Loyola of Los Angeles Law Review

Volume 39
Number 4 *Symposium: Celebrity Prosecutions*

Article 10

12-1-2006

An Enemy of Freedom: United States v. James J. Smith and the Assault on the Fourth Amendment

Kelly J. Smith

AN ENEMY OF FREEDOM: *UNITED STATES V. JAMES J. SMITH* AND THE ASSAULT ON THE FOURTH AMENDMENT

I. INTRODUCTION

Much has been written about the changes in our society's approach to law enforcement in the wake of the events of September 11, 2001.[1] Media and scholarly journals have discussed at length amendments to existing statutes, such as the Classified Information Procedures Act ("CIPA"),[2] and completely new statutory schemes,

---

1. *E.g.*, William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. MIAMI L. REV. 1147, (2003); John E. Branch III, *Statutory Misinterpretation: The Foreign Intelligence Court of Review's Interpretation of the "Significant Purpose" Requirement of the Foreign Intelligence Surveillance Act*, 81 N.C. L. REV. 2075, (2003); 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); Nathan C. Henderson, *The Patriot Act's Impact on the Government's Ability to Conduct Electronic Surveillance of Ongoing Domestic Communications*, 52 DUKE L.J. 179 (2002); David S. Jonas, *The Foreign Intelligence Surveillance Act Through the Lens of the 9/11 Commission Report: The Wisdom of the Patriot Act Amendments and the Decision of the Foreign Intelligence Surveillance Court of Review*, 27 N.C. CENT. L.J. 95, (2005); Craig S. Lerner, *The USA Patriot Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement*, 11 GEO. MASON L. REV. 493 (2003); Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234 (2003); Paul Rosenzweig, *Civil Liberty and the Response to Terrorism*, 42 DUQ. L. REV. 663 (2004); Jeremy C. Smith, *The USA PATRIOT Act: Violating Reasonable Expectations of Privacy Protected by the Fourth Amendment Without Advancing National Security*, 82 N.C. L. REV. 412, (2003); George P. Varghese, *A Sense of Purpose: The Role of Law Enforcement in Foreign Intelligence Surveillance*, 152 U. PA. L. REV. 385, (2003).

2. Act of Oct. 15, 1980, Pub. L. No. 96-456 (providing certain pretrial, trial, and appellate procedures for criminal cases involving classified

such as the USA Patriot Act ("Patriot Act").[3] Names like Hamdi, Padilla, and Moussaoui have appeared in cases that have bounced back and forth through the federal courts. These cases have tested the constitutional rights of defendants under these amended and new statutory schemes.[4]

However, few Americans understand the breadth of the laws that give the U.S. government an avenue to secretly invade every aspect of their lives. Through a secret court known as the Foreign Intelligence Surveillance Court ("FISC"), the government may apply *ex parte* for permission to tap our phones, read our mail and e-mail, track our cars, place microphones in our homes and cars, view our library records and financial information, and follow us wherever we go. And, it is extraordinarily easy for the government to get permission to do so.

While the Foreign Intelligence Surveillance Act ("FISA")[5] was originally passed into law as a *protection* against abuses by the federal government against its own citizens,[6] the federal government has relied heavily upon FISA to spy on its own citizens in hopes of gaining information to use in criminal prosecutions. In order to understand how the government uses a statutory scheme originally designed to *protect* U.S. citizens from warrantless surveillance to now spy on U.S. citizens during a current criminal investigation, this article examines the changes the Patriot Act made to FISA, and in particular, how the newly revised statutes can be used in a specific criminal investigation. Additionally, specific court documents and motions relating to FISA prosecutions will detail what the Patriot Act's changes to FISA mean for defendants subject to surveillance under these statutes.

A perfect case to examine the nuances of FISA is *United States v. James Jay Smith.*[7] Using the surveillance techniques granted to

---

information).

3. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA Patriot Act) of 2001, Pub. L. No. 107-56 (2001).

4. *See* Hamdi v. Rumsfeld, 542 U.S. 507 (2004); Rumsfeld v. Padilla, 542 U.S. 426 (2004); United States v. Moussaoui, 33 F.3d 509 (2003).

5. 50 U.S.C. §§ 1801–1871 (2005).

6. *See infra* p. 36.

7. United States v. James J. Smith, No. CR 03-428-FMC (C.D. Cal. Apr.

them under a FISA warrant, in April 2002, the Federal Bureau of Investigation ("FBI") arrested and indicted James Jay Smith ("Smith"), a U.S. citizen. Smith is a United States Army veteran of the Vietnam War and a thirty-year veteran of the FBI. He was arrested on charges of gross negligence in the handling of classified documents.[8] At the outset, it should be noted that the author is directly related to James Smith, and his communications were also monitored during Smith's FISA surveillance. He attempts to remain as unbiased as possible in the discussion of this case and of FISA.

This note uses *United States v. James Jay Smith* to demonstrate the potential abuses of the FISC and of FISA. In particular, it details: (1) the history of the case using publicly available court documents, court transcripts, and newspaper articles; (2) the available investigative techniques under FISA that were used in *Smith*; (3) the potential abuses of FISA; (4) the recent developments in domestic surveillance; and (5) the ways in which the laws could be modified to deal directly with privacy and abuse concerns.

