

1-1-2007

The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act

Andrew Adler

Follow this and additional works at: <https://repository.law.miami.edu/umlr>



Part of the [Law Commons](#)

Recommended Citation

Andrew Adler, *The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act*, 61 U. Miami L. Rev. 393 (2007)

Available at: <https://repository.law.miami.edu/umlr/vol61/iss2/5>

This Note is brought to you for free and open access by the Journals at University of Miami School of Law Institutional Repository. It has been accepted for inclusion in University of Miami Law Review by an authorized editor of University of Miami School of Law Institutional Repository. For more information, please contact library@law.miami.edu.

NOTES

The Notice Problem, Unlawful Electronic Surveillance, and Civil Liability Under the Foreign Intelligence Surveillance Act

ANDREW ADLER*

I. INTRODUCTION	393
II. ORIGIN AND BASIC FRAMEWORK OF FISA	399
III. THE NOTICE PROBLEM	404
IV. ERRORS IN THE FISA PROCESS	408
A. <i>Application Process</i>	408
B. <i>Implementation Process</i>	412
1. INTERNAL FBI COMMUNICATIONS: APRIL 2000	412
2. SIMILAR ERRORS REVEALED FIVE YEARS LATER: SEPTEMBER 2005	415
V. RETURN AND NOTICE PROCEDURE	416
VI. REMEDY	426
A. <i>Enlarging the Scope of Civil Liability</i>	426
B. <i>Claims Procedure and Compliance with Due Process</i>	429
VII. CONCLUSION	437
A. <i>Specific Proposals of this Note</i>	437
B. <i>Informing the Broader Debate About Judicial Oversight</i>	439

I. INTRODUCTION

The nation awoke on December 16, 2005, to an article published in *The New York Times* which reported that, in 2002, President George W. Bush secretly authorized the National Security Agency (“NSA”) to conduct warrantless electronic surveillance of international communications involving those with links to al-Qaeda.¹ The NSA program sparked a number of notable events in 2006,² yet at the time of this writing more

* J.D. Candidate, University of Miami School of Law, 2007; B.A., Emory University, 2004. Many thanks are due to Professor Stephen Vladeck for helping me develop the topic of this Note and for guiding me through the writing process.

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

2. The most significant development of 2006 was the ruling of a federal district court declaring the NSA program unconstitutional. See *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006). In the preceding months, the Senate Judiciary Committee held numerous hearings on the legal issues surrounding the NSA program. See, e.g., *An Examination of the Call to Censure the President Before the S. Comm. on the Judiciary*, 109th Cong. (2006); *NSA III: War Time Executive Power and the FISA Court Before the S. Comm. on the Judiciary*, 109th Cong. (2006); *Wartime Executive Power and the National Security Agency's Surveillance Authority Before the S. Comm. on the Judiciary*, 109th Cong. (2006), available at http://www.senate.gov/committees/committee_109/judiciary/hearings/NSAIII/NSAIII%20Hearing%20Transcript.pdf.

than one year later, the law remains fundamentally unchanged.³

The principal law implicated by the revelation of the NSA program, the Foreign Intelligence Surveillance Act (FISA), is the “exclusive means” by which the executive branch may lawfully conduct foreign intelligence surveillance in this country.⁴ The future of this statutory warrant procedure, enacted nearly thirty years ago⁵ in response to the history of abuse committed by the executive branch in conducting war-

judiciary.senate.gov/hearing.cfm?id=1727 (testimony of Alberto Gonzales, Attorney General). The Senate Select Committee on Intelligence declined to investigate the breadth and scope of the NSA program. See Walter Pincus, *Senate Panel Blocks Eavesdropping Probe*, WASH. POST, Mar. 8, 2006, at A03, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/03/07/AR2006030701549.html>. The majority of the provisions of the Patriot Act that were due to sunset were renewed in March 2006. See USA Patriot Act Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192 (codified as amended in scattered sections and titles of the U.S.C.A.). Also in March, Senator Russell Feingold introduced a resolution calling for the censure of President Bush for authorizing the NSA program. See S. Res. 398, 109th Cong. (2006), available at <http://thomas.loc.gov/cgi-bin/query/z?c109:S.RES.398> (text of censure resolution); Ed O’Keefe, *Feingold Calls for Bush’s Censure*, ABC News, Mar. 12, 2006, <http://abcnews.go.com/ThisWeek/Politics/story?id=1715495&page=1>.

3. It is worth noting that FISA was amended on March 9, 2006, when Congress renewed the majority of the expiring provisions of the Patriot Act (which itself amended FISA in 2001), but this did not acknowledge, relate, or respond to the revelation of the NSA program three months earlier. See USA Patriot Act Improvement and Reauthorization Act of 2005, *supra* note 2. Interestingly, few pointed out the contradiction in the administration’s position as it applauded the renewal of major provisions of FISA while simultaneously flouting that same law with its defense of the NSA program. See *infra* note 7 and accompanying text; Statement of President George W. Bush on Passage of Bill to Reauthorize the USA PATRIOT Act (Mar. 9, 2006), <http://www.lifeandliberty.gov/index.html> (“I applaud the Senate for voting to renew the Patriot Act and overcoming the partisan attempts to block its passage. . . . The Patriot Act is vital to the war on terror and defending our citizens against a ruthless enemy.”); Letter from Alberto Gonzales, Attorney General, to William H. Frist, Majority Leader, United States Senate, Legal Authorities Supporting the Activities of the National Security Agency Described by the President (Jan. 19, 2006), available at <http://permanent.access.gpo.gov/lps66493/White%20Paper%20on%20NSA%20Legal%20Authorities.pdf> (defending the legality of the NSA program on statutory and constitutional grounds); Posting of Anonymous Liberal to Unclaimed Territory, http://glenngreenwald.blogspot.com/2006_03_01_glenngreenwald_archive.html (Mar. 10, 2006 09:15 EST) (“On Thursday the President once again signed into law a statute - the Patriot Act renewal - which amends the Foreign Intelligence Surveillance Act (FISA). The Patriot Act made many significant changes to FISA – changes which were made permanent by this bill – but there is one crucial provision that has not changed; FISA still clearly states that its procedures ‘shall be the exclusive means by which electronic surveillance . . . may be conducted.’ *In other words, the President has once again reaffirmed the validity of a law which expressly criminalizes the type of warrantless surveillance which his administration has been conducting for four and a half years.*” (emphasis added)). Indeed, certain provisions of the Act actually strengthened judicial review of the executive’s surveillance authority. See, e.g., USA Patriot Improvement and Reauthorization Act of 2005, *supra* note 2, § 106 (strengthening judicial review over the government’s ability to access certain business records under section 215 of the Patriot Act); *id.* § 108 (strengthening judicial review over the government’s roving wiretap authority under section 206 of the Patriot Act).

4. 18 U.S.C. § 2511(2)(f) (Supp. I 2002).

5. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C.A. §§ 1801-1862 (West 2006)).

rantless wiretapping,⁶ was called into severe doubt by the NSA program. This was so because the NSA program was fundamentally inconsistent with the core requirement of FISA, namely that an Article III court authorize foreign intelligence surveillance.⁷

At the time of this writing, however, it appears that this tension may now be resolved, as the Bush administration has suddenly and remarkably reversed its position by agreeing to subject the NSA program to court supervision.⁸ On January 17, 2007, Attorney General Alberto Gonzales informed the Senate Judiciary Committee that an Article III judge issued orders one week earlier authorizing the surveillance previously conducted under the NSA program.⁹ The key point here is the sudden and wholesale reversal by the administration to accept judicial oversight of its surveillance activities.¹⁰ If the administration's intentions expressed in the Attorney General's letter are indeed sincere,¹¹ then the situation should revert back to the status quo – to over

6. See *infra* notes 32-33 and accompanying text.

7. There are two notable exceptions to the requirement of advanced court authorization under FISA. See 50 U.S.C. § 1802 (2000); 50 U.S.C. § 1805(f) (Supp. I 2002). Section 1805(f) is discussed in Part II.

8. Eric Lichtblau & David Johnston, *Court to Oversee U.S. Wiretapping in Terror Cases*, N.Y. TIMES, Jan. 18, 2007.

9. Letter from Alberto Gonzales, Attorney General, to Patrick Leahy, Chairman, Senate Judiciary Committee, and Arlen Specter, Ranking Minority Member, Senate Judiciary Committee (Jan. 17, 2007), <http://www.talkingpointsmemo.com/docs/nsa-doj-surveillance/?resultpage=2&t>. At this time, there is no information available regarding the content of these orders, and it is unclear exactly how the NSA program will be subsumed under the FISA framework. See Lichtblau & Johnston, *supra* note 8.

10. See Lara Jakes Jordan, *Secret Court to Govern Wiretapping Plan*, ASSOCIATED PRESS, Jan. 17, 2007, available at http://news.yahoo.com/s/ap/20070117/ap_on_go_ca_st_pe/domestic_spying ("The turnaround [comes] after more than a year of stubborn insistence by the White House that oversight by the secret court was not required by law and, in fact, would be a hindrance to stopping terrorists.").

11. See Posting of Glenn Greenwald to Unclaimed Territory, <http://glenngreenwald.blogspot.com/> (Jan. 17, 2007, 20:02 EST) ("There is no repentance here, nor (more importantly) is there any rescission of their claimed powers of lawbreaking. Quite the contrary. Gonzales' letter affirms, as one would expect, their belief that they were legally entitled to violate this law. That means (a) that they can violate it again at any future point when they want to, (b) they can violate other laws under the same theories, and (c) whatever other lawbreaking is already occurring as a result of those theories is not going to stop."). It has been suggested that the administration's decision to submit the NSA program to court supervision is designed to both pre-empt upcoming congressional investigations by the new Democratic majority and moot an appeal pending in the Sixth Circuit Court of Appeals of a district court's decision holding the NSA program unconstitutional. Lichtblau & Johnston, *supra* note 8; see *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006); Posting of Glenn Greenwald to Unclaimed Territory, *supra* ("Every time [the Bush administration] is about to face consequences for their conduct, they stop doing what they are doing and find another way. When the Supreme Court was about to rule on the legality of their detention of Jose Padilla, they transferred him to a criminal court and finally charged him, then told the [C]ourt that the questions were 'moot.' When the Supreme Court in *Hamdan* ordered them to give Hamdan (a U.S. citizen) a venue to charge him with a crime and prove his guilt, they simply let This Extremely Dangerous Terrorist go free instead of charging him. . . .

five years ago, before the NSA program was authorized – with FISA undoubtedly representing the exclusive means by which the executive branch may conduct foreign intelligence electronic surveillance within this country.¹²

But throughout 2006, there was a serious push by the administration and many in Congress for a warrantless electronic surveillance regime not subject to any judicial review at all.¹³ While that push appears for the moment not to have outlived the November 2006 midterm elections (where the Democrats regained both houses of Congress), this Note nonetheless seizes on this element of disagreement regarding the role of the judiciary in foreign intelligence electronic sur-

They have not conceded anything and they have certainly not done anything which mitigates their lawbreaking – their crimes – over the past five years with regard to eavesdropping without warrants.”).

12. Of course, should the executive branch renew the NSA program in the future or authorize a similar warrantless wiretapping program, this status quo would again be disrupted. *See id.*; *infra* note 13.

In light of this lingering uncertainty surrounding FISA at the time of this writing, the author feels compelled to point out the enduring value of this Note in the drastic event that FISA is eliminated or rendered optional. This is the first Note to document the errors in the FISA process and examine the issue of civil liability in the foreign intelligence electronic surveillance context since the enactment of FISA. For these reasons, this Note should continue to inform the broader, long-term debate regarding judicial participation in the foreign intelligence surveillance process.

13. Prior to the November 2006 midterm elections and the Attorney General’s January 17 letter, there were at least five proposed bills (representing two distinct camps) that sought to resolve the tension between the NSA program and FISA. *See* Electronic Surveillance Modernization Act, H.R. 5825, 109th Cong. (2006), *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=109_cong_bills&docid=f:h5825ih.txt.pdf (Wilson); Foreign Intelligence Surveillance and Improvement Act of 2006, S. 3001, 109th Cong., *available at* <http://ryansingel.tripod.com/documents/2006/feinsteinspectorbill.pdf> (Specter-Feinstein); Lawful Intelligence and Surveillance of Terrorists Act in an Emergency Act by NSA (LISTEN), H.R. 5371, 109th Cong. (2006), *available at* http://www.fas.org/irp/congress/2006_cr/hr5371.pdf#search=%22%22HR%205371%22%22 (Harman); National Security Surveillance Act of 2006, S. 2453 109th Cong., *available at* http://www.fas.org/irp/congress/2006_cr/s2453.html (Specter); Terrorist Surveillance Act of 2006, S. 2455, 109th Cong., *available at* <http://www.scotusblog.com/movabletype/archives/DeWinebill.pdf> (DeWine). One camp, led by Senator and then-Chairman of the Senate Judiciary Committee Arlen Specter proposed repealing the “exclusive means” language of FISA, thus eviscerating it by making its requirements entirely optional. *See* National Security Surveillance Act of 2006, *supra*, § 801; Posting of Just an Observer to <http://www.haloscan.com/comments/glenngreenwald/115757928072604291/#23140> (Sept. 6, 2006 11:40 EST) (“The current Specter bill in the Senate, S 2453, as amended in committee [would] repeal the core requirement of FISA that its procedures and the criminal Wiretap Act (Title III) ‘shall be the exclusive [sic] means’ for conducting electronic surveillance. The bill essentially makes FISA optional overall, by explicitly deferring to the President’s ‘inherent’ constitutional authority instead.”). This would have essentially permitted the warrantless wiretapping that Congress expressly outlawed nearly thirty years ago. The other camp sought to reaffirm the exclusivity of FISA by making it clear (if it was not already) that warrantless wiretapping outside the bounds of FISA was prohibited. *See, e.g.*, Foreign Intelligence Surveillance and Improvement Act of 2006, *supra*, §§ 101-02. The central disagreement therefore was between those who sought to maintain judicial involvement in the process and those who wanted to remove the courts from the process altogether in order to ease the government’s task of fighting the War on Terror.

veillance. It does not do this by discussing the weighty constitutional issues pertaining to executive power so clearly implicated by the NSA program.¹⁴ Instead, this Note takes a different route by exposing actual errors in the FISA process as it has operated over the last five years; it does so not to argue that FISA should be eliminated but rather to support the proposition that the degree of judicial participation inherent in the FISA process must be *strengthened*. Understanding the nature of the errors occurring in the FISA process provides insight into how the foreign intelligence electronic surveillance process can be improved.

This Note therefore illuminates the broader issue of judicial participation by examining a narrower issue that has literally gone unnoticed for the last thirty years: whether it is possible to compensate individuals who have been victims of unlawful electronic surveillance under FISA.¹⁵ By focusing on the individuals affected in the process, the narrower issue of civil liability under FISA provides an appropriate lens through which one can then better examine the broader issue of judicial participation in the foreign intelligence surveillance process.

