (2007).

29. SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 6-7 (1976) [hereinafter SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS], *available at* http://www.aarclibrary.org/publib/contents/church/contents_church_reports_book2.htm.

30. *Id.* at 5.

exercised its vast power with restraint or due regard for the Constitution."[31]

After 9/11, the NSA had again started secret surveillance activities within the United States. Once the *New York Times* revealed this NSA warrantless wiretapping, the White House vigorously defended this activity, which it termed "the Terrorist Surveillance Program" (TSP). As President Bush stated, "The activities I have authorized make it more likely that killers like these 9/11 hijackers will be identified and located in time."[32]

The Bush administration has discussed aspects of the TSP, but the full extent of the NSA's activities remains unknown. Several lawsuits have challenged the legality of the NSA surveillance. Some of these cases were brought against the NSA; others against the telecommunications companies that cooperated with the government in conducting the surveillance.[33] There have also been allegations in the media that the NSA has engaged in a program of surveillance of purely domestic communications.[34] Indeed, in August 2007, Mike McConnell, the director of national intelligence, stated that TSP "applied only to 'one particular aspect'" of "'a number of . . . intelligence activities.'"[35]

Although traditional Article III courts have not yet ruled on the TSP in a conclusive fashion, the Foreign Intelligence Surveillance Court (FISC) has issued important non-public decisions about it. Pursuant to FISA, the FISC, a special court, reviews the government's request for a FISA surveillance order. This court is staffed by a small number of federal district court judges; there are now eleven FISC judges.[36] FISC proceedings are ex parte, with the Department of Justice (DOJ) making the application to the court.[37] The FISC meets in secret, and its proceedings are generally not revealed to the public or to the targets of the surveillance.

Early in 2007, a FISC decision denied permission for certain NSA surveillance activities. Some information about the secret opinion has been leaked to the press. According to the *Los Angeles Times*, the FISC refused an NSA request to engage in surveillance of multiple targets rather than a specific and determinate suspect or suspects.[38] The NSA request concerned a so-called "basket warrant," which also has been termed a kind of "umbrella

31. SCHWARZ & HUQ, *supra* note 28, at 128.

32. President's Radio Address (December 17, 2005), http://www.whitehouse.gov/news/releases/2005/12/20051217.html.

33. *See, e.g.*, ACLU v. NSA, 493 F.3d 644 (6th Cir. 2007); Hepting v. AT&T, 439 F. Supp. 2d 974 (N.D. Cal. 2006), *vacated*, 539 F.3d 1157 (9th Cir. 2008) (remanded in light of FISA Amendments Act of 2008); Terkel v. AT&T, 441 F. Supp. 2d 899 (N.D. Ill. 2006).

34. *See, e.g.*, Seymour M. Hersh, *Listening In*, NEW YORKER, May 29, 2006, at 26, *available at* http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh.

35. Dan Eggen, *NSA Spying Part of Broader Effort*, WASH. POST, Aug. 1, 2007, at A1.

36. 50 U.S.C. § 1803(a) (2006).

37. For a discussion of applications under FISA for court orders authorizing electronic surveillance, see KRIS & WILSON, *supra* note 20, § 6:2, at 6-2 to 6-9.

38. Greg Miller, *New Limits Put on Overseas Surveillance*, L.A. TIMES, Aug. 2, 2007, at A16.

surveillance." Under FISA, the FISC traditionally was required to make a probable cause determination regarding each "target," that is individual, and each "facility" of telecommunications before surveillance could be carried out.[39] The NSA request called for a different approach. Under it, the NSA would sweep in a wide amount of data up front and then sift through it. The process involved is likely some kind of data mining, which I will discuss in more detail below. At the end of the sifting process, the FISC would review the NSA judgment as to the captured data.[40] An anonymous official also explained that the FISC ruling concerned cases "'where one end is foreign and you don't know where the other is.'"[41] The Bush administration had argued that the FISC's opinion impeded the government's ability to investigate threats of imminent terrorist attacks and necessitated amendment of FISA.

This saga has two additional chapters, both of which involve recent amendments to FISA. The first such amendment is the Protect America Act of 2007 (PAA), which was made subject to a sunset and has now expired. The second is the FISA Amendments Act of 2008 (FAA), which is still in effect.

In the summer of 2007, Congress enacted the PAA, which had the effect of authorizing the NSA surveillance program.[42] It did so after a volley of White House threats issued through the media. Consider the following exchange between a reporter and Mike McConnell, the Director of National Intelligence: "Q. So you're saying that the reporting and the debate in Congress means that some Americans are going to die? A. That's what I mean. Because we have made it so public."[43]

The PAA was an administration-friendly bill; one of its most notable provisions freed electronic surveillance from FISA constraints when it is "directed at a person reasonably believed to be located outside of the United States."[44] The PAA did not define the critical term "directed at," but assigned responsibility to the attorney general to shape it through the development of "reasonable procedures."[45] Finally, this law did not require a link between the subject of surveillance and an agent of a foreign power or terrorist. It only

39. *See* KRIS & WILSON, *supra* note 20, § 6:2, at 6-2 to 6-9.

40. As Kris summarizes, the idea was "to move the individualized probable-cause determination from the front end, to the back end, of the FISA process." KRIS & WILSON, *supra* note 20, § 15:18, at 15-33.

41. Miller, *supra* note 38.

42. The Protect America Act created an exception to FISA's requirements. The exception, section 105A, exempted all communications "directed at" people outside of the United States from FISA's definition of "electronic surveillance." Once a communication fell within section 105A, the government could carry it out subject to section 105B and its requirements—rather than FISA and its obligation to seek a warrant from the FISC. Protect America Act § 2 (codified as amended at 50 U.S.C.A. §§ 1805(a)-(b)).

43. Chris Roberts, *Transcript: Debate on the Foreign Intelligence Surveillance Act*, EL PASO TIMES, Aug. 22, 2007, *available at* http://www.elpasotimes.com/news/ci_6685679.

44. Protect America Act § 2.

45. *Id.*

required that a "significant purpose of the acquisition" be the "obtain[ment] [of] foreign intelligence information."[46] Congress passed the PAA subject to a 120- day sunset, and then went on its summer recess.