The potential for FISA and Fourth Amendment abuses are staggering. The scales favor the government from the outset of the FISA application process. For example, in order to receive FISC authorization to conduct invasive surveillance and monitoring of a subject, the government only needs to meet an extremely low standard during its *ex parte* proceeding.[9] Additionally, because the Patriot Act broadened the scope of FISA surveillance, the government can argue more easily for the eligibility of potential subjects.[10] Those subjects are never told that they, members of their families, or friends will also be monitored under FISA surveillance.[11] Limiting the breadth of surveillance would require constant attention by FBI agents. FISA surveillance easily can pick up and record calls made by people who are not under investigation, including privileged conversations, such as attorney-client or spousal communications.[12]

Also, the government need not have foreign intelligence as the primary reason for its investigation. The FISC still will approve the

---

8, 2003).

8. 18 U.S.C. § 793(f) (2005); *see also id.*

9. *See* 50 U.S.C. § 1805(a) (2005).

10. *See infra* Part III.B.1.

11. *See* 50 U.S.C. §§ 1806(c), 1825(d).

12. *See infra* Part III.B.6.

government's application for surveillance even if the government's primary focus is a criminal investigation.[13] When the investigation reaches trial, unless the government intends to use FISA surveillance information in a criminal proceeding, the government need not disclose that the targeted individual was a FISA surveillance subject.[14] And, even if the government does intend to offer the information as evidence, because the FISA warrant is classified, it is not easily subject to constitutional review by defense attorneys.[15] Even if all parties have the necessary security clearances, the government argues strenuously against disclosure of FISA affidavits and applications. As a result, massive surveillance of a subject is rarely, if ever, tested in an open proceeding in a court of law. Abuses will not be discovered, and multiple violations of a defendant's rights can occur without any remedy.

Although the potential for abuse is enormous, a simple solution exists to ensure the rights of defendants subject to surveillance under the auspices of FISA. This paper proposes that Congress ban all *ex parte* applications to the FISC except in times of emergency and create a division of the Federal Public Defender's Office with the sole purpose of ensuring that adequate probable cause exists to issue a FISA warrant against a U.S. citizen.

II. THE HISTORY OF UNITED STATES V. JAMES JAY SMITH AND UNITED STATES. V. KATRINA LEUNG

When Smith and Katrina Leung ("Leung") were arrested, the media produced sensationalized headlines, the FBI produced ferocious press releases, and the media portrayed the zeal with which the U.S. Attorney's Office decided to prosecute the case.[16] The FBI Director stated Smith "betrayed his country," and the FBI was quick to use Smith to show that it could police its own agents and prevent wrongdoing.[17] The U.S. Attorney's Office did not spare the public the more salacious details of Smith's conduct over the past twenty years in its affidavits and indictments, including a long-term affair

13. *See infra* pp. 68–70.

14. *See infra* pp. 31, 42.

15. *See infra* p. 70.

16. Greg Krikorian, David Rosenzweig & K. Connie Kang, *Ex-FBI Agent Is Arrested in China Espionage Case*, L.A. TIMES, Apr. 10, 2003, at B1.

17. *Id.*

with Leung.[18] Smith and Leung were depicted as intense threats to national security, and the U.S. Attorney's Office promised a thorough and diligent prosecution to determine how much damage had been done to national security as a result of their conduct.[19]

As a result of the FBI and U.S. Attorney's Office's zeal to protect national security, both agencies repeatedly violated both defendants' rights throughout the investigation.

A. Background and Overview

On April 8, 2003, Special Agent Randall Thomas of the Los Angeles Division of the FBI gave sworn testimony that would form the necessary support to arrest Smith and search his home.[20]

Smith began his FBI career in Salt Lake City, Utah in October 1970.[21] In 1971, Smith was transferred to the FBI's Los Angeles Division.[22] In July 1978, Smith was assigned to a Foreign Counterintelligence ("FCI") Squad focusing on the People's Republic of China ("PRC"), where he worked until his retirement in November 2000.[23] Smith was the Acting Supervisor of the FCI China Squad from March 1983 through October 1983, and was also a Relief Supervisor throughout the 1990s.[24] He also became the Supervisory Special Agent ("SSA") of the squad in 1996 until his retirement.[25] As a supervisor, Smith had access to classified materials as both an agent and as a supervisory agent.[26]

In the probable cause section of the affidavit, Agent Thomas detailed the activities of Katrina Leung, an FBI "asset" providing information about the PRC from the early 1980s until 2002.[27] Smith was the FBI agent who recruited her and was her primary handler

18. Indictment, United States v. James J. Smith, No. CR-03-429-M (C.D. Cal. May 7, 2003).

19. Krikorian, Rosenzweig & Kang, *supra* note 16.

20. Complaint for Violation of Title 18, United States Code, Section 793(f), United States v. James J. Smith, No. CR 03-428-FMC (C.D. Cal. Apr. 8, 2003) [hereinafter Smith Complaint].

21. *Id.* at 7.

22. *Id.*

23. *Id.*

24. *Id.* at 8.