The concept of civil liability under FISA cannot be so easily dismissed, as FISA itself expressly contemplates such relief.¹⁶ Indeed, 50 U.S.C. § 1810 provides for a civil cause of action for damages against federal officials.¹⁷ This provision has laid dormant for nearly thirty years not because there have been no errors in the FISA process,¹⁸ but

14. See generally CONG. RES. SERV., PRESIDENTIAL AUTHORITY TO CONDUCT WARRANTLESS ELECTRONIC SURVEILLANCE TO GATHER FOREIGN INTELLIGENCE INFORMATION (Jan. 5, 2006), available at <http://www.fas.org/sgp/crs/intel/m010506.pdf> (analyzing the central statutory and constitutional issues regarding the NSA program); U.S. DEP'T OF JUSTICE, LEGAL AUTHORITIES SUPPORTING THE ACTIVITIES OF THE NATIONAL SECURITY AGENCY DESCRIBED BY THE PRESIDENT (2006), <http://www.fas.org/irp/nsa/doj011906.pdf> (defending the legality of the NSA program on statutory and constitutional grounds); Letter from Alberto Gonzales, Attorney General, to William H. Frist, Majority Leader, United States Senate (Jan. 19, 2006), <http://www.fas.org/irp/nsa/doj011906.pdf> (same); Letter from Constitutional Law Scholars and Former Government Officials, to Members of Congress (Jan. 9, 2006), <http://www.fas.org/irp/agency/doj/fisa/doj-response.pdf> (arguing that the NSA program violates FISA and the separation of powers and, if upheld, would raise serious constitutional questions under the Fourth Amendment); see also *ACLU v. NSA*, 438 F. Supp. 2d 754 (E.D. Mich. 2006) (holding that the NSA program violates the First and Fourth Amendments and the separation of powers).

15. The term "unlawful" used throughout is meant to describe electronic surveillance that violates the statute. This not only includes violations of concrete statutory provisions but violations of core structural requirements as well. For example, no provision in FISA requires that the facts presented in an application to the court be accurate, but such a requirement is necessarily compelled by the structure of FISA. See *infra* Part III.A. In addition, although there is no statutory requirement that the electronic surveillance conducted conform to the surveillance authorized by the court order, such a requirement is necessarily compelled by the statute. See *infra* Part III.B.

16. See 50 U.S.C. § 1810 (2000).

17. *Id.*; see *infra* Parts II & V.A.

18. See *infra* Part III

rather because the victims of these errors have had no way of discovering that they were subject to unlawful electronic surveillance.¹⁹

This notice problem is perhaps best illustrated by the Brandon Mayfield incident. During the investigation of the Madrid train bombings that killed hundreds of people on March 11, 2004, a set of fingerprints was lifted off of a plastic bag of detonators found at the site.²⁰ The FBI matched these prints to Brandon Mayfield, an attorney and Muslim-convert living in Portland, Oregon. Mayfield was then the target of extensive electronic surveillance and physical searches under FISA²¹ that culminated in his arrest and two week detention.²² The FBI "copied four computer hard drives, digitally photographed several documents, seized ten DNA samples and took approximately 335 digital photographs of the residence and Mr. Mayfield's property."²³ When the Spanish authorities notified the FBI that its fingerprint analysis was erroneous, Mayfield was released with an apology from the FBI.²⁴

This incident, like the violations described in Part III, illustrates that the government's surveillance powers, even under FISA, are susceptible to error. One can only imagine the dramatic increase in violations that would occur under a regime like the NSA program, where the executive branch has the ability to conduct electronic surveillance free from judicial scrutiny.

19. See *infra* Part II.

20. *Reauthorization of the USA Patriot Act Before the H. Permanent Select Comm. on Intelligence*, 108th Cong. 18 (2005), available at <http://intelligence.house.gov/Media/PDFS/EdgarTestimony.pdf> (statement of Tim Edgar, National Security Policy Counsel, American Civil Liberties Union).

21. See OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE 2 (Jan. 2006), available at <http://www.usdoj.gov/oig/special/s0601/final.pdf> [hereinafter A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE] ("As part of the investigation, the FBI obtained authority to conduct covert electronic surveillance and physical searches of Mayfield pursuant to the Foreign Intelligence Surveillance Act of 1978 (FISA)."). Although the details of the electronic surveillance were not disclosed, it is likely that the government used the full extent of its broad electronic surveillance powers. See *In re All Matters*, 218 F. Supp. 2d 611, 616-17 (FISA Ct. 2002) ("[I]n many U.S. person electronic surveillances the FBI will be authorized to conduct, simultaneously, telephone, microphone, cell phone, e-mail and computer surveillance of the U.S. person target's home, workplace, and vehicles.").

22. *Reauthorization of the USA Patriot Act Before the H. Permanent Select Comm. on Intelligence*, *supra* note 20. See A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE, *supra* note 21, at 20 (finding no violation of the material witness statute that provided the basis for Mayfield's detention); but see HUMAN RIGHTS WATCH, MISUSE OF THE MATERIAL WITNESS LAW TO HOLD SUSPECTS AS WITNESSES (June 2005), http://hrw.org/reports/2005/us0605/5.htm#_ftn53 (criticizing, using the Mayfield case as one example, the government's use of the material witness statute to detain suspected terrorists following September 11, 2001).

23. *Reauthorization of the USA Patriot Act Before the H. Permanent Select Comm. on Intelligence*, *supra* note 20.

24. See Press Release, Federal Bureau of Investigation, Statement on Brandon Mayfield Case (May 24, 2004), available at <http://www.fbi.gov/pressrel/pressrel04/mayfield052404.htm>.

Furthermore, the Mayfield incident demonstrates that the only way that these errors will be brought to light is if the government makes an arrest. The reason that the Mayfield incident has been perceived as anomalous is because it is the only known case where the FBI, after conducting extensive surveillance of the target, was still convinced that a completely innocent man was a terrorist. As a result, they arrested him and revealed the existence of the surveillance. Had the FBI discovered that the fingerprint analysis was erroneous *prior* to arresting Mayfield, he simply never would have discovered that he had been the target of such surveillance. This Note focuses on those individuals who, like Brandon Mayfield, are subject to unlawful electronic surveillance under FISA, but who, unlike Mayfield, will not discover that it ever took place.

I propose the adoption of a statutory remedial scheme designed to provide compensation to individuals subject to the most grievous instances of unlawful electronic surveillance. This scheme has two components. The first component, outlined in Part IV, proposes a return and notice procedure that allows the court responsible for authorizing the FISA surveillance to screen for these violations and discretionarily notify an individual subject to such surveillance. The second component, outlined in Part V, establishes a claims procedure, governed by the same court, designed to affirmatively compensate these individuals in a manner consistent with both due process and national security concerns.

These proposals calling for the increased involvement of the judiciary in the foreign intelligence surveillance process illustrate not only that the courts, as a practical matter, have an invaluable role to play in preventing and monitoring the executive's surveillance powers, but also that they may be put to use in new and creative ways to fulfill their historic role of safeguarding individual liberties. If the courts are removed from the equation, these dual objectives become impossible to achieve.

II. ORIGIN AND BASIC FRAMEWORK OF FISA

FISA was enacted in 1978²⁵ to regulate electronic surveillance²⁶

25. Foreign Intelligence Surveillance Act (FISA) of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C.A. §§ 1801-1862 (West 2006)).

26. Electronic surveillance is defined as:

1) [T]he acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes; 2) the acquisition by an

used to gather foreign intelligence information.²⁷ FISA sought to strike a "fair and just balance between protection of national security and protection of personal liberties."²⁸ It is largely modeled after Title III of the Omnibus Crime Control and Safe Streets Act of 1968 that regulates electronic surveillance in the criminal context.²⁹ Title III was enacted in response to a pair of Supreme Court cases the prior year that recognized electronic surveillance as a search within the meaning of the Fourth Amendment³⁰ and required wiretapping statutes to comply with Fourth Amendment requirements.³¹

The passage of FISA was motivated by the extensive findings of the Church Committee in 1976.³² The Church Committee concluded that the absence of regulation allowed every president since President Franklin Delano Roosevelt to engage in unbridled electronic surveillance for national security purposes, thus trampling on the rights of

electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include the acquisition of those communications of computer trespassers that would be permissible under section 2511 (2)(i) of title 18, United States Code; 3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or 4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes.

50 U.S.C. § 1801(f) (Supp. I 2002).

27. Foreign intelligence information is defined as:

1) [I]nformation that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against: a) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; b) sabotage or international terrorism by a foreign power or an agent of a foreign power; or c) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or 2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to: a) the national defense or the security of the United States; or b) the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e) (2000).

28. S. REP. NO. 95-604, pt. 1, at 7 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3908.

29. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, tit. III, 82 Stat. 197, 211 (current version at 18 U.S.C.A. §§ 2510-2522 (West 2006)).

30. *See Katz v. United States*, 389 U.S. 347 (1967).

31. *See Berger v. New York*, 388 U.S. 41 (1967).

32. STAFF REPORT OF THE SENATE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, 94TH CONG., BOOK II: INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS (1976), *available at* <http://www.aarclibrary.org/publib/church/reports/book2/contents.htm>.

American citizens and organizations in the process.³³ FISA sought to “relegate to the past the wire-tapping abuses brought to light during the [Church] Committee hearings by providing, for the first time, effective substantive and procedural statutory controls over foreign intelligence electronic surveillance.”³⁴ In doing so, Congress invoked the Supreme Court’s seminal opinion in *United States v. United States District Court*, better known as the *Keith* case, as the basis for crafting a new statute that would govern electronic surveillance outside the criminal context.³⁵ In a much quoted passage, the Court in *Keith* stated:

Moreover, we do not hold that the same type of standards and procedures prescribed by Title III are necessarily applicable to this case. . . . Given these potential distinctions between Title III criminal surveillances and those involving domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III. Different standards may be compatible with the Fourth Amendment if they are reasonable both in relation to the legitimate need of government for intelligence information and the protected rights of our citizens. For the warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection.³⁶

FISA established its own secret Article III court called the Foreign Intelligence Surveillance Court (“FISC”) that is currently composed of eleven district court judges selected by the Chief Justice of the Supreme Court.³⁷ The FISC sits “in a locked, windowless room with walls of corrugated steel, in a restricted area of a Justice Department building in Washington.”³⁸ It reviews applications *ex parte*, submitted by the Department of Justice to conduct foreign intelligence surveillance against foreign powers and agents of a foreign power.³⁹ FISA also created a Foreign Intelligence Surveillance Court of Review, composed of three district or circuit court judges selected by the Chief Justice, to review, also *ex parte*, the denial of applications submitted to the FISC.⁴⁰ FISA has more recently been amended to provide authority for physical

33. *Id.*

34. S. REP. NO. 95-604, pt. 1, at 15 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3917.

35. *Id.* at 13-14, *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3914-16.

36. *United States v. United States District Court*, 407 U.S. 297, 322-23 (1972). Although *Keith* expressly limited its holding to domestic security intelligence, this case was cited as the authority to enact such a statute in the foreign intelligence context. *See* S. REP. NO. 95-604, pt. 1, at 13-15 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3914-17.

37. 50 U.S.C. § 1803(a) (Supp. I 2002).

38. Nola Breglio, *Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance*, 113 YALE L.J. 179 (2003).

39. *See infra* notes 47-48.

40. 50 U.S.C. § 1803(b) (2000).

searches,⁴¹ pen registers and trap and trace devices,⁴² and access to certain business records.⁴³

Applications submitted to the FISC for electronic surveillance must meet several requirements. All applications must be approved by the Attorney General⁴⁴ and certified by an executive official with national security responsibilities.⁴⁵ The central standard for approving applications is that the FISC must find probable cause⁴⁶ to believe that the target of the surveillance is a foreign power⁴⁷ or an agent of a foreign

41. Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, tit. VIII, 108 Stat. 3423, 3443 (current version at 50 U.S.C.A. §§ 1821-1829 (West 2006)).

42. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, Pub. L. No. 107-56, § 214, 115 Stat. 272, 286-87 (codified at 50 U.S.C. §§ 1841-1846 (Supp. I 2002)), *amended by* USA Patriot Improvement and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 228-29, § 128 (2006).

43. USA PATRIOT Act of 2001, § 215, 115 Stat. 272, 287-88 (codified at 50 U.S.C. §§ 1861-62 (Supp. I 2002)) (amended 2006).

44. 50 U.S.C. § 1804(a) (Supp. I 2002) (amended 2006).

45. *Id.* § 1804(a)(7).

46. *See* *Illinois v. Gates*, 462 U.S. 213, 238 (1983) ("The task of the issuing magistrate is simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit before him, . . . there is a fair probability that contraband or evidence of a crime will be found in a particular place."); *Brinegar v. United States*, 338 U.S. 160, 175 (1949) ("In dealing with probable cause, . . . as the very name implies, we deal with probabilities. These are not technical; they are the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.").

47. Foreign power is defined as:

1) [A] foreign government or any component thereof, whether or not recognized by the United States; 2) a faction of a foreign nation or nations, not substantially composed of United States persons; 3) an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments; 4) a group engaged in international terrorism or activities in preparation therefore; 5) a foreign-political organization, not substantially composed of United States persons; or 6) an entity that is directed and controlled by a foreign government or governments.

50 U.S.C. § 1801(a) (2000).

power⁴⁸ as defined in the statute.⁴⁹ The application must also contain the proposed minimization procedures to be used during the surveillance that must meet the statutory definition of such procedures.⁵⁰ The executive official submitting the application must also certify “that the purpose of the surveillance is to obtain foreign intelligence information”⁵¹ and “that such information cannot reasonably be obtained by normal investigative techniques.”⁵² The FISC will issue the order if it finds that the above core requirements and all other statutory requirements are met. The order for electronic surveillance will last “for the period necessary to achieve its purpose, or for ninety days, whichever is less”⁵³ and “extensions of an order . . . may be granted on the same basis as an original order”⁵⁴

FISA also imposes reporting requirements on the executive

48. Agent of a foreign power is defined as:

1) any person other than a United States person, who: A) acts in the United States as an officer or employee of a foreign power, or as a member of a foreign power as defined in subsection (a)(4) of this section; B) acts for or on behalf of a foreign power which engages in clandestine intelligence activities in the United States contrary to the interests of the United States, when the circumstances of such person's presence in the United States indicate that such person may engage in such activities in the United States, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or 2) any person who: A) knowingly engages in clandestine intelligence gathering activities for or on behalf of a foreign power, which activities involve or may involve a violation of the criminal statutes of the United States; B) pursuant to the direction of an intelligence service or network of a foreign power, knowingly engages in any other clandestine intelligence activities for or on behalf of a such foreign power, which activities involve or are about to involve a violation of the criminal statutes of the United States; C) knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power; D) knowingly enters the United States under a false or fraudulent identity for or on behalf of a foreign power or, while in the United States, knowingly assumes a false or fraudulent identity for or on behalf of a foreign power; or E) knowingly aids or abets any person in the conduct of activities described in subparagraph (A), (B), or (C) or knowingly conspires with any person to engage in activities described in subparagraph (A), (B), or (C).

Id. § 1801(b).

49. This standard has generally been recognized as more lenient than the traditional probable cause standard that the target is or is about to commit a crime. *See* S. REP. NO. 95-701, at 12 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3973, 3980 (“The international character of foreign terrorist activities fully supports the more flexible probable cause standard . . .”).

50. § 1804(a)(5); *see id.* § 1801(h); *infra* Parts III.A. & IV.

51. 50 U.S.C. § 1804(a)(7)(b) (Supp. I 2002); *see infra* note 64 and accompanying text.