Ultimately, Congress allowed the PAA to expire and did not enact a new law. The expiration was due to a revolt by certain House Democrats, who refused to buckle to White House threats and agree to a Senate Bill that, among other elements, contained immunity provisions for telecommunications companies that had participated in the TSP. At that point, the original FISA once again took effect until July 2008, when Congress enacted the FISA Amendments Act of 2008 (FAA). This enactment was due to the decision of House Democrats from Southern states, the so-called "Blue Dogs," to support the Senate Bill and to defect from support of the House Bill that had denied immunity to telecommunications providers.

The FAA of 2008 is the final chapter in this statutory story (at least thus far). It establishes new rules for at least some of the contested NSA behavior. While it expands the government's surveillance abilities, it also adds some new privacy protections. Its most important expansion of surveillance authority is to allow government collection of information from U.S. telecommunications facilities where it is not possible to know in advance whether a communication is purely international (where all parties are located outside of the United States) or whether the communication involves a foreign power or its agents. Like the PAA in 2007, the FAA in 2008 appears to authorize the TSP.

FAA amends FISA to permit "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[47] The person targeted must not be a United States person. The critical substantive requirements are (1) the "target" of the surveillance is located overseas, and (2) a "significant purpose" of the surveillance must be to acquire foreign intelligence information.[48] The collection of the information must be carried out pursuant to certain "targeting procedures" that ensure that the collection is targeted at persons located outside the United States.[49]

The acquisition must also involve new minimization procedures, which the attorney general is to adopt.[50] The FAA's requirement of minimization is not a new one for FISA. As the leading FISA treatise explains, the idea of minimization generally is that electronic surveillance pursuant to FISA be implemented to ensure conformity to its "authorized purpose and scope" and in a fashion that requires the government to collect the least amount of "irrelevant

46. *Id.*

47. FISA Amendments Act of 2008 (FAA), Pub. L. 110-261, § 702(a), 122 Stat. 2436 (codified as amended at 50 U.S.C.A. § 1881(a) (2008)).

48. *Id.* §§ 703(b)(1)(C)(i), 703(b)(1)(F)(ii) (codified as amended at 50 U.S.C.A § 1881(b) (2008)).

49. *Id.* § 702(c)(1)(A).

50. *Id.* § 702(e).

information."[51] The attorney general's minimization procedures under the FAA, regarding the targeting of persons outside the United States, must comply with FISA's existing requirements. It should be noted, moreover, that these requirements contain a significant possible escape valve. FISA states that minimization must be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[52] Finally, in advance of surveillance activity, the FAA also requires the DOJ and the Director of National Intelligence to certify that targeting and minimization procedures meet the statutory standards and that "a significant purpose" of the surveillance is to acquire foreign intelligence information.[53]

Concerning the role of the judiciary, the FAA requires the FISC to review certifications and the targeting and minimization procedures adopted. If a certification does not "contain[] all the required elements," or the procedures "are [not] consistent with the requirements" of the FAA, the FISC must issue an order directing the government to correct any deficiencies.[54] The FAA also explicitly instructs the FISC to review whether this statute comports with the Fourth Amendment. Many aspects of the constitutional requirements for the government in carrying out intelligence surveillance with domestic components are unsettled.[55] At the same time, the FISC, like any Article III court, already has this authority of constitutional review. As a consequence, it is unclear how much additional weight the FAA or any statute adds to the power of judicial review by explicitly requesting it.

We have thus far considered Congress's crafting of new rules for some of the contested NSA behavior through the FAA. This statute also expands FISA's existing privacy protections. Until this new enactment, FISA had not regulated surveillance of targets, whether U.S. citizens or not, when they were located *outside* the United States. The FAA now requires that a FISC approve surveillance of a U.S. citizen abroad based on a finding that the person is "an agent of a foreign power, or an officer or employee of a foreign power."[56]

The statute also contains a prohibition on "reverse targeting." As discussed, the FAA permits surveillance of foreign-to-domestic communications that have a nexus to "foreign intelligence." Reverse targeting would involve the government using this link as a pretext to gather intelligence about the domestic party to the communication. The FAA states that the government cannot target "a person reasonably believed to be outside the

51. KRIS AND WILSON, *supra* note 20, § 9:1, at 9-1.

52. 50 U.S.C. § 1801(h).

53. FISA Amendments Act § 702(g)(2).

54. *Id.* § 702(i)(3).

55. The leading case is *United States v. United States District Court* (the *Keith* case), 407 U.S. 297 (1972). For a discussion, see KRIS & WILSON, *supra* note 20, at 3-15 to 3-18; DANIEL J. SOLOVE & PAUL M. SCHWARTZ, INFORMATION PRIVACY LAW 360-61 (3d ed. 2009).

56. FISA Amendments Act § 704(b)(3)(b) (codified as amended at 50 U.S.C.A. § 1881(c) (2008)).

United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."[57] As a final privacy safeguard, the FAA also contains new mechanisms for congressional oversight and crafts new audit functions for the Inspectors General of the DOJ and intelligence community. I will return to these safeguards in Part III.

One of the most contentious issues in foreign intelligence policy has been immunity for telecommunications providers. A major roadblock to passing a FISA amendment had been whether Congress should grant legal immunity for companies that participated in TSP or similar programs. As we have seen, the House bill lacked such a measure, while the Senate bill and the FAA contained it. President Bush stated that such a safeguard was needed to provide "meaningful liability protection to those who are alleged to have assisted our nation following the attacks of September 11, 2001."[58] Yet, at the time that TSP began, FISA already contained immunity provisions.[59] FISA stated that "[n]o cause of action" would lie "in any court against any provider of wire or electronic communication service . . . for providing information, facilities, or assistance in accordance with the terms of . . . this chapter."[60] Therefore, the cooperation of the telecommunication companies with the NSA must have been *outside* the existing FISA safe harbor language.