25. *Id.*

26. *Id.*

27. *Id.* at 3.

until he retired from the FBI in November 2000.[28] Agent Thomas declared that Smith would debrief Leung at her residence and, on occasion, would take classified documents along and leave them unattended in his unlocked briefcase.[29] Agent Thomas stated that Leung surreptitiously photocopied some of these documents without Smith's knowledge, and that the FBI had obtained some of these documents from Leung's home.[30]

In addition, Agent Thomas revealed that the FBI investigation uncovered evidence that a sexual relationship between Smith and Leung began in the early 1980s and lasted until December 2002.[31] Agent Thomas also asserted that Smith learned in 1991 that Leung was providing classified information to PRC intelligence services without FBI authorization.[32]

1. Timeline of the Investigation

Beginning in April of 2002, Smith was subject to surveillance under the auspices of FISA.[33] The FISC's warrant allowed FBI agents to engage in covert physical searches of Smith's home, to wiretap, intercept, and record telephone and fax communications, and to intercept email.[34] In addition, the investigation also included physical surveillance that did not require the FISC's authorization.[35] On November 5, 2002, Agent Thomas participated in a FISC-authorized electronic surveillance of Smith and Leung having sexual relations in a Los Angeles hotel.[36]

On November 11, 2002, Agent Thomas participated in a FISA-authorized covert search of Leung's luggage at Los Angeles International Airport ("LAX") prior to her departure for the PRC.[37] Agents found a facsimile cover sheet from Smith to Leung.[38] The

28. *Id.* at 8.
29. *Id.* at 3.
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.* at 9.
34. *Id.*
35. *Id.*
36. *Id.* at 17.
37. *Id.* at 16.
38. *Id.*

second page included six photos from an October 2002 meeting of the Society of Former Special Agents of the FBI, including photos of active-duty agents.[39] On November 25, 2002, Agent Thomas engaged in another FISA-authorized covert search of Leung's luggage at LAX when she returned from the PRC.[40] The photos were not in her luggage.[41]

On December 11, 2002, Assistant Section Chief ("ASC") Bruce Carlson interviewed Leung at her residence.[42] During that interview, Leung voluntarily provided ASC Carlson with certain items she and Smith had discussed earlier that day.[43] Leung voluntarily removed a document from her bedroom safe and provided it to ASC Carlson.[44] Leung admitted that she obtained the document from Smith without his knowledge approximately twelve years earlier.[45] The document was an excerpt or transcript of a conversation between Leung and her Chinese "handler."[46]

The day after that, Agent Thomas participated in a limited consensual search of Leung's home, finding a Los Angeles FBI telephone directory dated December 20, 1994, a telephone list of agents assigned to a code-named FBI investigation, a classified FBI memo regarding Chinese fugitives dated June 12, 1997, and a FBI Legal Attaché Directory dated March 17, 1994.[47]

Four days later, upon review of classified documents in the Los Angeles Secure Compartmented Information Facility ("SCIF"), agents found that the transcript contained verbatim portions of classified material.[48] In interviews spanning December 11 to December 17, 2002, Leung admitted to "sneak[ing]" the transcript from Smith without his knowledge, and that although Smith sometimes allowed her to review classified documents, he would not

39. *Id.*
40. *Id.* at 16–17.
41. *Id.* at 17.
42. *Id.* at 13.
43. *Id.* at 12.
44. *Id.*
45. *Id.*
46. *Id.*
47. *Id.* at 13–14.
48. *Id.* at 13.

allow her to retain them.[49] She also admitted to taking the telephone directory and generally admitted to taking and copying documents from Smith's open briefcase when he left it unattended.[50] She also admitted that she made handwritten notes of the copied files and disposed of the copies.[51] Leung stated that she had also previously made notes without copying documents from information Smith told her.[52] An interview between Leung and two FBI agents was also cited where Leung admitted to her and Smith's sexual relationship, beginning in the early 1980s.[53]

A week later, Agent Thomas swore an affidavit before a federal magistrate to apply for a warrant to search Leung's home and business for evidence of violations of various bankruptcy statutes and tax statutes.[54] The federal magistrate granted the requests.[55]

The FBI's San Francisco Counterintelligence Division accessed a top secret source who relayed the information found in both the top secret document and the five-page transcript found in Leung's home safe.[56] When San Francisco SSA William Cleveland, Jr. ("Cleveland") listened to the audio recording provided by the source, he recognized the voice on the tape as Leung's.[57] Cleveland notified Smith of the unauthorized contact with the Ministry of State Security ("MSS").[58] Smith traveled to San Francisco, telling Cleveland that he had no knowledge of Leung's unauthorized communications with the MSS.[59] Cleveland stated that he relied upon Smith as Leung's handler to appropriately address the problem, and before his next meeting with Smith and Leung, he asked Smith if the unauthorized communications had been addressed.[60] Smith assured Cleveland that

49. *Id.* 14–15.
50. *Id.* at 15.
51. *Id.* at 15–16.
52. *Id.* at 16.
53. *Id.* at 10.
54. *Id.* at 9–10.
55. *Id.* at 10.
56. *Id.* at 20.
57. *Id.*
58. *Id.* at 20. The MSS is an intelligence service of the PRC, conducting intelligence operations focusing on the United States intelligence community. *Id.* at 4.
59. *Id.* 20.
60. *Id.* at 21.

he had addressed the issue of the unauthorized communications.[61]

2. The Search Warrant

The information detailed above provided probable cause to obtain a warrant to investigate Smith's alleged violation of § 793(f)[62] (gross negligence in handling national defense information) and §§ 1343 and 1346[63] (deprivation of the right to honest services and wire fraud).[64] Using the warrant, agents searched and seized specific items from Smith's home.[65] Later, agents relied on the affidavit to obtain a warrant to arrest Smith at his home on April 9, 2003. Smith later pled not guilty.[66]