52. 50 U.S.C. § 1804(a)(7)(c) (2000).

53. 50 U.S.C.A. § 1805(e)(1) (West 2006). When the target is a foreign power, the order may last for one year. *Id.* § 1805(e)(2). Some orders against agents of foreign powers may last up to 120 days. *See id.* § 1805(e)(1)(B).

54. *Id.* § 1805(e)(2). There is an exception for the targets described *supra* note 53, where extensions may be granted for up to one year. *Id.*

branch.⁵⁵ Each year, the Attorney General must inform Congress of “the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter; and the total number of such orders and extensions either granted, modified, or denied.”⁵⁶ The Attorney General is also required, on a semi-annual basis, to “fully inform” the Select Committees on Intelligence in the House of Representatives and the Senate on the criminal cases in which information gathered has been shared and authorized for use at trial.⁵⁷

III. THE NOTICE PROBLEM

As mentioned at the outset, FISA provides for a civil cause of action for damages against federal officials.⁵⁸ Unlike many civil actions that may simply be invoked by a plaintiff whenever the proper conditions permit, the cause of action in section 1810 requires implementing legislation. Because those subject to unlawful electronic surveillance will never discover that they are under surveillance, they are incapable of bringing the action even when circumstances would allow. When enacting Title III, Congress recognized this need for implementing legislation by crafting a general notice provision in order to make the analogous Title III cause of action meaningful.⁵⁹ “It is expected that civil suits, if any, will instead grow out of the filing of [notice] inventories under section 2518(8)(d).”⁶⁰ By contrast, FISA provides for notice only in narrow circumstances that are incapable of effectuating the statutory cause of action in section 1810.

First, FISA provides for notice of the fact that electronic surveillance has occurred when the government intends to introduce the fruits of that surveillance in a federal or state criminal proceeding.⁶¹ Those who receive such notice have a statutory suppression remedy and may challenge the legality of the FISA surveillance before a judge.⁶²

FISA differs from Title III, however, in that FISA was designed as

55. *Id.* §§ 1807-1808.

56. 50 U.S.C. § 1807 (2000).

57. 50 U.S.C.A. § 1808(a) (West 2006).

58. 50 U.S.C. § 1810 (2000).

59. *See* 18 U.S.C. § 2518(8)(d) (2000) (notice provision); 18 U.S.C. § 2520 (2000) (providing for recovery of civil damages).

60. S. REP. NO. 90-1097, at 2196 (1968).

61. 50 U.S.C. § 1806(c)-(d) (2000).

62. The court will suppress such evidence if it is “unlawfully acquired” or if the “surveillance was not made in conformity with an order of authorization or approval.” *Id.* § 1806(e). If the Attorney General files an affidavit swearing that disclosure of the order or any contents of the surveillance to the defendant would harm national security, the judge will review the legality of the surveillance in camera and ex parte. *Id.* § 1806(f).

a tool for gathering foreign intelligence as opposed to incriminating evidence:

Although there may be cases in which information acquired from a foreign intelligence surveillance will be used as evidence of a crime, these cases are expected to be relatively few in number, unlike Title III interceptions the very purpose of which is to obtain evidence of criminal activity.⁶³

Although the Patriot Act's amendments to FISA now allow the government's primary purpose to be gathering incriminating evidence⁶⁴ and permit increased coordination between intelligence officers and law enforcement,⁶⁵ it is still often unwise to prosecute an agent of a foreign power who is successfully being monitored under FISA:

And there are costs associated with the prosecution of somebody using FISA information. *Chief among them, you have to reveal publicly the fact that there has been FISA surveillance*, and that if there are others out there who are not being prosecuted, they are then alerted to the fact that the Government is on to the conspiracy. . . . [A]nd there are also other concerns that arise when you prosecute an intelligence case involving protection of source and method information, and a variety of other concerns. And just as a tactical matter, sometimes prosecution is not the right way to go. Other times you just want to monitor these people or do something else. You try to recruit one of them as a double agent. You feed them false information. You disrupt them using some other technique. In some cases you do want to prosecute.⁶⁶

In addition, since September 11, 2001, the FBI has undergone a broad transformation aimed at focusing the agency on terrorism and intelligence-related matters. . . . [OIG has] found that the FBI's investigative efforts [have been] generally consistent with its post-9/11 priorities and that the FBI [is] performing less work in certain traditional criminal investigative areas and more work in matters related to terrorism.⁶⁷

63. S. REP. NO. 95-604, pt. 1, at 39 (1978), as reprinted in 1978 U.S.C.C.A.N. 3904, 3940.

64. The Foreign Intelligence Surveillance Court of Review interpreted section 218 of the Patriot Act in *In re Sealed Case*, 310 F.3d 717, 735-36 (FISA Ct. Rev. 2002), to allow the government's primary purpose, when conducting electronic surveillance under FISA, to be gathering evidence of a crime as long as gathering foreign intelligence information was still a significant purpose. See 50 U.S.C. § 1804(a)(7)(B) (Supp. I 2002) ("a certification . . . that a significant purpose of the surveillance is to obtain foreign intelligence information").

65. See 50 U.S.C. § 403-5d (Supp. I 2002).

66. *The USA Patriot Act in Practice: Shedding Light on the FISA Process Before the S. Comm. on the Judiciary*, 107th Cong. (2002), http://www.fas.org/irp/congress/2002_hr/091002transcript.html (statement of David Kris, Associate Deputy Attorney General, U.S. Department of Justice) (emphasis added).

67. OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, AUDIT REPORT NO. 05-37,

This reprioritization has led to a significant reduction in the number of criminal investigations and prosecutions initiated. OIG found that the FBI opened 28,331 fewer criminal cases in fiscal year (FY) 2004 than it had in FY 2000, a 45-percent reduction. During FY 2000, the FBI initiated 67,782 criminal investigations, while in FY 2004 the number of investigations declined to 34,451.⁶⁸

These strategic concerns and reprioritization efforts supplement the conclusion that, absent another Brandon Mayfield incident, this notice provision will never be triggered in situations where innocent individuals have been subject to unlawful electronic surveillance. These individuals will not face criminal prosecution necessary to trigger the notice provision and will therefore never become aware that they have been subject to surveillance.

FISA also contains a notice provision in its subchapter governing physical searches which provides that:

[A]t any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search.⁶⁹

When the government takes the position, as it did in the Mayfield case, that a "mistake does not mean the government should be required to disclose its spying techniques and tactics," and that "[t]hose things deal with national security and should be kept secret, even when their target is found to be innocent,"⁷⁰ this notice provision will never be used. Despite this apparent unfettered discretion vested in the Attorney General, there is no analogous provision applicable to electronic surveillance under FISA where the secrecy of the surveillance is determined to pose no threat to national security.

FISA also permits the Attorney General to conduct electronic surveillance under his own authority if there is an emergency situation where going to the FISC would present too much of a delay.⁷¹ This emergency surveillance is authorized as long as the FISC is informed at the time it is authorized by the Attorney General, the standard factual

THE EXTERNAL EFFECTS OF THE FEDERAL BUREAU OF INVESTIGATION'S REPRIORITIZATION EFFORTS (2005), available at <http://www.usdoj.gov/oig/reports/FBI/a0537/final.pdf>.

68. *Id.* at v.

69. 50 U.S.C. § 1825(b) (2000); see *infra* note 161 and accompanying text.

70. Joseph Rose, *Judge Gives Mayfield Ok on Challenge to Patriot Act: The Ruling Orders the FBI to Release Information About Spying and Retains Monetary Claims*, THE OREGONIAN, July 29, 2005, at A01, available at <http://www.westlaw.com> (search "2005 WLNR 23960027").

71. 50 U.S.C. § 1805(f) (Supp. I 2002).

bases for such surveillance exist, the minimization procedures are followed, and an application is submitted to the FISC at the end of seventy two hours.⁷² If subsequent approval by the FISC is not obtained at the end of those seventy two hours, the notice provision is triggered.⁷³ It provides that:

[T]he judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of: 1) the fact of the application; 2) the period of the surveillance; and 3) the fact that during the period information was or was not obtained. On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.⁷⁴

This notice provision applies only to those narrow situations where the Attorney General has authorized emergency electronic surveillance and no subsequent approval by the FISC is obtained. In this respect, it is worth noting that the FISC has only denied a total of six applications out of the near twenty thousand submitted over the last twenty seven years.⁷⁵ Disagreements between the FISC and the executive over an application have recently resulted in modification instead of denial.⁷⁶ Regardless of whatever inferences one draws from this, the conclusion is that the only way that those subject to unlawful electronic surveillance can be notified is when the emergency surveillance is so grievously erroneous as to provoke one of these extraordinary denials by the FISC.

The emergency notice provision above is modeled after a very similar provision located in Title III.⁷⁷ In fact, the two provisions are nearly identical, except for one major difference in scope. Title III's notice provision applies not only to retroactive denials of emergency electronic surveillance but to *all* electronic surveillance that has been completed.⁷⁸ It is triggered "[w]ithin a reasonable time but not later than ninety days after the filing of an application for an order of approval under [Title III's emergency surveillance provision] which is denied *or the termina-*

72. *Id.*

73. 50 U.S.C. § 1806(j) (2000).

74. *Id.*

75. FISA Annual Reports to Congress, <http://www.fas.org/irp/agency/doj/fisa/#rept>.

76. The FISC has increasingly modified applications over the last two years. It substantively modified ninety-four applications in 2004 and seventy-nine in 2003, but only a total of eight in all prior years. *Id.*

77. 18 U.S.C. § 2518(8)(d) (2000).

78. *Id.*

tion of the period of an order or extensions thereof”⁷⁹ Like the emergency notice provision in FISA, this provision requires a judge to notify any named person in the application and permits the judge to notify any other person subject to the surveillance if it is in the interest of justice.⁸⁰ Such a provision is therefore capable of providing notice to those who are erroneously named in an application or those otherwise subject to unlawful surveillance. As noted above, this general notice provision was drafted in order to effectuate Title III’s civil liability provision.⁸¹ Despite enacting an analogous civil action in FISA ten years later, Congress neglected to provide a notice provision similarly capable of effectuating the statutory cause of action.

While it is certainly awkward to have a cause of action incapable of being utilized, it becomes unacceptable when the cause of action is incapable of remedying concrete statutory violations. The question then becomes whether such statutory violations are occurring.

IV. ERRORS IN THE FISA PROCESS

Neither the general public nor the victims of unlawful electronic surveillance have any knowledge regarding the frequency with which such surveillance occurs. Although this secrecy necessarily makes the following description incomplete, the errors in the FISA process that have been revealed to the public have been severe and are likely to recur in the future.

A. Application Process

In the FISC’s first and only published opinion, it wrote:

In September 2000, the government came forward to confess error in some 75 FISA applications The errors related to misstatements and omissions of material facts After receiving a more detailed explanation from the Department of Justice about what went wrong, but not why, the Court decided not to accept inaccurate affidavits from FBI agents whether or not intentionally false. One FBI agent was barred from appearing before the Court as a FISA affiant.⁸²

These errors involved violations of minimization procedures that imposed an informational “wall” between FBI intelligence investigators and criminal prosecutors.⁸³

79. *Id.* (emphasis added).

80. *Id.*

81. See *supra* note 60 and accompanying text.

82. *In re All Matters*, 218 F. Supp. 2d 611, 620-21 (FISA Ct. 2002).

83. See Memorandum from Janet Reno, Attorney General on Procedures for Contacts Between the FBI and Criminal Division Concerning Foreign Intelligence and Foreign Counterintelligence Investigations (July 19, 1995), <http://www.fas.org/irp/agency/doj/fisa/>

The wall prevented criminal prosecutors and investigators from directing foreign intelligence investigations.⁸⁴ For instance, “the government’s misstatements and omissions in FISA applications and violations of the court’s orders involved information sharing and unauthorized disseminations to criminal investigators and prosecutors.”⁸⁵ Despite the fact that such information sharing is currently permissible under the Patriot Act and the government’s revised minimization procedures,⁸⁶ the errors were quite serious at the time because the wall was thought to be what saved FISA from violating the Fourth Amendment.⁸⁷ The FISA Court of Review disagreed, holding that FISA, as amended by the Patriot Act, did not violate the Fourth Amendment.⁸⁸ Prior to the Patriot Act and the new minimization procedures, however, the errors related to material omissions in the sense that had the FISC known of these violations at the time, they would not have issued the application as presented. So despite the fact that the DOJ had successfully obtained a FISA order, the electronic surveillance conducted pursuant to the order would have been unlawful because the synthesis of the initial application violated the minimization procedures.⁸⁹

1995procs.html. “The 1995 Procedures formalized the unwritten policy that had existed since the 1980s requiring the Criminal Division, rather than the local USAO, to be consulted about intelligence investigations when questions of criminal activity or criminal prosecution arose.” OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, A REVIEW OF THE FBI’S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS (NOV. 2004), available at <http://www.usdoj.gov/oig/special/0506/final.pdf>. This policy arose in response to a number of federal appellate decisions requiring the “primary purpose” of a FISA investigation to be gathering foreign intelligence information. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980); *United States v. Johnson*, 952 F.2d 565 (1st Cir. 1991); *United States v. Pelton*, 835 F.2d 1067 (4th Cir. 1987). The executive became concerned that any information obtained in violation of the primary purpose standard would be inadmissible in a criminal proceeding.

84. *All Matters*, 218 F. Supp. 2d at 619-20 (“The Criminal Division may then consult with the FBI and give guidance to the FBI aimed at preserving the option of criminal prosecution, but may not direct or control the FISA investigation toward law enforcement objectives.”).

85. *Id.* at 621.

86. See *id.* at 621-22; *supra* notes 64-65.

87. See *All Matters*, 218 F. Supp. 2d at 620 (“In order to preserve both the appearance and the fact that FISA surveillances and searches were not being used sub rosa for criminal investigations, the Court routinely approved the use of information screening “walls” proposed by the government in its applications, where . . . FBI criminal investigators and Department prosecutors were not allowed to review all of the raw FISA intercepts or seized materials lest they become de facto partners in the FISA surveillances and searches.”); see also David Hardin, *The Fuss over Two Small Words: The Unconstitutionality of the USA Patriot Act Amendments to FISA Under the Fourth Amendment*, 71 GEO. WASH. L. REV. 291 (2003); Michael P. O’Connor & Celia Rumann, *Emergency and Anti-Terrorist Powers: Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT’L L.J. 1234 (2003); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385 (2003).

88. *In re Sealed Case*, 301 F.3d 717, 746 (FISA Ct. Rev. 2002).