Title II of the FAA provides such immunity to telecommunications companies and thereby raises a new challenge to the litigation challenging the TSP. Specifically, the FAA prohibits a civil action against anyone for assisting the intelligence community in connection with an activity that falls within a defined safe harbor.[61] The assistance in question had to be (1) authorized by the president during the period beginning on September 11, 2001, and ending on January 17, 2007; (2) designed to detect or prevent a terrorist attack; and (3) the subject of a written request from the attorney general or the head of the intelligence community. The attorney general must certify that the party who is being sued falls within this safe harbor, and the court presented with such a certificate must review it for the support of "substantial evidence."

II
A HOLMESIAN PERSPECTIVE ON NSA SURVEILLANCE

An analysis of the challenges posed to private and public liberty by NSA warrantless wiretapping and the amendments to FISA, informed by a Holmesian perspective, can be organized around three topics: (1) the

57. *Id.* § 702(b)(2).

58. Press Release, President Bush Commends Congress on Passage of Intelligence Legislation (Aug. 5, 2007), *available at* http://georgewbush-whitehouse.archives.gov/news/releases/2007/08/20070805.html.

59. 18 U.S.C.A. § 2511(2)(a)(ii) (2008).

60. *Id.*

61. *Id.* § 802.

lawmaker's attitude toward past wisdom as codified in law; (2) the impact of secrecy on government behavior; and (3) institutional lessons. Has FISA helped facilitate an "adaptation to reality," as Holmes puts it, by forcing the government to provide "plausible reasons for its actions"?[62]

A. The Attitude Toward Past Wisdom as Codified in Law

While rapidly changing technology and global security imperatives have prompted FISA reform, a Holmesian perspective urges lawmakers to consider the wisdom of previously codified rules governing surveillance. Recall that Holmes warns against harms to privacy—especially when they occur with excessive governmental secrecy. The NSA warrantless surveillance, accompanied by a lack of congressional scrutiny or any level of public knowledge, fits the outlines of just such a situation in which the public's privacy shrinks and the government's secrecy expands.

The enactment of FISA in 1978 reflects the lessons regarding the perils of unrestricted executive discretion and the use of the intelligence community within the United States.[63] A pair of important congressional investigations, led by Senator Frank Church and Representative Otis Pike respectively, revealed these dangers and a history of past abuses of intelligence powers. Yet, at the same time, FISA also left unregulated the collection of information *outside* of the United States. The United States and the United Kingdom have long been engaged in a joint program for intercepting satellite communications; this program is termed ECHELON and is not regulated by FISA.[64] FISA also does not regulate surveillance by the U.S. intelligence community on communications cables in international waters and foreign countries. As the Kris and Wilson treatise summarizes, "In general, FISA applies only to investigative conduct inside the United States."[65] Congress expressed an intention in 1978 when enacting FISA to return to the issue of surveillance outside of the country, but did not do so. Its absence from this regulatory field is in part due to the complexity of the policy issues, and also due to the relative weakness of other branches of government compared to the executive branch in the area of national security.[66] I return to this topic below.

Another key lesson from FISA is its adaptability. The statute was not frozen in place in 1978; it has been amended both before and since 9/11 as the government has responded to new national security threats. For example,

62. Holmes, *supra* note 1, at 329, 324.

63. *See, e.g.*, SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS, *supra* note 29, at 7-10.

64. PATRICK RADDEN KEEFE, CHATTER 50-75 (2005).

65. KRIS & WILSON, *supra* note 20, § 4:2, at 4-4.

66. In the absence of congressional activity, the main legal authority for surveillance abroad, apart from a president's inherent constitutional powers, is Executive Order 12333. For a case examining this Executive Order, see U.S. v. Bin Laden, 126 F. Supp. 2d 264 (S.D.N.Y. 2000).

Congress amended FISA in 1994 to permit physical searches of foreign intelligence agents.[67] After 9/11, amendments increased cooperation among and sharing of information between intelligence agencies and traditional law enforcement.[68] Additionally, Congress amended the definition of an "agent of a foreign power" to extend to so-called "lone wolf" terrorists, non-U.S. persons who engage in international terrorism or preparatory activities of international terrorism.[69] This amendment, called the "Moussaoui-fix," was a response to the FBI's difficulty, before the terrorist attacks on September 11, 2001, in linking Zacharias Moussaoui to a known terrorist organization.[70]

In thinking about these past amendments, and the critical issues at stake in the recent round of changes to FISA, one must also keep in mind two technological issues that prompted the need for FISA modernization after 9/11. One poses a difficulty for government surveillance; the other offers new promise to heighten its effectiveness. The first technological issue is the increasing challenge of determining the source of an electronic communication. FISA was based on a paradigm in which land-line telephones were associated with area codes and country codes, which made it possible to know if someone was located in the United States or not. In contrast, e-mails, Voice Over Internet Protocol (VOIP), and other kinds of digital telecommunications are not necessarily linked to a physical location. As David Kris explains, "[T]he central operational problem in foreign intelligence surveillance is the difficulty of determining, at least in real time, the location of communicating parties who do not wish to be found."[71]

The second technological issue concerns advances in computer hardware and software that make it possible to collect massive amounts of information and sift through it using search parameters. This process, termed "data mining" is a possible solution to the government's problem of correlating identity and location. It offers a kind of "vacuum-cleaner" capacity to sift vast stores of digital information. Difficult questions remain, however, regarding how such surveillance activities can be reconciled with FISA's traditional warrant requirements for collecting foreign intelligence information in the United States.[72]

---

67. *See* 50 U.S.C.A. § 1821(5).

68. The two critical amendments were Section 218 and Section 504 of the Patriot Act of 2001. For a discussion, see KRIS AND WILSON, *supra* note 20, § 10:10, at 10-23 to 10-25.

69. Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. No. 108-458, 118 Stat. 3638 (Dec. 17, 2004).

70. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 273-76 (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.

71. David S. Kris, Modernizing the Foreign Intelligence Surveillance Act 27 (Nov. 15, 2007) (working paper, on file with the Brookings Institute), *available at* http://www.brookings.edu/papers/2007/1115_nationalsecurity_kris.aspx.

72. *See id.*; *see also* Orin Kerr, Updating the Foreign Intelligence Surveillance Act, 75 U. CHI. L. REV. 225, 234 (2008) (discussing how "today's surveillance tends to be divorced from the identity and location of the parties to the communication").