B. The Legal Proceedings Timeline

Both Leung and Smith were arrested at their homes in the early hours of April 9, 2003.[67] Leung was charged with the more serious crime of violating § 793(b),[68] the unauthorized access and willful retention of documents relating to the national defense.[69]

One month later, on May 7, 2003, the government detailed its case against Smith in its first indictment.[70] Counts One through Four, deprivation of honest services and wire fraud, alleged that Smith deprived the FBI of his honest services when he: 1) had an improper sexual relationship with Leung; 2) failed to report his inappropriate relationship with Leung to the FBI; 3) failed to make truthful and complete reports to the FBI concerning Leung's unauthorized contacts with the PRC; 4) filed as well as caused other agents to file reports which concealed and omitted negative information about Leung; and 5) mishandled information relating to

61. *Id.*
62. 18 U.S.C. § 793(f) (2005).
63. *Id.* §§ 1343, 1346.
64. Smith Complaint, *supra* note 20, at 24.
65. *Id.* at 24-25.
66. Krikorian, Rosenzweig & Kang, *supra* note 16.
67. *Id.*
68. 18 U.S.C. § 793(b).
69. Complaint for violation of Title 18, United States Code, Section 793(b), United States v. Katrina Leung, No. 03-0729-M (C.D. Cal. Apr. 8, 2003), at ¶ 34.
70. Indictment, United States v. James J. Smith, No. CR 03-429-M (C.D. Cal. May 7, 2003).

the national defense and classified information.[71]

The government alleged that the relationship "deprived defendant Smith of the required objectivity in evaluating the ongoing reliability of Katrina Leung."[72] The government also alleged that when Smith submitted a required periodic asset evaluation, he did not disclose the relationship, nor did he inform the FBI that Leung refused to submit to a polygraph examination when it was learned that Leung had unauthorized contact with an agent of the MSS.[73] The government alleged that, between 1991 and 2000, Smith did not disclose this information despite nineteen separate asset evaluation reports.[74]

Furthermore, the government alleged that on four separate occasions from September 22, 1998 to March 20, 2000, Smith sent his asset evaluations from the Los Angeles office to FBI headquarters in Washington, D.C. via wire transmissions, thereby violating the wire fraud statute.[75] Count Five alleged gross negligence in the handling of classified documents.[76]

One day after Smith's indictment, Leung was indicted on five separate counts relating to her unauthorized copying and retention of classified documents.[77] Count One, unauthorized copying of national defense information with reason to believe that it will injure the United States or benefit a foreign nation, alleged that Leung took and copied a document connected with national defense. The document was a memo that detailed a classified off-site location related to a previous FBI investigation.[78] Count Two alleged the authorized taking and copying of a "SECRET" document.[79] Counts Three through Five alleged the unauthorized possession and failure to return three separate documents: 1) the five-page transcript, 2) the memo regarding the past FBI investigation and classified offsite

71. *Id.* at 8.
72. *Id.* at 9.
73. *Id.* at 11, 12.
74. *Id.* at 11.
75. *Id.* at 11, 13–15.
76. *Id.* at 16.
77. Indictment, United States v. Katrina Leung, No. CR 03-434 (C.D. Cal. May 8, 2003).
78. *Id.* at 1–2.
79. *Id.* at 3.

location, and 3) the "SECRET" memo.[80]

Smith's lawyers filed a motion on November 26, 2003, detailing the classified documents they would be requesting to view in order to mount their defense under CIPA.[81] The motion consisted of thirty-two redacted pages before a single paragraph of text could be seen. The paragraph of text, however, referred only to intercepted cellular phone calls that cast no doubt on Leung's reliability and bona fides.[82] The remainder of the document was redacted. Presumably,[83] the document listed the specific pieces of classified evidence that Smith's attorneys would offer in his defense as well as the grounds for their admission under CIPA and the Federal Rules of Evidence ("FRE").

Foreshadowing the conclusion of the case, on December 17, 2003, government lawyers argued a motion that would have prohibited the two defense teams to speak to each other regarding documents that had already been disclosed to both sides.[84] Assistant U.S. Attorney ("AUSA") Emmick stated in court, "Smith knows everything. Smith knows all the secrets and has been communicating with his counsel for months."[85] Leung's attorney, Janet Levine ("Levine"), was "disparaged and insulted" by Emmick's statements. "We are not asking to go into Mr. Smith's head in any way, shape or form. All we are asking is to discuss with Mr. Smith's counsel discovery that both sides have received from the government. This is information that we are using to defend our client."[86] Judge Cooper agreed with Levine, granting the motion to

80. *Id.* at 4–5.

81. Defendant's First Notice Under § 5 Of The Classified Information Procedures Act, United States v. James J. Smith, No. CR 03-429-FMC (C.D. Cal. Nov. 26, 2003). Because the documents dealing with classified information (CIPA and FISA motions) were recently released to the public in redacted format, there will be gaps in the substance of these motions.

82. *Id.* at 33.

83. The author only has access to the redacted, unclassified versions of the recently released documents. All conjectures as to the redacted content of the motions or arguments of the attorneys are speculative and are not based on citable facts.

84. Linda Deutsch, *Lawyers Argue Motion About Discussing Documents in Spy Case*, VENTURA COUNTY STAR, Dec. 18, 2003, at A1.