89. See 50 U.S.C. § 1805(a)(4) (2000).

Just as the minimization procedures play a fundamental role in the FISA process, so too does the accuracy of the substantive information forming the basis of the FISA application. As one FBI attorney acknowledged: "It is imperative that the facts contained in FISA declarations are accurate."⁹⁰ If the facts are not accurate, this will unacceptably taint the FISC's probable cause determination regarding whether the individual is an agent of a foreign power. The agent of a foreign power standard is the linchpin of FISA, and if the probable cause determination is based on inaccurate facts, the corresponding surveillance must be considered unlawful.⁹¹

Although the FISC opinion described omissions relating to the unauthorized sharing of information, even prior to the FISC opinion the government independently acknowledged that their methods to ensure the accuracy of FISA applications were inadequate. Deputy Attorney General David Kris testified before the Senate Judiciary Committee that:

The main challenge to accuracy in FISA applications is that the FBI agent who signs the affidavit *describing* the investigation for the court is not the agent who actually *conducts* the investigation. . . . And that is where inaccuracy can creep in: If the headquarters agent has a miscommunication with the agents in the field, his affidavit will be inaccurate.⁹²

In order to prevent these inaccuracies, the FBI adopted the Woods Procedures in April 2001.⁹³ The preface of these procedures states: "The goal of the procedures set out below is to ensure accuracy with regard to . . . the specific facts supporting probable cause for the authority."⁹⁴ These procedures are detailed, but generally require information sharing between the field office and headquarters and confirmation that the target is neither the subject of an ongoing criminal investigation nor an FBI informant.⁹⁵

The Senate Judiciary Committee reviewed these procedures, however, and concluded that: "Even the much touted 'Woods Procedures' governing the procedures to be followed by FBI personnel in preparing FISA applications do not require Headquarters personnel to conduct even the most basic subject matter computer searches or checks as part

90. E-mail from Michael Woods, National Security Law Unit, FBI Office of the General Counsel, to All Field Offices, at 2 (Apr. 5, 2001) [hereinafter E-mail from Michael Woods], <http://www.fas.org/irp/agency/doj/fisa/woods.pdf>.

91. See *supra* note 15.

92. *The USA Patriot Act in Practice: Shedding Light on the FISA Process Before the S. Comm. on the Judiciary*, *supra* note 66.

93. E-mail from Michael Woods, *supra* note 90.

94. *Id.* at 2.

95. *Id.*

of the preparation and review of FISA applications.”⁹⁶ The Committee, in a set of written questions addressed to FBI Director Robert Mueller, noted that the background checks required inputting only the target’s name and not a general subject matter search.⁹⁷ In addition, the field office is primarily responsible for conducting this research and the Committee noted that their computers do not always have the same degree of access as those at headquarters.⁹⁸ And finally, the Committee asked: “Is it intended that the Woods Procedures be the extent of the investigation in connection with the preparation of a FISA application, or is it expected that the field agents and headquarters unit will pursue all necessary and logical leads, including a basic key word search?”⁹⁹ Acknowledging that the FBI computer system will not always contain all of the relevant information, the FBI responded that the Woods Procedures “in no way constitute the extent of the investigation in connection with the preparation of a FISA application.”¹⁰⁰ So although the Woods Procedures help formalize the application process by providing a checklist for agents to follow, they do not preclude factual inaccuracies from permeating the application on which the probable cause determination depends.

Not only can miscommunication and inadequate research lead to factual inaccuracies forming the basis of a FISA application, but so too can errors in the investigative process. The erroneous fingerprint analysis in the Mayfield case is a prime example of this. After conducting an investigation of the incident, the Office of the Inspector General “concluded that the FBI’s field investigation of Mayfield was initiated because of and largely driven by the identification of his fingerprint on evidence associated with the train bombings”¹⁰¹ Even after the Mayfield incident and its negative publicity, systemic performance problems relating to latent fingerprint analysis still represent a potential source of factual inaccuracy.¹⁰² Although the investigation acknowledged that the FBI Laboratory has initiated some significant reforms, it

96. *FISA Implementation Failures Before S. Comm. on the Judiciary*, 108th Cong. (2003), available at http://www.fas.org/irp/congress/2003_rpt/fisa.html.

97. *Interim Report on FBI Oversight in the 107th Congress by the Senate Judiciary Committee: FISA Implementation Failures Before the S. Comm. on the Judiciary*, 107th Cong. (2002) (written answers by William Moschella, Assistant Attorney General, in response to questions addressed to Robert Mueller, FBI Director, by Sen. Patrick Leahy, at 10), available at <http://www.fas.org/irp/agency/doj/fisa/fbi082903.pdf>.

98. *Id.* at 11.

99. *Id.*

100. *Id.*

101. A REVIEW OF THE FBI’S HANDLING OF THE BRANDON MAYFIELD CASE, *supra* note 21, at 18.

102. *Id.* at 20 (“While we did not find any intentional misconduct by FBI employees, either in the Laboratory or by those conducting the FBI field investigation, we did find performance issues

“found that the actions proposed by the Laboratory were not fully responsive to the issues raised by the Mayfield misidentification and that additional or more specific modifications to Laboratory practices should be adopted.”¹⁰³ In sum, miscommunication, poor research, fingerprint errors, and other forensic mistakes may all contribute to factual inaccuracies in a FISA application that will unacceptably taint the probable cause determination, thus rendering the corresponding surveillance unlawful.

B. *Implementation Process*

1. INTERNAL FBI COMMUNICATIONS: APRIL 2000

Two brief internal FBI communications written in April 2000 provide a rare and privileged glimpse into the FISA implementation process. The first is a moderately redacted e-mail dated April 5, 2000, describing a technological error involving electronic surveillance.¹⁰⁴ The second, dated April 14, is a more comprehensive memorandum directed to “All Field Offices,” entitled “Caution on FISA Issues,” and released more than two years after the FBI recognized the severe problems described in the memo.¹⁰⁵

Unlike application errors that affect the validity of a FISA order, the examples that follow are unlawful in the sense that the target or type of surveillance described in the application and approved by the FISC did not correspond to the surveillance that was actually conducted.¹⁰⁶ In other words, although the FISA order may have been valid, the implementation of that order was erroneous.

The April 14 memorandum begins:

In the first quarter of the year 2000, different field offices have encountered difficulties in their management of electronic surveillances and physical searches authorized under FISA. After one quarter of reporting we are aware of potential violations numbering three and one-half times those reported in 1999. Examples of problems encountered follow.¹⁰⁷

by various FBI employees. Most significantly, we found a series of systemic issues, particularly in the FBI Laboratory, that helped cause the errors in the Mayfield case.”).

103. *Id.* at 14.

104. E-mail from [Redacted], to Spike (Marion) Bowman (Apr. 5, 2000, 17:29 EST) [hereinafter E-mail from [Redacted]], <http://www.fas.org/irp/agency/doj/fisa/del061402.pdf>.

105. Memorandum from FBI Counterterrorism Division, Office of General Counsel, to All Field Offices (Apr. 14, 2000) [hereinafter Memorandum from FBI Counterterrorism Division], <http://www.fas.org/irp/agency/doj/fisa/ec.pdf>.

106. *See supra* note 15.

107. Memorandum from FBI Counterterrorism Division, *supra* note 105.

It is useful to quote the examples described at length in order to properly illustrate the nature of these errors. Two examples follow:

In one case, a field office secured a FISA which had to be implemented by a second field office. *The second field office implemented the FISA order incorrectly, and videotaped a meeting even though videotaping was not authorized in the FISA order. . . .* In [another] example, a target's E-mail was correctly intercepted under a FISA order. When time came to renew the FISA, the field office decided to omit E-mail coverage since the coverage was not productive. Thus, the FISA renewal order did not cover E-mail. *The field office then continued to cover the target's E-mail even though there was no authorization for E-mail coverage in the FISA renewal order.*¹⁰⁸

When one asks *how* these errors occurred, the implications extend beyond unauthorized videotaping and e-mail coverage. The most likely explanation is that the executing official simply did not read the FISA order carefully. This assumption is supported by a later portion of the same FBI memorandum: "It is important that field offices read carefully every FISA package and not assume that the FISA packages are similar, [or] have the same authorities. . . . Every FISA package must be assumed to be unique and read in its entirety by agents responsible for the investigation."¹⁰⁹ Failure to meticulously read an order will undoubtedly lead to surveillance that has not been authorized by the FISC.

Another example describes the following error:

In another investigation, a field office secured a FISA order which authorized the coverage of a target's cell phone. Unknown to the field office, some time after the FISA order, the target gave up his cell phone, and the target's cell phone number was assigned by the cell phone carrier to a new person. The new owner of the cell phone spoke a language other than the language spoken by the target of the FISA. When the language specialist listened to the FISA tape, and heard a new language, the specialist reported it to the agent working the case. Nothing was done for a substantial period of time, and timely reported [sic] was not made to FBIHQ. *The new owner of the cell phone number was therefore the target of unauthorized electronic surveillance for a substantial period of time.*¹¹⁰

Although the controversial roving wiretap provision was enacted to respond to these kinds of evasive terrorist tactics,¹¹¹ the above example

108. *Id.* (emphasis added).

109. *Id.*

110. *Id.* (emphasis added).

111. See United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, § 206, 115 Stat. 272, 282 (codified at 50 U.S.C. § 1805(c)(2)(B) (Supp. I 2002)), amended by USA Patriot Improvement

represents a serious failure to minimize the acquisition of non-foreign intelligence information by continuing to monitor someone who was known not to be the agent of a foreign power named in the order.¹¹²

The memo then briefly adds without explanation that “[o]ther examples include unauthorized searches, incorrect addresses, incorrect interpretation of a FISA order and overruns of [electronic surveillance].”¹¹³ Not only does this sentence suggest that the examples above are not isolated incidents, but it also indicates that more severe errors, such as conducting electronic surveillance of the wrong home, have occurred as well.

The e-mail of April 5 provides another concrete example of unauthorized surveillance and introduces technology as the source of this error:

The FBI technical people went to install the FBI software . . . to accomplish the electronic surveillance on March 16. The software was turned on and did not work correctly. The FBI software not only picked up the e-mails under the electronic surveillance of the FBI target . . . but *also picked up e-mails on non-covered targets* [Office of Intelligence and Policy Review (OIPR) of the DOJ] was never told that the FBI software was experimental. OIPR was informed that it would work. . . . When you add this story to the FISA mistakes covered in the [April 14 memo] prepared to go to the field . . . you have a pattern of occurrences which indicate to OIPR an inability on the part of the FBI to manage its FISAs.¹¹⁴

Perhaps the most troubling aspect of technological malfunction is the inability to predict when it will occur. Steps can be taken to ensure that technological devices are tested before being employed, but such mea-

and Reauthorization Act of 2005, Pub. L. No. 109-177, 120 Stat. 192, 195, 203-04, §§ 102(b), 108 (2006) (codified as amended in scattered sections and titles of the U.S.C.A.). Instead of identifying the particular device that an agent of a foreign power will be using, roving wiretaps authorize electronic surveillance of a particular target and the devices that he may use. This makes it unnecessary for the government to return to the FISC every time the agent of a foreign power changes cell phones. Some have argued that both this provision, and the Title III provision after which it is modeled, violate the Fourth Amendment's particularity requirement. See Kelly R. Cusick, *Thwarting Ideological Terrorism: Are We Brave Enough to Maintain Civil Liberties in the Face of Terrorist Induced Trauma?*, 35 CASE W. RES. J. INT'L L. 55, 75 (2003); Bryan R. Faller, *The 1998 Amendment to the Roving Wiretap Statute: Congress "Could Have" Done Better*, 60 OHIO ST. L.J. 2093, 2093 (1999).

112. See 50 U.S.C. § 1805(c)(2)(a) (Supp. I 2002) (“An order approving an electronic surveillance under this section shall direct that the minimization procedures be followed.”).

113. Memorandum from FBI Counterterrorism Division, *supra* note 105.

114. E-mail from [Redacted], *supra* note 104 (emphasis added). It should also be noted that technological deficiencies are not limited to the FBI but extend to the service providers that assist the FBI with electronic surveillance. See *infra* note 118 and accompanying text. These service providers are shielded from liability in connection with these services. See 50 U.S.C. § 1805(i) (Supp. I 2002).

asures cannot eliminate technology as a potential and perhaps inevitable source of error.

2. SIMILAR ERRORS REVEALED FIVE YEARS LATER: SEPTEMBER 2005

Demonstrating that the errors described above are likely to recur, on September 30, 2005, the Associated Press released an article entitled *Wrong Number: FBI Says it Makes Mistakes in National Security Wiretaps*.¹¹⁵ In this article, the FBI admitted again to problems nearly identical to those identified in the April communications.

With respect to technological errors, and making the counterintuitive point that improvements in technology will actually make it more difficult to conduct accurate surveillance, the general counsel for the Electronic Privacy Information Center observed that “technological advances have made it harder, not easier, to ‘conduct wiretapping in a surgical way’ because digital communications often carry many conversations. It’s not like the old days when there was one dedicated line between me and you.”¹¹⁶ The FBI admitted that “38,514 untranslated hours [of FISA intercepts] included an *undetermined* number from what the FBI called ‘collections of materials from the wrong sources due to technical problems.’”¹¹⁷

The article further revealed additional instances of unauthorized surveillance. Where “the tap was placed on a telephone number other than the one authorized by the court,” for example, was attributed to “an instance in which the telephone company hooked us up to the wrong number or a clerical error [that] gives us the wrong number.”¹¹⁸ Clerical errors therefore present an obvious, additional source of error that is also systematically difficult to prevent. An “O” instead of a “0”, for example, can result in the unauthorized surveillance of the wrong phone number, address, or e-mail account.

Regardless of what steps may be taken to heighten prevention of the implementation errors described in this section, the last five years have demonstrated that these errors may simply be inevitable casualties of foreign intelligence surveillance. (Again, one can only imagine the

115. Mark Sherman, *Wrong Number: FBI Says it Makes Mistakes in National Security Wiretaps*, ASSOCIATED PRESS, Sept. 30, 2005, at 1, available at <http://www.oppression.org/cgi-bin/viewnews.cgi?category=4&id=1128143231>.

116. *Id.*

117. *Id.* (emphasis added); see generally OFFICE OF THE INSPECTOR GENERAL, DEPARTMENT OF JUSTICE, REPORT NO. 04-25, THE FEDERAL BUREAU OF INVESTIGATION’S FOREIGN LANGUAGE PROGRAM – TRANSLATION OF COUNTERTERRORISM AND COUNTERINTELLIGENCE FOREIGN LANGUAGE MATERIAL (July 2004), available at <http://www.usdoj.gov/oig/reports/FBI/a0425/index.htm#note> (auditing the FBI’s ability to translate critical foreign language material derived from FISA in a manner consistent with the Bureau’s priorities).

118. Sherman, *supra* note 115.

extent of the violations if there was no judicial oversight. “Imagine” is the appropriate word here, because without the FISC, there would have been no impetus for the government to reveal any errors.) This conclusion supports the adoption of affirmative measures designed to provide relief to those who are victims of such errors.

V. RETURN AND NOTICE PROCEDURE

It is indisputable that the government cannot be in the business of informing suspected terrorists that they are being monitored. “If the existence of these searches were known to the foreign power targets, they would alter their activities to render the information useless. Accordingly, a notice requirement, such as exists in the criminal law, would be fatal.”¹¹⁹ Nor would it be appropriate to inform those with connections to an agent of a foreign power that they had been subject to surveillance for the same reason.