It is important to note that the concept of data mining was not unknown to the Congress that enacted FISA, nor the ones that subsequently amended it on several occasions. Here, we see that identifying a legal codification of wisdom, as Holmes wishes, can be a complex task—especially when technology is involved. Holmes speaks of rules embodied in law "as steadying guidelines, focusing our aim, and reminding us of long-term objectives and collateral dangers that might otherwise slip from view in the flurry of an unfolding crisis."[73] But what past wisdom does FISA embody? FISA had permitted data mining so long as it was carried out on telecommunications captured outside of the United States. The difficulty of determining the source of an electronic communication, as noted above, makes this an increasingly unstable compromise in the twenty-first century.

In addition, FISA's history fails to provide a direct answer to the question of how Congress should treat telecommunications with both a foreign and a domestic component. On one hand, there had been a requirement for warrants in such instances. On the other hand, FISA had entirely omitted from its coverage the issue of how to treat these communications when captured outside the United States, such as from a satellite positioned above the earth.

To restate the first of the Holmesian questions: How does the FAA draw on this complex past, and how does it modify the existing structure of FISA? In some respects, the FAA abrogates past lessons about the importance of checks on the executive branch. As Marty Lederman has concisely summarized, the FAA "gets rid of the FISA requirement of a court order (and a finding that the target is an agent of a foreign power) for foreign-to-domestic phone calls and e-mails that are intercepted in the U.S."[74] The FAA permits the government to respond to uncertainty about the location of a target and to draw on new data mining capacities. As already noted, it does so by permitting "targeting of persons reasonably believed to be outside the United States" where a "significant purpose" of the surveillance is to acquire foreign intelligence information.[75]

Thus, the FAA removes FISA's requirement of a judicial determination concerning the identity and location of a specific "target of the surveillance." Rather, the judicial determination need only be that a *process* of surveillance is able to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[76] The change is significant. To quote Lederman again, the NSA has now obtained the ability under the FAA "to intercept foreign communications coming over domestic wires where (i) it does not have probable cause to believe that *any* of the parties is a terrorist

73. Holmes, *supra* note 1, at 303-04.

74. Posting of Marty Lederman to Balkanization, http://balkin.blogspot.com/ (July 11, 2008, 08:21 EST).

75. FISA Amendments Act § 702.

76. *Id.*

or agent of a foreign power; *and* (ii) there is a chance that some of the intercepted communications will be with persons in the U.S."[77]

At the same time, however, the FAA does honor some of the lessons of FISA's history by adding several checks to the government's new powers. These include requirements for targeting and minimization (already discussed above), for audits by inspectors general, and for sharing certain kinds of information with congressional committees. The information to be shared with Congress includes a semiannual assessment by the attorney general and director of national intelligence about compliance with their new targeting and minimization procedures.[78] In addition, the intelligence community is to carry out an annual review regarding their acquisition of information authorized by the FAA and provide this report to certain congressional committees.[79] There is also a judicial oversight role. The FISC is to review the new procedures subject to "the need of the United States to obtain, produce, and disseminate foreign intelligence information."[80]

As a final similarity to the original FISA, the FAA does not explicitly address the question of data mining. As noted above, the NSA appears to engage in such activities, which raise complex legal questions under FISA standards regarding probable cause and its concepts concerning specification of targets and facilities. To the extent that there is regulation of this practice, it takes place outside of direct congressional purview. The regulation will occur through the attorney general's evaluation of the NSA's processes for minimization and targeting, and the FISC's review of these processes. It is worth noting, moreover, that there is an emerging policy consensus regarding the appropriate legal safeguards needed for data mining. As the Pentagon's Terrorism and Privacy Advisory Committee stated in 2004, "Data mining is a vital tool in the fight against terrorism, but when used in connection with personal data concerning U.S. persons, data mining can present significant privacy issues."[81]

Given the heightened importance of data mining to modern intelligence gathering, it would have been constructive for the FAA to spell out certain specific safeguards for the use of data mining, and require the Attorney General to certify, and the FISC to review, whether the NSA's procedures fulfilled these conditions. Elements of the emerging consensus include requirements that data mining be used in conjunction with: access controls and authentication of users; a rule-based processing; anonymization of data in initial searches with only

77. Posting of Marty Lederman to Balkanization http://balkin.blogspot.com/ (Aug. 2, 2007, 11:47 EST).

78. FISA Amendments Act § 702(l)(1).

79. *Id.* § 702(l)(2)(D)(iii).

80. 50 U.S.C. § 1801(h)(1) (2006).

81. TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM, at viii (2004), *available at* http://epic.org/privacy/profiling/tia/tapac_report.pdf.

selective revelation of personal data; audit functions; protections to address false positives; and general and specific accountability functions. [82] At the same time, however, there are also significant voices raised in dissent regarding this policy consensus. [83]

All and all, the first Holmesian factor, a need to consider past wisdom embodied in law, proves difficult to assess in this context. In a recent article, however, Jed Rubinfeld views FISA and its history in far different terms. As he puts it, "FISA has stuck."[84] By this phrase, Rubinfeld wishes to indicate that there are relatively clear cut FISA-principles, that is, a solid statutory framework, and one that has endured. In his reading, "FISA requires the executive not only to obtain authorization from specially designated judges in almost all wiretapping cases involving United States persons, but also to notify these judges—and to a lesser extent, congressmen too—of foreign intelligence wiretaps even when no authorization is required and even when the surveillance exclusively targets foreign powers."[85] In consequence, Rubinfeld reads FISA and the Fourth Amendment as requiring judges to meet programs such as the NSA warrantless wiretapping program "with intense constitutional suspicion."[86]

This logic only gets us so far. First, there is evidence, as discussed above, that the FISC did meet the NSA program with skepticism. The issue then became how Congress should react. Second, and regarding this issue of congressional action, the history of FISA, its detailed and even convoluted statutory approach to core concepts as such as "targeting" and "facilities," and even the constitutional caselaw in this area, provides a more complex landscape and one with more shades of gray than Rubinfeld acknowledges. In important congressional testimony, Kris, one of the most knowledgeable FISA experts, concluded his analysis of the NSA program circa 2006 in the light of FISA and relevant caselaw with the guarded observation that it likely raised "significant legal questions."[87] It is no easy task to assess the legal codification of past wisdom in FISA, and it provides only so much guidance for the future.