85. *Id.*

86. *Id.*

allow discussion of information already disclosed to both parties.[87]

On the same day, Smith's lawyers filed a motion to compel production of FISC applications, orders, and related documents.[88] Smith's lawyers argued that the government had to produce the FISC applications for the following reasons. First, the surveillance conducted under FISA was not minimized, as required by FISA.[89] Thus, surveillance included privileged conversations between Smith and counsel, between Smith and his wife, and dozens of conversations and emails that were unrelated to the case or to foreign intelligence generally.[90] Second, the government asserted that, as a U.S. citizen,[91] Smith was "an agent of a foreign power"[92] who "knowingly engage[d] in clandestine intelligence gathering activities for or on behalf of a foreign power."[93] The government has yet to produce, however, any evidence of Smith knowingly collecting information for a foreign power. Finally, because of this lack of evidence, the FISC application contained "intentional or reckless material falsehoods or omissions."[94]

Smith's lawyers filed another, more detailed, FISA-related motion on January 28, 2004.[95] In addition to restating many of the

---

87. *Id.*

88. Notice of Motion and Motion of Defendant James J. Smith to Compel Production of Foreign Intelligence Surveillance Act Applications, Orders, and Related Documents, and Memorandum in Support, United States v. James J. Smith, No. CR 03-429-FMC (C.D. Cal. Dec. 17, 2003) [hereinafter Motion to Compel].

89. 50 U.S.C. § 1801(h) (2005) (defining minimization procedures for electronic surveillance); 50 U.S.C. § 1821(4) (defining minimization procedures for physical searches).

90. Motion to Compel, *supra* note 88, at 1–2.

91. 50 U.S.C. § 1801(i) (2005).

92. 50 U.S.C. § 1801(a)(1).

93. 50 U.S.C. § 1801(b)(2)(a).

94. Motion to Compel, *supra* note 88, at 8. For timeline purposes, the content of the FISA-related motions will be cursory only. The bulk of the FISA history and application to this specific case study will be discussed at length in Section III.

95. Notice of Motion and Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived from Foreign Intelligence Surveillance Act Surveillance, Memorandum in Support, and Declaration of John D. Cline, United States v. James J. Smith, No. CR 03-429-FMC (C.D. Cal. Jan. 28, 2004) [hereinafter Motion to Suppress].

original FISA motion's arguments, Smith's lawyers argued that FISA, on its face and as applied, violated the Fourth Amendment following the enactment of 2001 Patriot Act amendments.[96] Additionally, Smith argued that the "Fourth Amendment [r]equires a [t]raditional [w]arrant [s]upported by [c]riminal [p]robable [c]ause [u]nless the '[p]rimary [p]urpose' of the [s]urveillance is the [c]ollection of [f]oreign [i]ntelligence."[97] Further, Smith argued that "[t]he Supreme Court's '[s]pecial [n]eeds' [c]ases [d]emonstrate that the FISA '[s]ignificant [p]urpose' [p]rovision [v]iolates the Fourth Amendment."[98]

In an additional motion,[99] Smith argued that any evidence obtained through FISA-related surveillance of Leung should be suppressed for many of the same reasons contained in the first January 28, 2004 motion. Smith argued that he was also an "aggrieved person"[100] for FISA purposes since communications between he and Leung were intercepted during the Leung FISA surveillance and during FISA searches of Leung's home. Thus Smith had standing[101] to challenge the FISA surveillance and physical searches of Leung.[102]

Following Smith's motions, the government shifted its focus and narrowed its case, issuing a superseding indictment against Smith on February 24, 2004. Count One alleged violation of 18 U.S.C. §§ 1341, 1346 (mail fraud/deprivation of honest services).[103] Instead of alleging, as before, that Smith sent his periodic asset evaluations via wire, the new indictment alleged that Smith delivered via mail the

96. *Id.* at 8–11.

97. *Id.* at 11.

98. *Id.* at 20.

99. Supplemental Memorandum in Support of Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived from Foreign Intelligence Surveillance Act Surveillance, United States v. James J. Smith, No. CR-03-429-FMC (C.D. Cal. Jan. 28, 2004).

100. 50 U.S.C. § 1801(k) (2005); 50 U.S.C. § 1821(2).

101. United States v. Belfield, 692 F.2d 141, 146 n.21 (D.C. Cir. 1982) (finding that a person incidentally overheard during FISA surveillance of another target is an "aggrieved person").

102. *See* 50 U.S.C. §§ 1806(e)–(g), 1825(f)–(h) (defining proper methods for challenging surveillance and physical searches undertaken pursuant to FISA).

103. First Superseding Indictment at 9, United States v. James J. Smith, No. CR 03-429(A)-FMC (C.D. Cal. Feb. 24, 2004).

results of an official security investigation[104] where Los Angeles FBI officials asked Smith, while not under oath, if he was aware of any current or past circumstances in his life which could have a bearing on his suitability for employment.[105]

Count Two also contained a new charge, a violation of 18 U.S.C. § 1001 (false statement to a federal agency).[106] Allegedly, Smith failed to disclose his improper sexual relationship with Leung to the interviewing agent.[107] Counts Three and Four remained the same, alleging violations of 18 U.S.C. § 793(f). The indictment, however, now included two counts of gross negligence against Smith.[108]

The next day, on February 25, 2005, the government argued a motion filed a month earlier that surprisingly abdicated any right it may have had to introduce any evidence gained from the FISA searches and wiretaps of Smith.[109]