FISA’s emergency notice provision is puzzling in light of this concern. As noted above, the emergency notice is triggered when a subsequent order approving emergency surveillance is not obtained.¹²⁰ Failure to obtain a subsequent order may be due to the denial of an application by the FISC or to the failure of the executive to submit an application at the end of the seventy-two hours as required by section 1805(f).¹²¹ The first thing to note is that if the FISC denies the subsequent application after emergency surveillance, undoubtedly a rare event,¹²² the FISC would be *required* to notify any United States per-

119. *Warrantless Physical Searches Conducted in the U.S. for Foreign Intelligence Before the H. Permanent Select Comm. on Intelligence*, 103rd Cong. 3-4 (1994) (statement of James S. Gorelick, Deputy Attorney General), available at <http://www.cnss.org/Gorelicktestimony.pdf>. In the criminal context, notice is a constitutional component of the Warrant Clause of the Fourth Amendment. See *Berger [sic] v. New York*, 388 U.S. 41, 60 (1967) (“[The New York wiretapping statute] has no requirement for notice as do conventional warrants, nor does it overcome this defect by requiring some showing of special facts.”). In discussing the proposed Title III notice provision, Senator Hart stated: “‘The *Berger [sic]* and *Katz [sic]* decisions established that notice of surveillance is a constitutional requirement of any surveillance statute. It may be that the required notice must be served on all parties to intercepted communications.’” *United States v. Donovan*, 429 U.S. 413, 430 (1977) (quoting 114 Cong. Rec. S14485-86 (1968) (statement of Sen. Hart)). If this was true with respect to foreign intelligence surveillance, there could be no effective foreign intelligence surveillance statute that complied with the Constitution. The lack of notice in FISA finds constitutional support in the rationale of the passage in *Keith* that flexibly construes the warrant requirement as one that may vary with new governmental interests. See *supra* note 36 and accompanying text; *infra* note 127. To be clear, this Note does not contend that the Fourth Amendment requires notice in the foreign intelligence context.

120. 50 U.S.C. § 1806(j) (2000).

121. 50 U.S.C. § 1805(f) (Supp. I 2002). It is not clear *how* notice is to be served in emergency surveillance cases without a return procedure making the surveillance available to the FISC. It is likely, although unknowable, that this notice provision has never been triggered.

122. *Supra* notes 75-76 and accompanying text.

son¹²³ named in the application,¹²⁴ who may be an agent of a power.¹²⁵ The FISC would also have discretion to notify any United States person not named in the subsequent application who is subject to the surveillance if it is in the interest of justice, subject to an ex parte showing of good cause by the government.¹²⁶ This again may include agents of a foreign power or those connected to an agent of a foreign power. Although the FISC would not choose to notify such individuals, the point is that the discretion to do so has been vested with the FISC in emergency surveillance situations, and no such discretion exists in ordinary FISA cases.

It is not clear why, based on checks and balances, such discretion should be foreclosed for victims of unlawful surveillance in the typical FISA case. Emergency surveillance is suspect because the Attorney General acts as the FISC, thus removing the check on executive power. If this is the rationale for providing notice in emergency cases then it should follow that surveillance conducted pursuant to an invalid order (application errors) or surveillance that is not authorized by an order (implementation errors) should trigger a notice provision as well. In these cases, there is similarly no effective check on the executive branch. With respect to application errors, the FISC cannot act as a check when it unknowingly approves FISA orders based on, for example, inaccurate facts. With respect to implementation errors, the FISC cannot act as an effective check after the order has been issued and the executive does not conduct the surveillance as authorized. Triggering notice only when the FISC has not retroactively approved emergency surveillance, but not when there has been an application or implementation error, is inconsistent with principles of checks and balances.

The legislative history does not offer an explanation for why notice is provided only in emergency cases (aside from the general need for

123. See 50 U.S.C. § 1801(i) (2000) (“‘United States person’ means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3) of this section.”).

124. § 1806(j).

125. See SEN. REP. NO. 95-604, pt. 1, at 59 (1978), as reprinted in 1978 U.S.C.C.A.N. 3904, 3960 (“The failure to obtain [FISC] approval . . . need not be based on a determination by the court that the target is not an agent of a foreign power Failure to secure a warrant could be based on a number of other factors, such as an improper certification.”). Simply making such notice discretionary can cure this flaw in the statute.

126. § 1806(j). In situations where no subsequent application was submitted to the FISC within seventy-two hours as required by section 1805(f), then this discretion would also seemingly apply to all United States persons subject to the surveillance. *Id.*; but see *supra* note 121.

secrecy in all foreign intelligence surveillance).¹²⁷ The closest explanation is the following passage:

A requirement of notice in all [emergency surveillance] cases would have the potential of compromising the fact that the government had focused an investigation on the target. Even where the target is not, in fact, an agent of a foreign power, given [sic] notice to the person may result in compromising an on-going foreign intelligence investigation because of the logical inferences a foreign intelligence service might draw from the targeting of the individual. For these reasons, the government is given the opportunity to present its case to the judge for initially postponing notice.¹²⁸

But this passage explains why notice cannot be provided to everyone subject to emergency surveillance, not why only a notice provision was provided for emergency surveillance. The same explanation applies in the instance where notice cannot be given to everyone subject to electronic surveillance under FISA in general, even those who are not agents of a foreign power, such as the spouse who is oblivious to her husband's terrorist activities. In that case, the spouse could not be notified because it would be functionally equivalent to notifying the agent of a foreign power himself.

The issue then is whether an analogous mechanism to the return and notice procedure of Title III could operate in the FISA context. To cure one of the defects of the New York wiretapping statute invalidated in *Berger v. New York*,¹²⁹ the first step under the Title III return and notice procedure is the actual return of the surveillance to the judge.¹³⁰ Section 2518(8)(a) requires that, after the expiration of a Title III order, the contents of the surveillance "shall be made available to the judge issuing such order and sealed under his directions."¹³¹ In *United States v. Donovan*, the Supreme Court required that the government supply additional information to allow the judge to effectively exercise his discretion under section 2518(8)(d) to provide notice to those not named in the warrant if it is in the interest of justice.¹³²

Notice to those not named in the application was made discretion-

127. S. REP. NO. 95-701 at 12 (1978), as reprinted in 1978 U.S.C.C.A.N. 3973, 3980 ("The need to preserve secrecy for sensitive counterintelligence sources and methods justifies elimination of the notice requirement . . .").

128. S. REP. NO. 95-604, pt. 1, at 59-60 (1978), as reprinted in 1978 U.S.C.C.A.N. 3904, 3960-61.

129. *Berger v. New York*, 388 U.S. 41, 60 (1967) ("Nor does the statute provide for a return on the warrant thereby leaving full discretion in the officer as to the use of seized conversations of innocent as well as guilty parties.").

130. 18 U.S.C. § 2518(8)(a) (2000).

131. *Id.*

132. *United States v. Donovan*, 429 U.S. 413, 430-32 (1977).

ary, rather than mandatory, because Congress recognized that in some cases it would be in the best interest of the target not to notify those incidentally subject to the surveillance.¹³³ Take for example: "A, a businessman, talks with his customers, and the latter are served with papers showing that A is being bugged. . . . [T]he damage to confidence in A and to A's reputation in general may damage A unjustly. In this case it would seem that the customers should not be served with the inventory."¹³⁴ In an analogous situation under FISA, the concern with notifying those incidentally subject to electronic surveillance would not be that it might be unjust to the agent of a foreign power, but that it would alert the agent of a foreign power that he was being monitored. In those situations, discretionary notice would be for the purpose of protecting an intelligence investigation.

The notice provision in section 2518(8)(d), like the emergency notice provision in FISA, then mandates inventory notice be served on those named in the application and provides for discretionary notice to all others subject to the surveillance for not longer than ninety days after the duration of the order has expired.¹³⁵ The notice may be postponed upon an *ex parte* showing of good cause by the government.¹³⁶

There are significant differences in the FISA process. Not only is there not a general notice provision, but there is no return provision analogous to section 2518(8)(a) that requires the FBI to return surveillance to the FISC. The FISC is unable to notify anyone that is subject to surveillance because once the FISA order has been granted, the matter is generally handled exclusively by the executive. There are two ways that the FISC can partially discover how a FISA order is being implemented. First, there is a provision in the statute that allows the FISC to assess the government's compliance with the minimization procedures.¹³⁷ Second, if the government applies for an extension, this requires the government to meet the same requirements as if the application was being originally filed.¹³⁸ In that situation, the application for an extension would likely contain information regarding previous applications, including past activities of the target.¹³⁹ Both of these situations, however, are a far cry from a general return provision like section 2518(8)(a) that provides a judge with direct supervision over the surveillance issued under his

133. *Id.* at 429-30.

134. *Id.* at 430.

135. 18 U.S.C. § 2518(8)(d) (2000).

136. *Id.* The FISA emergency surveillance provision allows a second showing of good cause to forego the notice entirely. 50 U.S.C. § 1806(j) (2000).

137. 50 U.S.C. § 1805(e)(3) (Supp. I 2002).

138. 50 U.S.C.A. § 1805(e)(2) (West 2006).

139. *See* 50 U.S.C. § 1804(a)(9) (2000); 50 U.S.C. § 1805(b) (Supp. I 2002).

authority. Not only does this structural separation between the FISC and the actual surveillance effectively prevent the FISC from discovering errors in the process,¹⁴⁰ but it also prevents the FISC from serving anyone with notice.

This structural separation in the FISA context arises from the minimization procedures and the preference in favor of immediate, non-supervised destruction, rather than retention, of non-foreign intelligence information that is gathered. As a general matter, minimization procedures under FISA are procedures adopted by the Attorney General that meet the flexible statutory definition of procedures that "are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."¹⁴¹

These procedures are borrowed from the concept of minimization in Title III,¹⁴² as they attempt to safeguard the privacy rights of American citizens, as much as practicable, by minimizing the acquisition, retention, and dissemination of information that is not foreign intelligence information.¹⁴³ Instead of returning such information to the judge, as is done under Title III, FISA presumes that the best way to safeguard the privacy of Americans is not to retain any such information but rather to destroy it.¹⁴⁴

It should be noted that this provision contains one significant change from the minimization provisions in [Title III]. [Section] 2518 (8) (a) requires that all interceptions be recorded, if possible, and that the tapes not be edited or destroyed for ten years. In a criminal context the maintenance of such tapes and files under court seal ensures that the interceptions will be retained in their original state so that when criminal prosecutions are undertaken it is clear that the evidence is intact and has not been tampered with. . . .

140. It is worth noting that the errors described by the FISC were not discovered by the FISC, rather, they were confessed by the FBI. *In re All Matters*, 218 F. Supp. 2d 611, 620-22 (FISA Ct. 2002).

141. 50 U.S.C. § 1801(h)(1) (2000).

142. 18 U.S.C. § 2518(5) (2000) ("Every order and extension thereof shall contain a provision that the authorization to intercept shall be executed as soon as practicable, shall be conducted in such a way as to minimize the interception of communications not otherwise subject to interception under this chapter, and must terminate upon attainment of the authorized objective, or in any event in thirty days.").

143. *See supra* note 27.

144. S. REP. NO. 95-604, pt. 1, at 38 (1978), *as reprinted in* 1978 U.S.C.C.A.N. 3904, 3939 ("By minimizing retention, the committee intends that information acquired, which does not relate to the approved purposes justifying the warrant, be destroyed.").

The Committee believes that in light of the relatively few cases in which information acquired under this chapter may be used as evidence, the better practice is to allow the destruction of information that is not foreign intelligence information or evidence of criminal activity. This course will more effectively safeguard the privacy of individuals, ensuring that irrelevant information will not be filed. . . . Destruction insures that the information cannot be used to 'taint' a civil or criminal proceeding¹⁴⁵

Instead, immediate destruction ensures that Americans whose conversations are unlawfully acquired will never find out about the interception of their communications, preventing civil proceedings from occurring at all.

If minimization procedures require that acquisition be limited to situations where foreign intelligence information is likely to be obtained, and dissemination of such communications is strictly prohibited,¹⁴⁶ it is worth asking how the immediate destruction of these communications materially safeguards privacy. Once the communication is acquired and sorted, the invasion of privacy has occurred.¹⁴⁷ That individual's privacy may only be further compromised if that recording is disseminated, which is prohibited unless it "is necessary to understand foreign intelligence information or assess its importance"¹⁴⁸ or if it is "information that is evidence of a crime which has been, is being, or is about to be committed."¹⁴⁹ The question is significant because it is this immediate destruction that effectively prevents the possibility of serving notice and conducting oversight in cases where something has gone astray in the process. The heavy costs that destruction imposes in terms of notice and oversight are not worth sacrificing when the principal invasion of privacy has already occurred.¹⁵⁰ Enabling the vindication, analysis, and oversight of unlawful surveillance more effectively serves the interests of privacy than perpetuating the belief that there are no problems occurring.

145. S. REP. NO. 95-604, pt. 1, at 39 (1978), as reprinted in 1978 U.S.C.C.A.N. 3904, 3940-41.

146. See 50 U.S.C. § 1801(h) (2000); *infra* note 179.

147. Judge Richard Posner has noted that the use of machines to conduct the initial collection and processing of private data protects the privacy of most private data because it keeps it from being read by an individual. Richard Posner, *Our Domestic Intelligence Crisis*, WASH. POST, Dec. 21, 2005, at A31. This distinction is irrelevant in the FISA context, however, because an FBI agent, and not a machine, is responsible for making the key determination of whether information that has been gathered under FISA qualifies as foreign intelligence information. See *infra* notes 154-55 and accompanying text.

148. 50 U.S.C. § 1801(h)(2) (2000).

149. *Id.* § 1801(h)(3).

150. Returning such information to the FISC does not significantly compound the invasion of privacy. This additional minor invasion is justified by the ultimate objectives of the return procedure to provide relief for, and improve oversight of, unlawful electronic surveillance.

The "principal steps in the minimization process"¹⁵¹ that lead to the destruction of non-foreign intelligence information are as follows:

[I]nformation is reduced to an intelligible form . . . once the information is understandable, a reviewing official, usually an FBI case agent, makes an informed judgment as to whether the information seized is or might be foreign intelligence information related to clandestine activities or international terrorism . . . if found not to be foreign intelligence information, it must be minimized, which can be done in a variety of ways depending upon the format of the information: if recorded the information would not be indexed, and thus become non-retrievable, if in hard copy from facsimile intercept or computer print-out it should be discarded, if on re-recordable media it could be erased, or if too bulky or too sensitive, it might be destroyed.¹⁵²

Information that could be foreign intelligence information is not minimized and "is logged into the FBI's records and filed in a variety of storage systems from which it can be retrieved for analysis"¹⁵³ In making this significant determination¹⁵⁴ under the minimization procedures, "minimization is required only if the information 'could not be' foreign intelligence. Thus, it is obvious that the standard for retention of FISA-acquired information is weighted heavily in favor of the government."¹⁵⁵ As such, when sorting the surveillance, there is little risk that relevant information will be placed in the wrong pile.

The non-foreign intelligence information sorted out by the case agent should not be immediately destroyed but should instead be returned to the FISC in a manner similar to the Title III process. The statute should therefore be amended to require the executive to return the non-foreign intelligence information to the FISC.¹⁵⁶ It should also require that, before destroying any information, the FISC sort through the information returned in order to determine if particular individuals should be provided with notice based on the standard enunciated below.¹⁵⁷ This procedure would therefore accomplish the dual objective

151. *In re All Matters*, 218 F. Supp. 2d 611, 617 (FISA Ct. 2002).

152. *Id.* at 617-18.

153. *Id.* at 618.

154. *Id.* ("The most critical step in retention is the analysis in which an informed judgment is made as to whether or not the communications or other data seized is foreign intelligence information.").