---

82. For a discussion of the emerging policy agreement, see Ira Rubinstein, Ronald Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 266-70 (2008).

83. These dissenters speak from a variety of policy perspectives. *See* Jed Rubinfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 152 (2008); RICHARD A. POSNER, NOT A SUICIDE PACT 96-97 (2006); BRUCE SCHNEIER, BEYOND FEAR 253-54 (2003). As a result of this dissent, the policy agreement about data mining can at best be viewed as tentative.

84. Rubinfeld, *supra* note 83, at 159.

85. *Id.*

86. *Id.* at 160.

87. The Kris testimony from 2006 is reprinted at KRIS & WILSON, *supra* note 20, §§ 15:1-18, at 15-1 to 15-54.

B. The Impact of Secrecy

Holmes warns of the negative impact of secrecy on decision making. This warning is especially apt in the context of FISA and its recent amendments. Holmes appears primarily worried about executive branch behavior during a national security crisis, excessive executive discretion, and, perhaps above all, the corrosive effect of the power to "decide which information to reveal or conceal."[88] These concerns are well founded, and to illustrate the corrosive impact of secrecy within the executive branch, we can consider events around the Department of Justice's refusal to provide an immunity certification for certain NSA surveillance activities in March 2004.

FISA provides legal immunity to telecommunications providers upon receipt of a certification from the attorney teneral that "no warrant or court order is required by law, that all statutory certifications have been met, and that the specified assistance is required."[89] Upon concluding in March 2004 that certain NSA activity required a warrant under FISA, James Comey, the Acting Attorney General, refused to provide an immunity certification. The top leadership at the Department of Justice, including Comey, was ready to resign if the program continued. A dramatic confrontation then took place between White House advisors and Attorney General John Ashcroft, incapacitated in a hospital and recovering from gall bladder surgery.[90] White House Counsel Alberto Gonzales and White House advisor Andrew Card visited Ashcroft and attempted to obtain his signature on the immunity certification. Ashcroft refused to take this action. Here, the lack of knowledge of the NSA activities becomes especially detrimental; it is possible that some other NSA program, rather than the TSP, was involved at that time.

Most crucially, it is clear that the circles were drawn extremely narrowly within the Bush administration when it came to NSA surveillance. The hospital visit to Attorney General Ashcroft demonstrates this point. Notes taken by FBI Director Robert Mueller have Ashcroft informing Mueller that Ashcroft "was 'barred from obtaining the advice he needed on the program by the strict compartmentalization rules of the [White House.]'"[91] This is a chilling picture:

---

88. Holmes, *supra* note 1, at 321.

89. 18 U.S.C. § 2511(2)(a)(ii).

90. Dan Eggen, *White House Secrecy on Wiretaps Described*, WASH. POST, Oct. 3, 2007, at A5.

91. David Johnston & Scott Shane, *Notes Detail Pressure on Ashcroft Over Spying*, N.Y. TIMES, Aug. 17, 2007, at A14, *available at* http://www.nytimes.com/2007/08/17/washington/17inquire.html. Barton Gellman also details the battle that Ashcroft faced in 2004 in having his deputy, James Comey, "read" into, that is, granted access to information about, the NSA program. BARTON GELLMAN, ANGLER: THE CHENEY VICE PRESIDENCY 289-90 (2008). Ashcroft may have been referring to this conflict in the conversation with Mueller in the hospital. In January 2004, Jack Goldsmith, at the Department of Justice's Office of Legal Counsel, threatened the White House that Ashcroft might withhold certification for the NSA program if he could not have the advice of his deputy Comey. *Id.* at 290. Only then under the force of this pressure was Comey authorized to have knowledge about the NSA program. The Office of the Vice President had

the White House did not permit the attorney general to gain legal advice from the DOJ about government activity, the legality of which he was required under law to play a central role in overseeing. Moreover, according to Barton Gellman's account in his book, *Angler*, Vice President Cheney chose not to inform President Bush that top leadership at the Department of Justice, as well as the FBI Director, were about to resign en masse in protest over the NSA program.[92] Acting Attorney General Comey requested a personal meeting with President Bush to provide his resignation, and only at that point did the president discover the brewing insurrection and intercede to alter the NSA program in a fashion to satisfy the Justice Department's concerns.[93] These scenes from the Bush administration vividly illustrate Holmes's warnings regarding the corrosive impact of secrecy within the executive branch itself.

Yet, one must also consider shortcomings in other branches of government. Put simply, there is enough blame to go around regarding the culture of excessive secrecy in the U.S. government and the flaws in the law's deliberative and information structure for regulating foreign intelligence surveillance. For example, Congress has been consistently outflanked by the executive branch regarding access to critical information needed for its decision making. Courts, too, have been largely powerless to intervene.

It is striking how little Congress knew about the hidden aspects of NSA activity while enacting the PAA and FAA. Though the DOJ issued a white paper justifying these activities, it kept secret the official legal opinions that are said to declare the program lawful.[94] Jack Goldsmith, who was well-positioned in the Office of Legal Counsel to be privy to Bush administration actions, noted that the Vice President, his counsel, David Addington, "and other top officials . . . dealt with FISA the way they dealt with other laws they didn't like: they blew through them in secret based on flimsy legal opinions that they guarded closely so no one could question the legal basis for the operations."[95]

Congress legislated in this area without the extensive and careful hearings that preceded the initial enactment of FISA. The contrast with the detailed public hearings held by Senator Church and Representative Pike could not be clearer. To make matters worse, the telecommunications immunity provisions, discussed further *infra*, will make it difficult for ongoing litigation to cast light

provided the key opposition to this authorization for Comey. *Id.* at 289-90. The president's counterterrorism adviser also had no knowledge of the NSA program. *Id.* at 298.

92. GELLMAN, *supra* note 91, at 309-21. Gellman also states that the entire contested operation had been developed by Cheney's office and that it "is unlikely that the history of U.S. intelligence includes another operation conceived of and supervised by the office of the vice president." *Id.* at 282.

93. *Id.* at 309-21.