Smith filed additional FISA-related motions to address the new charges against him on April 12, 2004.[110] The first motion objected to the government's responses to the original FISA-related defense motions regarding information gained from the Leung surveillance and searches.[111] The government filed two responses, one *ex parte* and classified, and one unclassified and shared with the defense.[112] The unclassified response did not address the intercepted attorney-client privileged communications between Smith and his lawyer.[113] The arguments contained in the motion were substantially the same

104. *Id.*
105. *Id.* at 14.
106. *Id.* at 15.
107. *Id.*
108. *Id.* at 16–17.
109. Government's Response to Defendant's Motion to Compel Production of FISA Applications, Orders, and Related Documents, United States v. James J. Smith, No. CR 03-429-FMC (C.D. Cal. Jan. 28, 2004).
110. Reply Memorandum in Support of Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived from Foreign Intelligence Surveillance Act Surveillance, United States v. James J. Smith, No. CR 03-429-FMC (C.D. Cal. Apr. 12, 2004) [hereinafter Reply in Support of Motion to Suppress].
111. *Id.* at 1.
112. *Id.*
113. *Id.*

as previous FISA-related motions.

Smith's second motion stated that the government had intercepted fifty-three privileged attorney-client conversations among Smith and his lawyers.[114] The government's purported protection of the attorney-client privilege was to have the calls retained, reviewed and transcribed by a "taint team" rather than by the "investigative team."[115] However, eight of the privileged conversations were produced to the "investigative team" and to Leung's defense team.[116]

Ultimately, the FISA questions were never decided. On May 12, 2004, Smith entered into a plea agreement with the government.[117] In exchange for dropping all other counts and providing extensive cooperation, Smith agreed to plead guilty to one count of 18 U.S.C. § 1001 (false statement to a federal agency).[118] It was speculated that, for his cooperation, Smith would serve no prison time even though he faced a maximum sentence of five years in federal prison.[119] Consequently, media outlets began to question the seriousness of the cases against Leung and Smith. "[F]ederal authorities have tried to lower expectations in the case since Smith and Leung's highly publicized arrests last year."[120] "[T]he FBI's investigation and other national security checks turned up no hard evidence that secrets had been compromised on a scale comparable to other recent espionage scandals—most notably . . . Robert Hanssen."[121] "[T]he message is clear that putting this agent in jail was not a priority for the government . . . and the outcome does seem contrary to the stated objective of the Justice Department of ferreting out corruption."[122]

Incredibly, in Smith's plea agreement,[123] the government

114. *Id.*

115. *Id.* at 2.

116. *Id.*

117. Greg Krikorian, *Handler of Alleged Spy Cuts Plea Deal*, L.A. TIMES, May 12, 2004, at B1.

118. *Id.*

119. *Id.*

120. Greg Krikorian, *Ex-FBI Agent Pleads to a Lesser Charge in Spy Case*, L.A. TIMES, May 13, 2004, at B1.

121. *Id.*

122. *Id.* (statement of Myles H. Malman, former federal prosecutor).

123. Plea Agreement for Defendant James J. Smith, United States v. James J. Smith, No. CR 03-429(A)-FMC (C.D. Cal. May 12, 2004).

mandated that Smith must not have any further contact with Leung or her counsel regarding *any* aspect of the continuing prosecution against Leung.[124]

Due to this highly unusual prohibition of not speaking with the only witness that could help exonerate Leung, attorneys for Leung made a motion on November 18, 2004, that asked Judge Cooper to dismiss all charges against Leung due to the illegal and unethical clauses contained within Smith's plea agreement.[125] Quickly, AUSA Lonergan sent a letter to Smith's attorneys explaining that the "no further sharing" clause was intended to limit defense counsel-to-counsel discussions, not to limit Smith's right to consent or decline to an interview with Leung's counsel.[126]

The media quickly got wind of the letter.[127] At the motion hearing on December 9, 2004, AUSA Emmick defended the plea agreement, calling the language "inartful," creating a possible mistaken impression that Smith could not talk to Leung's lawyers.[128]

In a tersely worded order filed January 6, 2005, Judge Cooper dismissed all charges against Leung.[129] Judge Cooper openly criticized the government, reminding them that the government "may not interfere with defense access to witnesses."[130] The government argued that the language in the plea agreement was ambiguous, that it never intended to restrict Smith's freedom to talk to Leung's defense counsel, and that the government cured any potential problem by explaining via a letter to Smith's attorneys that there was no restriction imposed.[131] The government's arguments were not persuasive to Judge Cooper.[132]

---

124. *Id.* at 7.

125. David Rosenzweig, *Lawyers for Alleged Spy Accuse Prosecution of Misconduct*, L.A. TIMES, Nov. 11, 2004, at B1.

126. Memorandum from Rebecca Lonergan re: United States v. James Smith, United States v. Katrina Leung (Nov. 24, 2004) (on file with author).

127. Gene Maddaus, *Ex-agent OK'd to Talk in Spy Case*, PASADENA STAR-NEWS, Nov. 30, 2004, at A1.

128. David Rosenzweig, *Alleged Spy's Lawyers Ask Dismissal of Case*, L.A. TIMES, Dec. 12, 2004, at B1.

129. Order Granting Defendant's Motion to Dismiss at 12, United States v. Katrina Leung, No. CR 03-434 FMC (C.D. Cal. January 6, 2005).

130. *Id.* at 2.

131. *Id.* at 3.

132. *Id.* at 3–7.