155. *Id.*

156. It should also be made explicit that returning the non-foreign intelligence information to the FISC in compliance with the return provision does not violate prohibitions on dissemination.

157. It is consistent with the statute and recent practice to grant the FISC the power to monitor surveillance conducted under its authority. See 50 U.S.C. § 1805(e)(3) (2000) ("At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the

of achieving greater oversight of the FISA process¹⁵⁸ and enabling the FISC to notify particular individuals who were subjects of unlawful electronic surveillance.

The statute should then be revised to provide for a notice provision similar to the one available in the Title III and FISA emergency contexts. Unlike the Title III provision, however, not everyone subject to electronic surveillance can or should be notified.¹⁵⁹ In fact, not even everyone subject to unlawful electronic surveillance should be notified. Indeed, “in the interest of justice” should include only those people who were subject to prolonged or particularly intrusive unlawful electronic surveillance.¹⁶⁰ This determination will be in the discretion of the

circumstances under which information concerning United States persons was acquired, retained, or disseminated.”); *All Matters*, 611 F. Supp. 2d at 620 (“[T]he Court was routinely apprised of consultations and discussions between the FBI, the Criminal Division, and U.S. Attorney’s offices in cases where there were overlapping intelligence and criminal investigations or interests.”). It is also consistent with the legislative history to enable the FISC to act as the ultimate decision-maker regarding the retention and destruction of information gathered under FISA. *See* S. REP. NO. 95-604, pt. 1, at 38 (1978), *as reprinted in* 1978 U.S.C.A.N. 3904, 3939 (“Procedures governing minimization – particularly how long information should be retained and how it should be destroyed once it is deemed irrelevant – are to be fashioned by the court and are, of course, subject to judicial supervision.”).

158. As important as the congressional reporting requirements are, they do not allow for the daily oversight that the FISC can provide in terms of spotting grievous errors in the process. Statistical information regarding the number of FISA applications submitted, granted, modified, and denied is unlikely to be of much use to Congress in fulfilling its oversight responsibilities. *See supra* notes 55-57 and accompanying text. Furthermore, the Senate Judiciary Committee has recently remarked:

Particularly with respect to our FISA oversight efforts, we are disappointed with the non-responsiveness of the DOJ and FBI. Although the FBI and the DOJ have sometimes cooperated with our oversight efforts, often, legitimate requests went unanswered or the DOJ answers were delayed for so long or were so incomplete that they were of minimal use in the oversight efforts of this Committee.

FISA Implementation Failures Before S. Comm. on the Judiciary, 108th Cong. (2003), available at http://www.fas.org/irp/congress/2003_rpt/fisa.html.

159. No mandatory notice for those named in the application should be required. If notice was required for all those named in a FISA order, then this, like the emergency notice provision, could have the effect of notifying many agents of a foreign power. *See supra* notes 123-25 and accompanying text.

160. When considering the degree of intrusiveness, the FISC should be guided by Fourth Amendment principles. For example, communications taking place in the home should be considered substantially more private than those made in public. *Compare* *Kyllo v. United States*, 533 U.S. 27, 37 (2001) (“The Fourth Amendment’s protection of the home has never been tied to measurement of the quality or quantity of information obtained. . . . In the home, our cases show, all details are intimate details, because the entire area is held safe from prying government eyes.”), *and* *Katz v. United States*, 389 U.S. 347, 352 (1967) (finding a reasonable expectation of privacy in communications made from inside a public telephone booth), *with* *United States v. Dionisio*, 410 U.S. 1, 14 (1973) (holding that an individual does not enjoy a reasonable expectation of privacy in the physical characteristics of his own voice because it is constantly exposed to the public).

FISC.¹⁶¹

When extracting non-foreign intelligence information, the FBI case agent familiar with the case should label communications made by the agent of a foreign power and those related to him. This will assist the FISC with its notice determination and oversight responsibilities. In addition, the government should be required, if necessary, and as it was in *Donovan*, to assist the FISC with any questions regarding the surveillance.¹⁶²

When the FISC decides that a particular individual should be notified, the government will have the same opportunity, on an ex parte showing of good cause, to have the notice postponed or dispensed with altogether. Those connected to an agent of a foreign power, such as the oblivious spouse or next door neighbor, should be initially filtered out by the FBI case agent, thus preventing the FISC from identifying them as potential notice recipients; the government, however, would act as an additional safety net in this regard.

The government as a matter of policy would likely contest every decision to notify, but good cause here should require a *specific* showing that the notice would inform one of these individuals that they were being monitored or that notice would have the effect of disclosing confidential intelligence methods. Generalized assertions that "information that is embarrassing to [the federal government] must be kept secret for reasons of national security"¹⁶³ should not suffice. The showing to the FISC must specifically demonstrate how serving notice to that particular individual will compromise national security.

Notifying individuals of the mere fact that they have been subject to surveillance under FISA, even if they are clearly not agents of a foreign power or connected to an agent of a foreign power, is, understandably, likely to be the most controversial proposal in this Note. The distinction must be made, however, between disclosure that concretely threatens national security and disclosure that would merely embarrass the government. Based on its experience, competence, and the separation of powers, the FISC is the ideal body to make the determination as to whether notice really would provide terrorists with a page in our

161. Separation of powers compels vesting this check on executive power with the FISC instead of with the executive branch itself. Cf. 50 U.S.C. § 1825(b) (2000) (granting the Attorney General unchecked discretion to serve notice to those subject to physical searches under FISA).

162. See *supra* note 132 and accompanying text; see also 50 U.S.C. § 1804(d) (2000) ("The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title.").

163. Letter from Anthony D. Romero, Director, American Civil Liberties Union, to Dianne Feinstein, United States Senator (Apr. 4, 2005), <http://www.aclu.org/safefree/general/17563leg20050404.html>.

playbook or whether it would merely confirm the widespread and uncontroversial knowledge of the existence of the playbook itself.¹⁶⁴ The safeguards in this procedure, as well as the limited information actually disclosed, as described in Part V.B, ensure that when notice is provided, it will not endanger national security.

To briefly sum up, the main safeguards in this proposed return and notice scheme are as follows. First, the FBI case agent, before filtering out non-foreign intelligence information, must be sure that such information could not be foreign intelligence information. This even prohibits the agent from including unlawfully obtained information in the non-foreign intelligence pile. Second, the FISC will only isolate those communications representing a prolonged and intrusive invasion of privacy. Third, the government here would be able to specifically explain how and why serving notice in a particular case would threaten national security.

Only after the FISC has made its notice determinations should the non-foreign intelligence information pertaining to all those not notified be destroyed. Non-foreign intelligence information forming the basis of notice should not be destroyed until a time after damages are assessed.¹⁶⁵

When notice is provided to an individual, it will then be left to the individual to decide whether to take further action. It may very well be that those who are notified would not take action; many may even con-

164. The government has refused to draw such a distinction. The following is a revealing exchange between Senator Joseph Biden and Attorney General Alberto Gonzales at the Senate Judiciary Committee's hearings regarding the NSA program:

BIDEN: General, how has this revelation [of the NSA program] damaged the program? I'm almost confused by it but, I mean, it seems to presuppose that these very sophisticated Al Qaida folks didn't think we were intercepting their phone calls. I mean, I'm a little confused. How did it damage this?

GONZALES: . . . I think, based on my experience, it is true – you would assume that the enemy is presuming that we are engaged in some kind of surveillance. But if they're not reminded about it all the time in the newspapers and in stores, they sometimes forget.

(LAUGHTER).

Wartime Executive Power and the National Security Agency's Surveillance Authority Before the S. Comm. on the Judiciary, *supra* note 2, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601359.html> (statements of Sen. Joseph Biden, Member, Sen. Comm. on the Judiciary, and Alberto Gonzales, Attorney General). Instead of a blanket and illogical prohibition on disclosure, an independent judicial body like the FISC would possess both the competence and experience to make such distinctions. Indeed, three federal district courts have recently denied the government's invocation of the states secret doctrine in an attempt to prevent lawsuits challenging the NSA program from going forward. *See* Al-Haramain Islamic Found., Inc. v. Bush, No. 06-274-KI, 2006 WL 2583425, at *9-*24 (D. Or. Sept. 7, 2006); ACLU v. NSA, 438 F. Supp. 2d 754, 758-66 (E.D. Mich. 2006); Hepting v. AT&T Corp., 439 F. Supp. 2d 974, 980-99 (N.D. Cal. 2006).

165. *See supra* note 145 and quoted text; *infra* note 187.

sider it a noble sacrifice in the name of helping the country fight the war on terror. "Although litigants may not often choose to seek relief, it is important, in a civilized society, that the judicial branch of the Nation's government stand ready to afford a remedy in these circumstances."¹⁶⁶ The next issue then must be determining the proper remedy for those individuals that are served with notice and do decide to seek relief.

VI. REMEDY

A. *Enlarging the Scope of Civil Liability*

The errors in Part III indicate that many individuals have been subject to unlawful electronic surveillance and have never found out. The FISC will serve some of these individuals with notice under the return and notice procedure set forth in Part IV. In order for the notice to mean anything, however, these individuals must be able to seek actual relief.

Section 1810 as currently written is not capable of affording such relief. That provision reads as follows:

An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 1801(a) or (b)(1)(A) of this title, respectively, who has been subjected to an electronic surveillance or about who information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 of this title shall have a cause of action against any person who committed such violation¹⁶⁷

Aggrieved person is defined as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic surveillance."¹⁶⁸ Not all aggrieved persons have a cause of action, however, because section 1810 requires that the electronic surveillance be in violation of section 1809, the provision governing criminal liability.¹⁶⁹ Any ambiguity in the language of

166. *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 411 (1971) (Harlan, J., concurring).

167. 50 U.S.C. § 1810 (2000). If an individual is found liable under section 1810, the plaintiff is "entitled to recover (a) actual damages, but not less than liquidated damages of \$1,000 or \$100 per day for each day of violation, whichever is greater; (b) punitive damages; and (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred." *Id.*

168. 50 U.S.C. § 1801(k) (2000).

169. Section 1809 has been subject to increased attention since the revelation of the NSA program because, by its very terms, it has the potential to subject administration officials to criminal liability for conducting electronic surveillance outside of FISA. An earlier version of Senator Specter's bill sought to retroactively immunize the conduct of government officials. See Posting of Glenn Greenwald to Unclaimed Territory, <http://glenngreenwald.blogspot.com/2006/09/arden-specter-is-lying-about-his-own.html> (Sept. 16, 2006 10:27 EST) ("But once a copy of Specter's became available that week, it turned out that Specter's bill *did contain the very blanket amnesty provision which he falsely denied on national television he was offering*. As I wrote at the time, the Post and the ACLU were completely correct and Specter – in order to make his bill seem

section 1810 over this point is clarified by the brief legislative history on these two provisions that states: "The conferees agree that the civil liability of intelligence agents under this Act should coincide with the criminal liability."¹⁷⁰

Section 1809(a) criminalizes *intentional* electronic surveillance that is unauthorized by the statute,¹⁷¹ but section 1809(b) makes it a complete defense if the "electronic surveillance was *authorized by and conducted pursuant to a search warrant or court order* of a court of competent jurisdiction."¹⁷² Consequently, it is only a violation of section 1809 for purposes of section 1810 when the surveillance is both intentional and not authorized by or conducted pursuant to a FISA order.

The Brandon Mayfield case illustrates how section 1809 and section 1810 apply to victims of errors in the application process. The primary fact contributing to the finding of probable cause to believe that Mayfield was an agent of a foreign power was the result of the erroneous fingerprint analysis.¹⁷³ Mayfield would have had no cause of action under section 1810 because the surveillance, though based on an erroneous factual premise, was authorized by and conducted pursuant to an order issued by the FISC. The same result would have followed even if Mayfield's allegations that the FBI had filed false affidavits were true.¹⁷⁴ This is due to the fact that nothing in section 1809 requires that the FISA order be valid. While this may be appropriate for criminal liability, it has created a situation where those subject to surveillance based on an invalid FISA order would not have a cause of action under section 1810 even though conducting the surveillance violates the statute.

For victims of implementation errors, the surveillance would not be

less draconian than it really was – simply lied about what his own bill said (that express amnesty provision was thereafter removed from the bill, though the effect of the current Specter bill might be the same)."). With the current bill's removal of the "exclusive means" language, Specter would also amend section 1809 so that there would be criminal liability only if the surveillance violated the Constitution (rather than merely the statute). See National Security Surveillance Act of 2006, *supra* note 13, § 801(c)(2).

170. H.R. REP. NO. 95-1720, at 34 (1978) (Conf. Rep.), as reprinted in 1978 U.S.C.C.A.N. 4048, 4063.

171. 50 U.S.C. § 1809(a) (2000) (emphasis added).

172. *Id.* § 1809(b) (emphasis added).

173. See A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE, *supra* note 21, at 18.

174. See Joel Gallob, *Local Attorney on Team Filing Suit Against Feds for Lawyer Brandon Mayfield*, NEWPORT NEWS-TIMES, Oct. 13, 2004, available at <http://www.newportnewstimes.com/articles/2004/10/13/news/news24.txt> ("He asserts the FBI then filed 'false and misleading affidavits with courts in Portland, Oregon and Washington, D.C., in order to justify eavesdropping, telephone wiretaps'"); A REVIEW OF THE FBI'S HANDLING OF THE BRANDON MAYFIELD CASE, *supra* note 21, at 20 (finding no intentional violations by the FBI).

“authorized by” the FISA order, thus removing the surveillance from the scope of the defense of section 1809(b). The obstacle for these individuals, rather, is the initial requirement of section 1809(a) that the surveillance be intentional. Implementation errors would not meet this requirement because, although the surveillance would be intentionally conducted, it would not be intentionally directed against that particular individual.

The solution requires that the scope of civil liability should not depend on section 1809. Instead, it should first require that the FISA order relied upon be valid under the statute. This would allow section 1810 to provide relief to victims of unlawful electronic surveillance where the underlying FISA order was invalid, whether due to factual inaccuracies, fingerprint or other forensic errors, false affidavits, failure to follow minimization procedures, or improper certification.¹⁷⁵ Additionally, in order to encompass victims of implementation errors, section 1810 should not require that the violation be intentional. While appropriate for criminal liability, the fact that an individual was unintentionally subject to unlawful electronic surveillance should be sufficient for purposes of civil liability. Therefore, in order to encompass both errors in the application and implementation processes, civil liability should extend to any aggrieved person subject to unlawful electronic surveillance. It is significant, however, that the only aggrieved persons actually capable of availing themselves of section 1810 will be those served with notice under Part IV.

Although the civil liability provisions in Title III preclude liability when there is “good faith reliance on a court warrant or order,”¹⁷⁶ FISA is distinguishable because it lacks a general notice provision. If the return and notice provision of Part IV is adopted, those served with notice must be able to seek relief for the unlawful surveillance, regardless of whether it was, like the errors in Part III, unintentional or authorized by and conducted pursuant to an invalid FISA order.

Respecting Congress’ original intent to make criminal and civil liability co-extensive,¹⁷⁷ changes must be made when major statutory violations have become incapable of being redressed. Indeed, when enacting the Patriot Act, Congress recognized the need to enlarge the scope of civil liability for the unlawful *disclosure* of information gathered under both Title III and FISA that previously had not been cov-

175. See *supra* note 125.

176. 18 U.S.C. § 2520(d) (2000); *id.* § 2707(e)(1).