94. U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), *available at* http://www.usdoj.gov/opa/whitepaperonnsalegalauthorities.pdf.

95. JACK GOLDSMITH, THE TERROR PRESIDENCY 181 (2007).

on the behavior of the Bush administration. In voting against the FAA, Senator Russell Feingold stated:

> I sit on the Intelligence and Judiciary Committees, and I am one of the few members of this body who has been fully briefed on the warrantless wiretapping program. And, based on what I know, I can promise that if more information is declassified about the program in the future, as is likely to happen either due to the Inspector General report, the election of a new President, or simply the passage of time, members of this body will regret that we passed this legislation.[96]

Despite this strong warning, Congress went on to enact FAA. As Feingold also noted, approximately seventy members of the Senate voted without being briefed on the Bush administration's wiretapping program.[97]

Congress should have sought more information about the TSP before it amended FISA. Moreover, given media allegations of purely domestic NSA surveillance activities, Congress should have sought to gain a clear sense of how the FAA would extend to such surveillance.[98] Instead, it amended FISA without that knowledge. The resulting FAA also eases the requirement for telecommunications immunity, and thereby raises new barriers in the path of current litigation.[99] It will make it difficult for the public to use litigation to gain information about past, present or future behavior of the U.S. intelligence community.

There is also the unwillingness of Congress to play a decisive role in lifting the veil of secrecy. For much of this period, Republicans, the president's political party, controlled Congress, which made the legislative branch unlikely to oppose the executive branch in this area. But the matter improved only

---

96. Senator Russell Feingold, Remarks of U.S. Senator Russell Feingold in Opposition to the FISA Amendments Act (July 9, 2008), http://feingold.senate.gov/~feingold/statements/08/07/20080709.htm.

97. *Id.*

98. *See, e.g.*, Seymour M. Hersh, *Listening In*, NEW YORKER, May 29, 2006, at 26, *available at* http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh. For a concise summary of the "semi-known unknowns" about the NSA's domestic surveillance, see Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 305-08 (2008).

99. FISA had provided legal immunity to telecommunications companies upon receipt of a certification from the attorney general that "no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." This certification had not been received—and the FAA of 2008 gives a tip-off regarding the improvised, extra-legal solution. Recall that this statute gives immunity to telecommunications companies for the period from September 11, 2001 to January 17, 2007 if they provided assistance authorized by the president, designed to detect terrorism, and the subject of a written request by the attorney general or head of the intelligence community. There is no need here for certification by the attorney general that a warrant would not be required, and that all legal requirements have been met. Indeed, according to Burton Gellman's recent account in *Angler*, then White House Counsel Alberto Gonzales had provided a signature on an improvised document when Attorney General Ashcroft had refused to sign the standard FISA certification for the contested NSA program. GELLMAN, *supra* note 91, at 314-15.

slightly once Democrats gained control of the House and Senate in 2006. Part of the reason for the congressional hesitancy is political. As Samantha Power has noted, "national security is the one matter about which Republicans have maintained what political scientists call 'issue ownership.'"[100] Powers means that the public's trust on this policy has largely been given to the Republican party. This faith in the Republicans on this issue has meant that Democrats are often afraid of being labeled as "soft" on terrorism. A *New York Times* headline from August 2007 nicely captured the resulting policy landscape: "Wielding the Threat of Terrorism, Bush Outmaneuvers the Democrats."[101]

Yet, there may be underlying factors here beyond party politics and the specific identity of the party in the executive branch and/or Congress at any specific moment. Indeed, a relative weakness vis-à-vis the executive branch may also be shared by the courts. In a historical comparison of a contested electronic surveillance program authorized by Franklin Roosevelt during World War II with the Bush administration's NSA program, Neal Katyal and Richard Caplan argue: "The most striking fact from both the FDR and Bush administration electronic surveillance programs is that the courts and Congress were powerless to stop them."[102] Katyal and Caplan argue that Congress's institutional weakness in this regard stems from the president's veto power. Without a supermajority, vetoed legislation will not pass, and gaining these many votes against the wishes of the president is especially difficult in any area involving national security.

As for the courts, Katyal and Caplan view them as "almost non-actors in such events."[103] Because the burdens that a potential plaintiff must meet are too high, the judicial branch tends not to be active in cases involving national security and collection of foreign intelligence. Among the difficulties that plaintiffs face are the procedural hurdles concerning standing, the "political question" doctrine, general judicial deference for the executive branch in this area, and the state secrets privilege. I will discuss the state secrets privilege further in the next section. Thus far, the analysis suggests that when we think of the emergency room and the problem of the unchecked presidency, we must also think about institutional realities in other branches, and how these conditions can be improved.

C. Institutional Lessons

The story of FISA-amendment through 2008 is one of executive branch

100. Samantha Power, *The Democrats & National Security*, 55 N.Y. REV. BOOKS 66 (Aug. 14, 2008).

101. Jeff Rutenberg & Jeff Zeleney, *Wielding the Threat of Terrorism, Bush Outmaneuvers the Democrats*, N.Y. TIMES, Aug. 7, 2007, at A14.

102. Neal Katyal & Richard Caplan, *The Surprisingly Stronger Case for the Legality of the NSA Surveillance Program: The FDR Precedent*, 60 STAN. L. REV. 1023, 1070 (2008).

103. *Id.* at 1071.

lawbreaking, congressional legislating with incomplete knowledge, and the alteration of a carefully crafted legal approach. Holmes argues that "a well-designed national-security constitution will not assign purely discretionary decision-making power to the executive branch alone."[104] But what should the policy reaction be if Congress and courts are reluctant to take on an active role? The requirement is for policies and laws that create new deliberative structions and new information structures.