Judge Cooper concluded that the prosecution had "engaged in willful and deliberate misconduct, depriving defendant of her right of access to a critical witness in her defense,"[133] and that "[d]eliberate misconduct which rises to the level of a due process violation warrants dismissal of criminal charges if it results in substantial prejudice to the defendant."[134] In addition, Judge Cooper considered the effect that the plea agreement had on Smith, recognizing the fact that Smith faced five serious felony charges, and the possible sentence of many years in federal prison and the loss of his federal pension.[135] She also stated that she believed that, but for the government prohibition against contact with Leung's counsel, Smith would have consented to an interview with her defense counsel.[136]

Judge Cooper found that Leung suffered substantial prejudice, stating:

> [T]he witness is critical to the defense; the witness has everything to lose by defying the government's wishes with respect to Ms. Leung's case; the admonition against talking to the defense was not just an instruction from the prosecutor, but was made a condition of what the defense has accurately described as his 'sweetheart deal.'[137]

Judge Cooper dismissed all charges, stating that any lesser remedy would not right the harm done, and that the government "engaged in a pattern of stone-walling entirely unbecoming of a prosecuting agency."[138]

---

133. *Id.* at 7.

134. *Id.* at 8.

135. *Id.* at 9–10.

136. *Id.* at 9–10.

137. *Id.* at 10.

138. *Id.* at 12. U.S. Attorney Debra W. Yang ("Yang") issued a statement saying, "I stand behind the work of the prosecutors in this case and I know that they have conducted themselves ethically." She reserved the right not to comment on any possible appeal. David Rosenzweig, *Spying Case Tossed Out*, L.A. TIMES, Jan. 7, 2005, at B10. The government quickly filed a motion for reconsideration on February 4, 2005. Memorandum of Points and Authorities in Support of Motion for Reconsideration of Order Granting Defendant's Motion to Dismiss, United States v. Katrina Leung, No. CR 03-434-FMC (C.D. Cal. filed Feb. 4, 2005). The government, in unusually blunt language, denied any misrepresentations to the court, again reiterating that the Wallace e-mail did not apply to the "no further sharing" clause and that Leung

Judge Cooper continued to disagree with the government. On March 23, 2004, she affirmed her order for dismissal, rejecting the contention that she failed to consider material facts and stating that she considered them, but ultimately disagreed with them.[139]

On July 18, 2005, AUSA Lonergan argued for a two-month prison term for Smith, stating that Smith seriously endangered national security.[140] Lonergan also complained that Smith could not answer specific questions asked of him during his one hundred hours of interrogation post-plea bargain.[141] While acknowledging that Smith's lack of memory may have been "genuine," Lonergan stated that intelligence agents would spend many years assessing the damage.[142] Defense counsel Brian Sun countered the allegations, accusing the government of "backdooring" the national security issue into the case when the plea agreement contained no such admission.[143] Sun stated that the "case ha[d] been largely driven by politics, image, Washington and saving face for all concerned."[144] Sun also argued that Smith cooperated fully and to the best of his ability, stating that Smith was asked questions about events that had taken place over twenty years prior.[145] Ultimately, Smith was sentenced to three months of unmonitored house arrest, a $10,000 fine, and a three-year probationary sentence.[146]

On December 16, 2005, even though the government had an

---

did not suffer substantial prejudice since Smith was allowed to talk to Leung's counsel. *Id.* at 2–3. Incredibly, the motion stated that AUSA Emmick did not draft the plea agreement, and that the "inartful" language was submitted after consultation with management at the U.S. Attorney's Office and attorneys with the Department of Justice. *Id.* at 4. Also, the government chastised the court for revealing *in camera* documents (namely, the Wallace and Emmick emails), stating that it should have had the opportunity to contest the disclosure. *Id.* at 21–22.

139. Greg Krikorian, *Dismissal of Spy Case is Reaffirmed*, L.A. TIMES, Mar. 24, 2005, at B6.

140. David Rosenzweig, *Former FBI Agent Given Probation*, L.A. TIMES, July 19, 2005, at B3.

141. *Id.*

142. *Id.*

143. *Id.*

144. *Id.*

145. *Id.*

146. *Id.*

appeal pending before the Ninth Circuit arguing that Leung's dismissal was premature and unwarranted, the government accepted Leung's plea to two counts: making false statements to FBI agents and filing a bogus tax return in 2000.[147] In exchange, the government terminated all investigations against her.[148] Judge Cooper sentenced Leung to three years' probation, one hundred hours of community service, participation in FBI debriefings and a $10,000 fine.[149]

The sensational case against Smith and Leung ended, not with a flashy trial with lurid details of an affair and shocking disclosures of breaches of national security, but with plea bargains to the least serious crimes included in their indictments. The high-profile press conferences were conspicuously absent. The pride in the investigation and prosecution of Smith and Leung that the FBI and U.S. Attorney's Offices were so eager to show the world was gone. The government's case had failed to produce substantial convictions, and, in the end, the government got exactly what it needed in the first place—cooperation from the two defendants in the case to determine the damage, if any, to national security. In the wake of the government's failure, the relationships of the families and colleagues of Smith and Leung were forever changed. Their rights were trampled by a government determined to protect its national security interests. There appears to be no remedy for those abuses.