177. See *supra* note 170 and accompanying text.

ered.¹⁷⁸ This enlargement destroyed the co-extensive scope of criminal and civil liability¹⁷⁹ in order to remedy the “inequitable situation” that emerged.¹⁸⁰

Congress, however, did not recognize the inequitable situation of the victims of unlawful surveillance and therefore failed to similarly enlarge the scope of section 1810.¹⁸¹ The current scope of section 1810 is far too narrow to provide relief for victims of the errors described in Part III and served with notice under the procedure of Part IV. If the notice procedure of Part IV is to be meaningful, it must be accompanied by civil liability capable of remedying the violations identified by the FISC.

The effect of this proposed enlargement would be that, in the process of identifying those individuals entitled to receive notice, the FISC would be making a determination that the individual is entitled to relief. The issue of liability would therefore be determined by the FISC as it decides who is eligible to receive notice. This would significantly eliminate the need for any subsequent judicial determination of liability. Concerns that these revisions unnecessarily broaden the scope of civil liability are again ameliorated by the fact that if the return and notice scheme of Part IV is adopted, only a select few within this scope would actually be served with the notice necessary to seek relief.

B. *Claims Procedure and Compliance with Due Process*

Because liability would be determined contemporaneously with the FISC’s decision to notify an individual, it would be inappropriate to

178. See DEPARTMENT OF JUSTICE, USA PATRIOT ACT: SUNSET REPORT 67 (2005), available at http://www.epic.org/privacy/terrorism/usapatriot/Sunsets_Report_Final.pdf.

179. Section 223 of the Patriot Act added a new cause of action for any willful violation of 50 U.S.C. § 1806(a) that prohibits disclosure of information obtained *both* lawfully and unlawfully under FISA. United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001, § 223(c)(1)(a), 115 Stat. 272, 292 (codified at 18 U.S.C. § 2712(a) (Supp. I 2002)). Section 1809, however, criminalizes disclosure of information obtained only by “electronic surveillance not authorized by statute.” 50 U.S.C. § 1809(a)(2) (2000).

180. DEPARTMENT OF JUSTICE, USA PATRIOT ACT: SUNSET REPORT, *supra* note 178 (“Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. Section 223 of the USA Patriot Act remedied this inequitable situation.”). It would really amount only to an inequitable situation in the FISA context if liability was possible in the former case which, as this Note demonstrates, is currently not a reality.

181. It should be noted that the House of Representatives sought to revise section 1810 in a bill that was considered three weeks prior to the enactment of the Patriot Act. The bill substituted as the defendant the individual *or entity* responsible and adopted the same statute of limitations, administrative discipline, and administrative settlement provisions found in Title III. See Provide Appropriate Tools Required to Intercept and Obstruct Terrorism (PATRIOT) Act of 2001, H.R. 2975, 107th Cong. § 161.

require that individual to bring a traditional cause of action. Section 1810 should be amended to eliminate the cause of action and to establish in its place a claims procedure by which notified individuals could file a claim in the FISC for damages. Authorizing the FISC to process these claims would prevent federal courts from being required to conduct in camera analyses of complex FISA investigations with which they are unfamiliar.

There would be no practical reason for claimants to bring suit because the FISC, an Article III court, would be responsible for determining liability and assessing damages. Nonetheless, if for some ideological or tactical reason an individual filed suit in open court, he would not be able to bring a *Bivens* action¹⁸² or a claim under the Federal Torts Claims Act (FTCA)¹⁸³ because the individual would not have the factual information necessary to state a claim. Similar to Title III and FISA emergency surveillance cases, the notice would merely inform the individual of the fact that information was unlawfully obtained using electronic surveillance pursuant to FISA.¹⁸⁴

Nonetheless, Congress should expressly declare the claims procedure to be the exclusive remedy, thus displacing all other judicial (*Bivens* claims) and statutory (FTCA) remedies.¹⁸⁵ So even if the individual

182. *Bivens v. Six Unknown Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971) (creating a judicial cause of action brought under the Fourth Amendment for damages against federal officials).

183. Federal Torts Claims Act, Pub. L. No. 79-601, 60 Stat. 842 (1946) (codified as amended in scattered sections of 28 U.S.C.).

184. Even if the notice itself could be included as evidence of unlawful electronic surveillance, this would not be sufficient to state a claim under *Bivens* or the FTCA. *Bivens* actions require that the plaintiff allege a constitutional harm. Although serious statutory violations of FISA would likely amount to a violation of the Fourth Amendment, this would not necessarily be true for all such violations. A *Bivens* plaintiff would also need access to the particular facts of his case in order to identify the individual responsible for the violation. See *Fed. Deposit Ins. Corp. v. Meyer*, 510 U.S. 471 (1994) (holding that *Bivens* actions may only be brought against the individual officer).

Similar factual obstacles would face a FTCA plaintiff who is required to allege narrow and particular tortious conduct. See 28 U.S.C. § 2674 (2000) ("The United States shall be liable, respecting the provisions of this title relating to tort claims, in the same manner and to the same extent as a private individual under like circumstances . . ."); 28 U.S.C. § 2680 (Supp. I 2002) (exempting broad categories of tortious conduct from liability).

185. It is significant that the claims procedure actually eliminates litigation obstacles for both *Bivens* and FTCA plaintiffs. See *supra* note 184. With respect to *Bivens* plaintiffs, it would remove the difficult requirement that the victim identify the individual directly responsible for the violation. In many cases, the FISA system itself will be responsible for the violation rather than any particular individual. Even if the victim could successfully identify an individual defendant, qualified immunity, and perhaps even absolute immunity, would pose a major obstacle to relief in light of the nature of the violations. See *Harlow v. Fitzgerald*, 457 U.S. 800, 812 (1982) ("For aides entrusted with discretionary authority in such sensitive areas as national security or foreign policy, absolute immunity might well be justified to protect the unhesitating performance of functions vital to the national interest.").

possesses sufficient factual information to state a claim, the action would be precluded by the elaborate and exclusive claims procedure.¹⁸⁶

The notice itself, aside from informing the individual that he has been subject to electronic surveillance under FISA, would also inform the individual that he is entitled to compensation if he chooses to file a claim. The claimant should be provided with: (1) the administrative filing details; (2) the statute of limitations;¹⁸⁷ (3) the fact that the remedy is

With respect to FTCA claims, the claimant would not need to satisfy stringent procedural requirements, *see* 28 U.S.C. § 2675 (2000), or show that the governmental conduct met particular substantive requirements, *see supra* note 184.

186. Most recently, the Supreme Court has expressed a staunch unwillingness to imply *Bivens* actions absent a showing that the plaintiff has no other remedy available. *See* *Corr. Serv. Corp. v. Malesko*, 534 U.S. 61, 74 (2001) (“In sum, respondent is not a plaintiff in search of a remedy as in *Bivens* and *Davis* [*v. Passman*, 442 U.S. 228 (1979)].”). Because the plaintiff here would clearly have an alternate remedy, his action would be precluded under this standard. Prior to *Malesko*, the Court found *Bivens* actions precluded where Congress provided for elaborate remedial mechanisms found to be constitutionally adequate, even though they were not as desirable or complete as the *Bivens* remedy and even though Congress did not specify that the remedy provided would be exclusive. *See* *Schweiker v. Chilicky*, 487 U.S. 412 (1988) (holding that the elaborate remedial system provided by the Social Security Act provided meaningful remedies and safeguards for those in the plaintiff’s position and therefore precluded a *Bivens* action); *Bush v. Lucas*, 462 U.S. 367 (1983) (holding that the Civil Service Commission’s Appeals Review Board was an elaborate remedial system providing plaintiffs with an adequate remedy sufficient to preclude a *Bivens* action). Because the claims procedure here would be expressly exclusive and would provide an adequate remedy for those claiming violations of the Fourth Amendment, a *Bivens* action would be precluded. Such an action would be precluded for the same reasons even under the generous standard articulated in *Bivens*. *Bivens*, 403 U.S. at 397 (“For we have here no explicit congressional declaration that persons injured by a federal officer’s violation of the Fourth Amendment may not recover money damages from the agents, but must instead be remitted to another remedy, equally effective in the view of Congress.”); *see also* *Carlson v. Green*, 446 U.S. 14, 18-19 (1980) (finding a *Bivens* action precluded when Congress provided an alternative remedy which it explicitly declared to be a *substitute* for recovery directly under the Constitution).

With respect to the FTCA, Congress may preempt its availability by expressly declaring the claims procedure to be the exclusive remedy against the United States. *See* *Johansen v. United States*, 343 U.S. 427, 441 (1966) (“As the government has created a comprehensive system to award payments for injuries, it should not be held to have made exceptions to that system without specific legislation to that effect.”); *see, e.g., Lockheed Aircraft Corp. v. United States*, 460 U.S. 190, 193-94 (1983) (“FECA’s exclusive liability provision . . . was designed to protect the Government from suits under statutes, such as the Federal Tort Claims Act, that had been enacted to waive the Government’s sovereign immunity. . . . This compromise is essentially the same as that found, for example, in the Longshoremen’s and Harbor Workers’ Compensation Act (LHWCA).”); *United States v. Demko*, 385 U.S. 149, 152 (1966) (finding FTCA claims brought by injured federal prisoners preempted by an exclusive compensation statute); *Pueschel v. Mineta*, 369 F.3d 345, 348 (4th Cir. 2004) (“With regard to Pueschel’s FTCA suit, we hold that it was properly dismissed on preemption grounds given that Title VII establishes the exclusive and preemptive scheme under which federal employees can seek redress for employment discrimination.”).

187. If the majority of notified individuals file claims, it will be preferable for the FISC to compute damages when they make their liability determination. This would allow the FISC to destroy the non-foreign intelligence information at that point instead of waiting for the statute of limitations to lapse. Even if the FISC determines that it would be preferable to wait for a claim to be filed before assessing damages, the statute of limitations should be relatively short in order to

exclusive; (4) that the contents of the surveillance will not be disclosed; and (5) that there will be no opportunity to appear before the FISC or appeal the amount of damages awarded.

This claims procedure would, however, be subject to the Due Process Clause of the Fifth Amendment. The first issue in the procedural due process analysis is whether unlawful electronic surveillance constitutes a deprivation of liberty within the meaning of the Due Process Clause.¹⁸⁸

Because many of the errors described in Part III will be unintentional, these violations may not qualify as deprivations of liberty based on the Supreme Court's opinion in *Daniels v. Williams*.¹⁸⁹ The Court in *Daniels* held that lack of due care by state officials does not constitute a "deprivation" within the meaning of the Due Process Clause.¹⁹⁰ The Court stated, "[f]ar from an abuse of power, lack of due care suggests no more than a failure to measure up to the conduct of a reasonable person. To hold that injury caused by such conduct is a deprivation within the meaning of the Fourteenth Amendment would trivialize the centuries-old principle of due process of law."¹⁹¹ This distinction between negligent and intentional governmental misconduct would be unworkable under the claims procedure because the scope of section 1810 above would eliminate that distinction for purposes of notice and liability.¹⁹²

To further complicate this threshold issue, a plurality of the Supreme Court in *Albright v. Oliver* held that an arrest and prosecution without probable cause did not state a substantive due process claim because the Fourth Amendment, and not the Fourteenth Amendment, protected individuals from that particular governmental conduct.¹⁹³ A

minimize the retention of the non-foreign intelligence information. Further justifying a short filing period would be the fact that filing the claim would require minimal preparation on the claimant's behalf because liability has already been determined.

188. This analysis assumes that the right to be free from electronic surveillance implicates a constitutionally protected liberty interest. See *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting) ("[The Framers] conferred, as against the government, the right to be let alone – the most comprehensive of rights and the right most valued by civilized men.").

189. *Daniels v. Williams*, 474 U.S. 327 (1986).

190. *Id.* at 330-31.

191. *Id.* at 332.

192. The Court in *Daniels*, however, did note:

[T]hat injuries inflicted by governmental negligence are not addressed by the United States Constitution is not to say that they may not raise significant legal concerns and lead to the creation of protectible legal interests. The enactment of tort claim statutes, for example, reflects the view that injuries caused by such negligence should generally be redressed.

Id. at 333.

193. *Albright v. Oliver*, 510 U.S. 266, 273 (1994) (plurality opinion) ("Where a particular Amendment provides an explicit textual source of constitutional protection against a particular sort of government behavior, that Amendment, not the more generalized notion of substantive due

broad reading of *Albright* may support the proposition that unlawful electronic surveillance is not a deprivation of liberty within the meaning of the Due Process Clause because such surveillance is a search under the Fourth Amendment,¹⁹⁴ and therefore, that Amendment must afford all the process that is due. However, "the Fourth Amendment probable cause determination is in fact only the first state of an elaborate system, unique in jurisprudence, designed to safeguard the rights of those accused of criminal conduct."¹⁹⁵ Because the individual subject to unlawful electronic surveillance under FISA is not brought into the criminal justice system, that individual must look to the claims procedure to vindicate his rights instead of traditional Fourth Amendment safeguards. Therefore, despite the fact that electronic surveillance is governmental conduct protected by the Fourth Amendment, it may nonetheless constitute a deprivation of liberty within the meaning of the Due Process Clause because traditional Fourth Amendment protections would not be available in this context. Due to the complexities arising from *Daniels*, *Albright*, and the unusual nature of the claims procedure, the remainder of this section assumes that the claims procedure must satisfy due process.

The next issue then is whether there is a violation of due process by affording process after the deprivation has occurred.¹⁹⁶ In *Parratt v. Taylor*, an inmate at a state prison filed suit in federal court under 42 U.S.C. § 1983 alleging a deprivation of property without due process when the prison misplaced and lost hobby materials that the inmate

process, must be the guide for analyzing these claims.") (internal quotations and citations omitted)). This rationale would similarly preclude a substantive due process challenge to the FISA process. Even if such a claim went forward, the compelling governmental interests in gathering foreign intelligence information would likely prevail, even under heightened scrutiny. See *Haig v. Agee*, 453 U.S. 280, 307 (1981) ("It is obvious and unarguable that no governmental interest is more compelling than the security of the Nation. . . . Measures to protect the secrecy of our Government's foreign intelligence operations plainly serve these interests.") (internal quotations and citations omitted)).

194. See *Katz v. United States*, 389 U.S. 347 (1967).

195. *Ingraham v. Wright*, 430 U.S. 651, 698 (1977) (White, J., dissenting); see also *Gerstein v. Pugh*, 420 U.S. 103, 114 (1975) ("Accordingly, we hold that the Fourth Amendment requires a judicial determination of probable cause as a prerequisite to extended restraint of liberty following arrest.").