The institutional questions loom large, in my view, and steps are needed to improve the performance of all branches of the government. Here, I will only sketch some of the possibilities. Regarding the executive branch, as Katyal and Caplan have argued, for example, "[i]f we want to create the conditions for an executive that acts with greater fidelity to the law, greater attention to internal checks is likely to be necessary."[105] Part of these checks will come from greater information sharing among the branches. Here is a way of furthering public liberty—it will ensure that many participants in democratic rule will know about executive branch activities beyond "a closed circle of like-minded political appointees" (as Holmes puts it).[106]

In this light, the FAA takes modest steps in the right direction. We can consider, for example, its new requirements regarding reporting to Congress and inspector general audits. Every six months, the attorney general and the director of national intelligence (DNI) are to assess compliance with targeting and minimization procedures and to submit their report to the congressional committees with oversight responsibilities. In addition, the inspectors general of the DOJ and each relevant element of the intelligence community are to review: (1) the compliance with the adopted targeting and minimization procedures; (2) the number of disseminated intelligence reports that involved U.S. persons; and (3) the number of targets that were later determined to be located in the United States.

As promising as these opportunities are for congressional involvement, it is necessary to note a poor past track record for this branch of government in carrying out oversight in a far simpler and less controversial area of telecommunications surveillance. As I have discussed elsewhere, Congress has manifested a notable lack of interest in obtaining pen register reports from the Department of Justice as required by statute.[107] Pen registers are devices that record not the content of telephone conversations, but the telephone numbers of outgoing and incoming calls. The Patriot Act of 2001 amended the Pen Register Act to more broadly include "dialing, routing, addressing, or signaling information" ("DRAS information") in its definition of data that fall under the

104. Holmes, *supra* note 1, at 323.

105. Katyal & Caplan, *supra* note 102, at 1073.

106. Holmes, *supra* note 1, at 323.

107. Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 295-97 (2008).

statute.[108] IP addresses and email addressing data ("to" and "from" lines on email and routing) are an example of DRAS information.[109]

The lack of pen register reports leads to a significant gap in knowledge about law enforcement use of its authorities under the Pen Register Act, an essential part of the framework for domestic electronic surveillance in the United States. More broadly, much of the past congressional oversight of telecommunications surveillance law has represented a kind of "privacy theater."[110] By this term, I mean that the law creates rituals of behavior, such as a formal requirement that pen register reports be sent to Congress, and the payoff is the creation of a myth of oversight. It is likely, moreover, to be far more difficult for Congress to engage in effective engagement with executive branch behavior in the foreign intelligence area. There is also a real risk that the FAA's oversight requirements will simply contribute to a new kind of privacy theater and bolster the old, reassuring myth that if excesses exist, Congress will respond by enacting reforms.

Regarding the judiciary, an important step would be enactment of legislation to narrow the state secrets privilege. We have already discussed the new FAA provisions for retroactive telecommunications immunity, which make it more difficult for the public to gain information through litigation about the contested NSA warrantless wiretapping activities. The state secrets privilege is a common law evidentiary privilege that has been interpreted by courts in a fashion that adds additional difficulties for the use of litigation to expose governmental abuses in areas that involve national security. This rule will, in the future, add to the specific hurdle that plaintiffs face from the FAA's telecommunications immunity provision. The state secrets privilege already has proved to be a formidable difficulty for plaintiffs in litigation concerning the NSA's warrantless telecommunications surveillance.[111]

One of the most striking things about the state secrets privilege is that its modern form came from *United States v. Reynolds*,[112] a Cold War era case in which we now know the government lied to the Supreme Court about the necessity of secrecy. The *Reynolds* litigation concerned the crash of a B-29 military aircraft that killed members of its crew as well as three civilian observers on board the flight. Their widows sued the government under the

108. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act) of 2001, Pub. L. No. 107-56, 115 Stat. 272, § 216(a) (2001) (codified as amended at 18 U.S.C. § 3121(c) (2000 & Supp. 2001)).

109. Orin Kerr, *Internet Surveillance Law after the USA Patriot Act: The Big Brother that Isn't*, 97 NW. U. L. REV. 607, 636 (2003).

110. Schwartz, *supra* note 107, at 310-11.

111. *See, e.g.*, ACLU v. NSA, 493 F.3d 644 (6th Cir. 2006) (dismissing data mining claim due to state secrets claim); Terkel v. AT&T, 441 F. Supp. 2d 899 (N.D. Ill. 2006) (dismissing claim by AT&T subscribers that telephone records were illegally disclosed to NSA under state secrets privilege).

112. 345 U.S. 1 (1953).

Federal Tort Claims Act and sought discovery of the official accident investigation of the Air Force. The Supreme Court reversed the Third Circuit's decision and sustained the government's claim of privilege because it found a "reasonable danger that the accident investigation report would contain" state secrets.[113] The *Reynolds* Court drew on English precedents regarding crown privilege, and declared that it was appropriate to let the government use the privilege when "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged."[114] In 2000, the Air Force declassified the accident report at stake in *Reynolds*, and as William Weaver and Robert M. Pallitto concisely state, "[I]t contained no classified or national security information."[115] The *Reynolds* Court had not examined the documents itself, or sought to release the information to plaintiffs in redacted form; it had relied entirely on the government's assertion.

Courts continue to be reluctant to examine information about which the government has claimed the state secret privilege. Weaver and Pallitto note: "In less than one-third of reported cases in which the privilege has been invoked have the courts required *in camera* inspection of documents, and they have only required such inspection five times out of the twenty-three reported cases since the presidency of George H.W. Bush."[116] The tie between public and private liberty can be close in this context. As Holmes warns, "During the Bush Administration, the secrecy/privacy boundary migrated considerably, with privacy shrinking and secrecy expanding."[117] In the context of privacy litigation concerning the NSA surveillance, courts have used the state secrets privilege to expand government's ability to keep the public in the dark about invasions of its privacy.

Congress should act to narrow the state secrets privilege.[118] A bipartisan bill, introduced by Senator Edward Kennedy and co-sponsored by Senator

---

113. *Id.* at 10.

114. *Id.*

115. William G. Weaver & Robert M. Pallitto, *State Secrets and Executive Power*, 120 POL. SCI. Q. 85, 99 (2005). Upon reading the report, Judy Palya Loether, the daughter of one of the deceased plaintiffs, thought that the accident report revealed only "lots of negligence" on the part of the government. BARRY SIEGEL, CLAIM OF PRIVILEGE 211 (2008).