196. See *Cleveland Bd. of Educ. v. Loudermill*, 407 U.S. 532, 542 (1985) ("The root requirement of the Due Process Clause [is] that an individual be given an opportunity for a hearing *before* he is deprived of any significant property interest.") (internal quotations omitted)); *Ingraham*, 430 U.S. at 701 (Stevens, J., dissenting) ("To be sure, the timing of the process may be a critical element in determining its adequacy that is, in deciding what process is due in a particular context. Generally, adequate notice and a fair opportunity to be heard in advance of any deprivation of a constitutionally protected interest are essential. The Court has recognized, however, that the wording of the command that there shall be no deprivation 'without' due process of law is consistent with the conclusion that a postdeprivation remedy is sometimes constitutionally sufficient.").

ordered through the mail.¹⁹⁷ The Court held that the post-deprivation remedy provided by state tort law was adequate and therefore satisfied due process.¹⁹⁸ The Court reasoned that such post-deprivation process was permissible where the alleged deprivation was the result of a "random and unauthorized act by a state employee."¹⁹⁹ In those cases, "it is not only impracticable, but impossible, to provide a meaningful hearing before the deprivation" because the "[s]tate cannot predict precisely when the loss will occur."²⁰⁰ Three years later, the Court extended the rationale of *Parratt* in *Hudson v. Palmer* to intentional deprivations by state employees when the state could still not predict when such deprivations would occur.²⁰¹ And a few years later, the *Parratt-Hudson* doctrine was extended to deprivations of liberty as well as property.²⁰²

Whether the rationale underlying *Parratt* and *Hudson* permits a post-deprivation remedy in the present context depends on the feasibility of pre-deprivation process.²⁰³ Although the errors in Part III may be generally foreseeable, it would be impossible for the government to provide the individual with any notice or process capable of preventing the violation. The errors contributing to the deprivation here are both random and unauthorized as these terms are used in *Parratt* and *Hudson*;

197. *Parratt v. Taylor*, 451 U.S. 527 (1981).

198. *Id.* at 543-44.

199. *Id.* at 541.

200. *Id.*

201. *Hudson v. Palmer*, 468 U.S. 517, 533 (1984) ("The state can no more anticipate and control in advance the random and unauthorized intentional conduct of its employees that it can anticipate similar negligent conduct."). *Daniels* overruled *Parratt* on the issue of whether negligent governmental conduct may constitute a deprivation of liberty. See *supra* notes 185-187 and accompanying text.

202. *Zinermon v. Burch*, 494 U.S. 113, 132 (1990) ("But the reasoning of *Parratt* and *Hudson* emphasizes the State's inability to provide predeprivation process because of the random and unpredictable nature of the deprivation, not the fact that only property losses were at stake."). It is worth noting that prior to *Parratt*, *Hudson*, and *Zinermon*, the Court held in *Ingraham* that state common law remedies available to students *after* they were subject to paddling, a constitutional deprivation of liberty, were sufficient to satisfy due process. *Ingraham v. Wright*, 403 U.S. 651, 682 (1977).

203. *Zinermon*, 494 U.S. at 132 ("[T]he reasoning of *Parratt* and *Hudson* emphasizes the state's inability to provide predeprivation process. . . ."). Limiting the application of *Parratt* to state deprivations is not central to its rationale. See Rodney A. Smolla, *The Displacement of Federal Due Process Claims by State Tort Remedies: Parratt v. Taylor and Logan v. Zimmerman Brush Company*, 1982 U. ILL. L. REV. 831, 881-83 (1982) ("*Parratt* was decided with reference to actions against state officers and agencies, but it should apply with equal force to deprivations of property or liberty by federal officials, whenever federal law establishes judicial or administrative remedies that are adequate to compensate the victim. . . . At both the federal and state level, *Parratt* could be legitimately invoked to bar a section 1983 or *Bivens* claim in cases in which administrative or judicial remedies other than compensatory tort mechanisms provide an individual with adequate relief."); see also *Weiss v. Lehman*, 676 F.2d 1320 (9th Cir. 1982) (holding that the Federal Torts Claims Act was an adequate remedy under *Parratt* for actions taken by a federal official).

even though the government may be aware that such incidents may occur, it is not capable of determining the precise instances where, for example, technology will fail or clerical errors will lead to surveillance of the wrong phone number. Because it is simply not possible to predict these specific incidents and provide pre-deprivation process, a post-deprivation remedy would not violate due process.

When post-deprivation process is permissible under *Parratt*, the remedy must be adequate in order to satisfy due process. The balancing test of *Mathews v. Eldridge* generally determines whether the process afforded by the state is sufficient,²⁰⁴ but:

Parratt and *Hudson* represent a special case of the general *Mathews v. Eldridge* analysis, in which postdeprivation . . . remedies are all the process that is due, simply because they are the only remedies the state could be expected to provide. . . . Thus, *Parratt* is not an exception to the *Mathews* balancing test, but rather an application of that test to the unusual case in which one of the variables in the *Mathews* equation – the value of predeprivation safeguards – is negligible in preventing the kind of deprivation at issue. Therefore, no matter how significant the private interest at stake and the risk of erroneous deprivation, the State cannot be required constitutionally to do the impossible by providing predeprivation process.²⁰⁵

Therefore, instead of analyzing the claims procedure under *Mathews*, all that *Parratt* requires is that the claims procedure provide for an adequate post-deprivation remedy.²⁰⁶

The Court in *Parratt* found the state law remedies adequate because they “could have fully compensated the respondent for the property loss he suffered.”²⁰⁷ Despite the fact that the “state remedies may not provide the respondent with all the relief which may have been available if he could have proceeded under § 1983, that does not mean that the state remedies are not adequate to satisfy the requirements of due process.”²⁰⁸

204. *Mathews v. Eldridge*, 424 U.S. 319, 335 (1976) (“[D]ue process generally requires consideration of three distinct factors: First, the private interest that will be affected by the official action; second, the risk of an erroneous deprivation of such interest through the procedures used, and the probable value, if any, of additional or substitute procedural safeguards; and finally, the Government’s interest, including the function involved and the fiscal and administrative burdens that the additional or substitute procedural requirement would entail.”).

205. *Zinerman*, 494 U.S. at 128-29 (internal citations omitted).

206. *Parratt* does not require or even suggest that the adequate post-deprivation remedy must come in the form of tort law. See Smolla, *supra* note 203, at 883 (“Although *Parratt* dealt with tort remedies as the alternative and adequate process due to an individual deprived of liberty or property, *Parratt*’s rationale is sufficiently expansive to encompass within the concept of adequacy a range of remedial systems substantially broader than the law of torts.”).

207. *Parratt v. Taylor*, 451 U.S. 527, 544 (1981).

208. *Id.*; *Hudson v. Palmer*, 468 U.S. 517, 535 (1984) (“[T]hat Palmer might not be able to recover under these remedies the full amount which he might receive in a § 1983 action is not . . . determinative of the adequacy of the state remedies.”). It has been suggested that *Parratt*

In this case, the claims procedure would fully compensate the claimant for statutory violations that previously had been completely unrecoverable. Furthermore, it would actually make such recovery easier than if the claimant had been forced to use traditional remedial avenues.²⁰⁹ First, the FISC would have conveniently determined liability in the claimant's favor before he even files the claim. Second, contrary to many post-deprivation remedies that impose additional obstacles, most notably immunity for governmental officials,²¹⁰ the claims procedure *removes* such obstacles for the claimant. This would be an exceptionally easy case for determining the adequacy of the remedy because the government is not attempting to statutorily limit its liability. Instead, it is striving to create a new and automatic avenue of relief where no remedy was previously available. Because the claims procedure would fully compensate victims of statutory violations who previously had no avenue for relief and would remove litigation obstacles for those individuals, this claims procedure must be considered adequate under *Parratt*'s deferential standard of review.²¹¹

Even considering the *Mathews* factors, the inability of the claimant to appear before the FISC or appeal the damages awarded would not compel a contrary result. While the opportunity to be heard is generally a critical aspect of due process, above all else "[d]ue process is flexible and calls for such procedural protections as the particular situation demands."²¹² Hearings are most appropriate when an individual's factual showing can prevent the anticipated deprivation.²¹³ In this situation, however, there is no reason to have the claimant appear before the FISC because the deprivation is complete and the FISC, in determining liability and assessing damages, is acting on the claimant's behalf. The notified individual would have nothing to challenge but the amount of damages awarded by the FISC. The governmental interests in maintaining the secrecy of the FISA process and protecting methods of gathering intelligence would outweigh the risk of erroneous deprivation with

announced a highly deferential standard of review with respect to the adequacy of post-deprivation remedies. See Smolla, *supra* note 203, at 878 ("*Parratt* will thus permit states considerable license to develop their own tort rules, including highly restrictive statutes of limitations and doctrines of immunity, but a modicum of investigation into the 'adequacy' of those tort rules will remain.").

209. See *supra* notes 184-85.

210. See Smolla, *supra* note 203, at 871 ("One of the most difficult problems to be addressed after *Parratt* involves the role of immunities in the adequacy determination.").

211. See *supra* note 208.

212. *Mathews v. Eldridge*, 424 U.S. 319, 334 (1976) (quoting *Morrissey v. Brewer*, 408 U.S. 471, 481 (1972)).

213. See, e.g., *Goldberg v. Kelly*, 397 U.S. 254 (1970) (holding that a pre-termination hearing is required for welfare recipients).

respect to the amount of damages awarded by the FISC, the same independent judicial body that would already have determined the issue of liability in the claimant's favor.²¹⁴

The absence of an opportunity to appeal the damages awarded is further justified by the separation of powers. This is the same logic that requires the FISC, an Article III court, to determine whether the executive branch should be liable for its actions. "The 'adequacy' concept, particularly when applied to . . . compensation systems, should be relatively deferential, but elemental notions such as conflict of interest, separation of powers, and accountability must remain as minimums below which states may not go."²¹⁵ Although it is possible that the FISC could determine liability in a claimant's favor only to subsequently award damages incommensurate with the violation, separation of powers dictates that this risk does not outweigh the same governmental interests that preclude the claimant from filing his claim in federal court and appearing before the FISC.

In sum, even if there was a deprivation of a constitutionally protected interest, the claims procedure satisfies due process. The unpredictability of the violations would permit the post-deprivation remedy, and the remedy would fully compensate claimants for the violations, thus satisfying the adequacy standard under *Parratt*. This conclusion is further supported by the flexibility of due process, which would recognize the unique context of the claims procedure, respect the sensitive governmental interests at stake, and uphold the voluntary efforts by the government to remedy statutory violations affecting personal privacy. It would indeed be ironic if the requirements of due process invalidated the government's first affirmative effort to effectuate civil liability under FISA.

VII. CONCLUSION

A. *Specific Proposals of this Note*

The proposed measures in this Note are admittedly imperfect and peculiar. These attributes, however, merely reflect the FISA process itself. When asked at his Senate confirmation hearing about the potential responsibility of appointing members to the FISC, then-Judge Roberts remarked, "I'll be very candid. When I first learned about the FISA court, I was surprised. It's not what we usually think of when we think

214. See *Hamdi v. Rumsfeld*, 542 U.S. 507, 533 ("In the words of *Mathews*, process of this sort would sufficiently address the 'risk of erroneous deprivation' of a[n] [individual's] liberty interest while eliminating certain procedures that have questionable additional value in light of the burden on the Government.").

215. Smolla, *supra* note 203, at 885-86.

of a court. . . . This is a very different and unusual institution.”²¹⁶ It should therefore be no surprise that the deficiencies of the unique and secretive FISA process require a compensatory scheme with similar attributes.

Continuing his testimony with respect to the FISC, Roberts went on:

But it does seem to me that the departures from the normal judicial model that are involved there put a premium on the individuals involved. I think the people who are selected for that tribunal have to be above reproach. There can't be any question that these are among the best judges that our system has, the fairest judges, the ones who are most sensitive to the different issues involved, because they don't have the oversight of the public being able to see what's going on.²¹⁷

During one of the Senate Judiciary Committee's NSA hearings, both Senator Specter and Attorney General Gonzales appeared to agree that the judges possessed these characteristics:

SPECTER: Mr. Attorney General, starting with the FISA Court: well-respected, maintains secrecy, experienced in the field – and I posed this question to you in my letter – why not take your entire program to the FISA Court within the broad parameters of what is reasonable and constitutional and ask the FISA Court to approve it or disapprove it?

GONZALES: Senator, I totally agree with you that the FISA Court should be commended for its great service

SPECTER: Well, speaking for myself, I would urge the President to take this matter to the FISA Court. They're experts. They'll maintain the secrecy.²¹⁸

If the judges on the FISC are indeed trustworthy, experienced, and competent, then there should be no hesitation to vest them with the additional powers that this Note proposes. Either the FISC can be trusted with these grave responsibilities or it cannot, but there should be no going half way.

To be sure, the proposals in this Note impose new duties on the FISC that will consume time and require increased effort. But rather than refer to these obligations as burdens, they should be recognized and

216. *The Nomination of John Roberts to be Chief Justice of the Supreme Court Before the S. Comm. on the Judiciary*, 109th Cong. (2005), available at <http://www.washingtonpost.com/wp-dyn/content/article/2005/09/13/AR2005091301469.html> (testimony of Hon. John G. Roberts Jr., Nominee for Chief Justice of the United States Supreme Court).

217. *Id.*

218. *Wartime Executive Power and the NSA's Surveillance Authority Before the S. Comm. on the Judiciary*, *supra* note 2, available at <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html> (statements of Sen. Arlen Specter, Chairman, S. Comm. on the Judiciary, and Alberto Gonzales, Attorney General).

appreciated for what they are: commitments to civil liberty. Regardless of whether the reader agrees with this Note's specific proposals, two things have become clear: first, helpless and oblivious Americans have been subject to unlawful electronic surveillance under FISA; and second, citizens can no longer rely solely on preventive measures if anything is to be done about it. FISA represents a fragile balance between national security interests and civil liberties.²¹⁹ As errors in the FISA process continue to upset this delicate balance, and as the use of electronic surveillance intensifies with the War on Terror, it is time to finally consider adopting affirmative measures that will provide relief for the civil liberties that are sacrificed.

B. *Informing the Broader Debate About Judicial Oversight*

Examining the notice problem, unlawful electronic surveillance, and civil liability under FISA should inform the broader debate and disagreement regarding the role of the judiciary in the foreign intelligence surveillance process.

To reiterate this Note's introductory points, the errors documented in Part III do not support the argument that the FISA process should be eliminated. Rather, they illustrate that the imperfections in the process can be more efficiently monitored, prevented, and documented by strengthening judicial oversight. It has not been disputed that the substitution of the NSA program's freedom to wiretap without judicial oversight for FISA's probable cause and certification requirements would drastically exacerbate the number and severity of civil liberty violations.²²⁰ This is simply a practical application of checks and balances.

Even if one disagrees with the proposals suggested in Parts IV and V to reveal and remedy these errors, they still illustrate that the judiciary may be employed in new ways to fulfill its historic role of safeguarding individual liberties. Employing a return and notice procedure analogous to the one in Title III could not be accomplished if the courts were removed from the process. Nor could civil claims be brought before

219. See *supra* note 28 and accompanying text.

220. To be sure, the errors identified in Part III would technically no longer occur if FISA becomes optional or is eliminated; application process errors would not occur because there would be no requirement that the government submit an application, and implementation errors would not occur because there would be no requirement that the government implement a court order. This illustrates the paradoxical conclusion that the existence of errors has some positive value because they reflect the presence of a constraining authority. Preventing errors by eliminating the statutory requirements does nothing to further civil liberty interests.

courts that had no access to or familiarity with the process. The moment that the judiciary is removed from the equation, not only will the number and severity of civil liberty violations increase, but the options available to remedy them will greatly diminish.