116. Weaver & Pallitto, *supra* note 115, at 101.

117. Holmes, *supra* note 1, at 327.

118. The privilege lacks a formal expression in any federal statute. Weaver and Pallitto observe:

> [O]ur own attempts to obtain policies governing assertion of the state secrets privilege met with failure, inasmuch as there appear to be no policy guidelines on the use of the privilege in any major department or agency of the executive branch. Freedom of Information Act requests to some three dozen agencies and their various subcomponents yielded nothing in the way of documentation of guidance for use of the privilege. Any limitations on assertion of the privilege appear to be self-imposed by the individual agencies, and use of the privilege seems to be carried out ad hoc at the discretion of the department heads and their assistants.

Weaver & Pallitto, *supra* note 115, at 111.

Arlen Specter would take a decisive step in this direction.[119] The bill would require the government to explain why it is invoking the privilege and to attempt to "craft a non-privileged substitute" for the privileged evidence.[120] This bill also takes important steps to structure how the judiciary reviews the government's claims. As an example, it contains this rule for determining the applicability of the privilege: "Evidence is subject to the state secrets privilege if it contains a state secret, or there is no possible means of effectively segregating it from other evidence that contains a state secret."[121]

These suggestions only touch the surface of the reforms that are needed. Let me conclude this Essay by pointing to three additional proposals. First, Anne Joseph O'Connell has made innovative suggestions for reforming the congressional oversight of intelligence agencies and how these agencies interact with each other.[122] In her view, there is a pressing need for finding an appropriate balance between unification and redundancy in congressional oversight committees and the intelligence agencies. She also calls for a variety of specific measures to allow policymakers in the executive branch and Congress to "more vigorously protect core democratic values."[123] Among the most promising of these suggestions are the revitalization of the Privacy and Civil Liberties Board in the executive branch, the need for subcommittees on civil liberties within intelligence-related committees, and amendment of intelligence oversight laws to provide greater notification of intelligence activities to members of Congress.[124]

Second, Katyal and Caplan have discussed reforms within individual intelligence agencies that would permit and even encourage government employees to dissent and warn of problematic actions.[125] Some of these reforms are borrowed from innovative approaches that the State Department long adopted for the foreign service. At the State Department, there is a "dissent channel" to allow members of the foreign service abroad to draw the attention of Washington officials to problematic policies based on their observations from their posting.[126] Katyal and Caplan also note, "[v]ibrant civil service protections are often necessary so employees feel they can do their job without reprisal."[127]

Finally, Jon Michaels has called for governmental operations with private

119. State Secrets Protection Act, S. 2533, 110th Cong. (2008).

120. *Id.*

121. *Id.*

122. Anne Joseph O'Connell, *The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World*, 94 CALIF. L. REV. 1655 (2006).

123. *Id.* at 1734.

124. *Id.*

125. Katyal & Caplan, *supra* note 102, at 1070-73.

126. *Id.* at 1073.

127. *Id.*

companies to be regulated according to the tenets of government contracting.[128] This area is important because of the ubiquity of government reliance on private companies in the twenty-first century, and the involvement of these organizations in sometimes dubious operations. This Essay has looked at one such area, namely the involvement of U.S. telecommunications companies in the NSA's warrantless wiretapping. Michaels proposes measures that include having corporations report any informal or formal agreement to share or transfer information about U.S. persons to military or intelligence operatives. These reports would be sent to the FISA Court and the members of the House and Senate intelligence committees.

In sum then, the NSA warrantless wiretapping and congressional response through FISA amendment raise a risk identified by Holmes, namely, an improper balance between the secrecy of government and the privacy of citizens. Holmes also points to the need, as noted above, to make choices among different aspects of security. These security-security tradeoffs require managing risk over time, and making complex choices between "security along one dimension for security along another."[129] Much about these surveillance activities remains secret, however, and for that reason it is difficult to assess the nature of the ensuing regulation, the FAA.

To be sure, some degree of secrecy was, is, and will be needed in this area. Yet, concerns about the merit of the ensuing legislation are inescapable. Consider merely the willingness of many members of Congress to legislate without making use of the briefings that were available to them, and the institutional weaknesses that Kaytal and Caplan identify. If we cannot even assess the governmental secrecy-personal privacy tradeoffs in the FAA, however, we cannot even begin to ponder the security-security tradeoffs made through this legislation. One danger is that the contested NSA program represents a Holmesian "labor-intensive and time-consuming needle-in-the-haystack fishing expedition[]."[130]

CONCLUSION

This Essay has used the Jorde Lecture by Stephen Holmes as a starting point for its examination of Congress's amendment of FISA against a background of warrantless surveillance by the NSA in violation of the law. Three themes of the lecture provide an ideal framework for this analysis: (1) the attitude of lawmakers to past wisdom as codified in legal frameworks; (2) the impact of secrecy on government behavior; and (3) institutional lessons.

When Congress amended FISA through the FAA, there were past lessons

128. Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CALIF. L. REV. 901 (2008).

129. Holmes, *supra* note 1, at 319.

130. *Id.* at 318.

available from the history of FISA, but they were complex and sometimes contradictory. There was no simple set of policy answers from which to resolve key issues, such as the need for a warrant requirement when data mining is used on communications flowing in and out of the United States. Technology also raises new challenges for which history can only provide partial answers.

As for the impact of secrecy, Congress legislated in this area without the kind of extensive hearings that preceded the initial enactment of FISA. Congress should have sought more information about the Bush administration's warrantless surveillance program before it amended FISA. This Essay also identified a number of political and institutional forces that have led to the relative weakness of Congress and the judicial branch vis-à-vis the executive branch in the area of national security. This Essay concluded by discussing new policies and laws capable of creating deliberative and information structures to help overcome the relative weaknesses of these two branches of government.

Public and private liberty represent different, albeit related, ways to bolster collective rationality. As Holmes observes, public liberty empowers citizens, who are to use this freedom to force government to justify its actions. Private liberty helps preserve public liberty, in my view, by ensuring that individual citizens have an underlying capacity for self-determination. As Holmes states, the "democratic character" of a society requires that its members not be "over-scrutinized."[131] In other words, information privacy is a critical component of private liberty. The resulting tradeoffs are difficult ones, and, as the Jorde Lecture demonstrates, the location of the security/privacy boundary in the United States will continue to be a critical issue.

131. *Id.* at 327.