III. THE INVESTIGATIVE TECHNIQUES AND STATUTORY SUPPORT UNDER FISA[150]

What lessons can one take away from the prosecution of Smith and Leung? What does the outcome of these two cases mean for future subjects of FISA surveillance? In order to answer these questions, this article takes a closer look at the underlying statutes that give the government the awesome power to subject U.S. citizens to surveillance without producing a warrant that can be tested in an

147. David Rosenzweig, *Judge OKs Plea Deal in Spy Case*, L.A. TIMES, Dec. 17, 2005, at B3.

148. Stan Wilson, *Accused Double Agent Pleads to Tax Charge*, CNN, Dec. 16, 2005, http://www.cnn.com/2005/LAW/12/16/spy.compromise/index.html.

149. *Id.*

150. This section relies heavily on the Smith pleadings and motions for structure and content. Where appropriate, direct quotations have been made.

open court of law.

A. FISA History and Procedures

"FISA was enacted in 1978 to establish procedures for the use of electronic surveillance in gathering foreign intelligence information .... The Act was intended to strike 'a sound balance between the need for such surveillance and the protection of civil liberties.'"[151] FISA creates FISC to which the government must apply for an order authorizing electronic monitoring[152] or a physical search.[153]

First, the statute requires that FISC applications be approved by the Attorney General and contain certain information and certifications.[154] The application must contain "a statement of the facts and circumstances relied upon by the applicant to justify his belief that ... the target of the electronic surveillance is a foreign power or an agent of a foreign power."[155] An "agent of a foreign power," as applied to a "United States person"[156] means "any person who ... *knowingly* engages in clandestine intelligence gathering activities for or on behalf of a foreign power;"[157] "any person who[,] ... pursuant to the direction of an intelligence service or network of a foreign power, *knowingly* engages in any other clandestine intelligence activities for or on behalf of such foreign power;"[158] and "any person who ... *knowingly* aids or abets any person in the conduct of activities"[159] described above.

Second, the application to FISC must provide a "statement of the proposed minimization procedures."[160] The statute specifies the requirements for these procedures with respect to both electronic surveillance[161] and physical searches.[162] Third, the application must

151. *In re* Kevork, 788 F.2d 566, 569 (9th Cir. 1986).
152. 50 U.S.C. §§ 1803, 1804 (2005).
153. *Id.* § 1823.
154. *Id.* § 1804 (electronic monitoring); *id.* § 1823 (physical search).
155. *Id.* § 1804(a)(4)–(a)(4)(A) (same requirement for a physical search).
156. *Id.* § 1801(i).
157. *Id.* § 1801(b)(2)–(b)(2)(A) (emphasis added).
158. *Id.* § 1801(b)(2)–(b)(2)(B) (emphasis added).
159. *Id.* § 1801(b)(2)–(b)(2)(E) (emphasis added).
160. *Id.* § 1804(a)(5); *see id.* § 1823(a)(5) (same requirement for physical searches).
161. *Id.* § 1804(a)(5).
162. *Id.* § 1821(4).

contain certain "certifications" by an appropriate executive branch official.[163] Among other things, the official must certify "that a significant purpose of the surveillance is to obtain foreign intelligence information"[164] and "that such information *cannot reasonably be obtained by normal investigative techniques*."[165]

Fourth, the statute specifies what findings FISC must make before it can approve electronic monitoring[166] or a physical search.[167] FISC must find that the procedural requirements are satisfied,[168] including the minimization requirements, and that there is "probable cause to believe that . . . the target of the electronic surveillance is a foreign power or *an agent of a foreign power*."[169] When the target of the surveillance is a "United States person," FISC must determine that the government's certifications under § 1804 "are not clearly erroneous."[170]

Fifth, FISA provides that "[n]o otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character."[171]

Sixth, FISA authorizes any "aggrieved person" to "move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that . . . the information was unlawfully acquired [or] the surveillance was not made in conformity with an order of authorization or approval."[172]

FISA defines the phrase "aggrieved person" as "a person who is the target of an electronic surveillance or any other person whose communications or activities were subject to electronic

163. *Id.* § 1804(a)(7).

164. *Id.* § 1804(a)(7)(B); *see id.* § 1823(a)(7)(B) (same requirements for physical searches).

165. *Id.* § 1804(a)(7)(C); *see id.* § 1823(a)(7)(C) (same requirements for physical searches) (emphasis added).

166. *Id.* § 1805.

167. *Id.* § 1824.

168. *Id.* §§ 1805(a)(1), (2), (4).

169. *Id.* § 1805(a)(3)–(a)(3)(A); *see id.* § 1824(a)(3)–(a)(3)(A) (similar requirements for a physical search) (emphasis added).

170. *Id.* § 1805(a)(5); *see id.* § 1824(a)(5) (similar requirement for a physical search).

171. *Id.* § 1806(a).

172. *Id.* § 1806(e)–(e)(2); *see id.* § 1825(e) (similar provision for physical searches).

surveillance."[173] An "aggrieved person" for purposes of a physical search "means a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search."[174]

Lastly, § 1806(f) provides that, "if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States," the court deciding the motion must consider the application and order for electronic surveillance *in camera* to determine whether the surveillance was lawfully conducted.[175] "In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance."[176]

B. Abuses of FISA in the Smith Case

1. Traditional Probable Cause and the Amended FISA Requirements

"[FISA] is not to be used as an end-run around the Fourth Amendment's prohibition of warrantless searches."[177] Courts have interpreted the Fourth Amendment as prohibiting the government from conducting electronic surveillance or physically searching a home or other private place without first demonstrating criminal probable cause, where "'the evidence sought will aid in a particular apprehension or conviction' for a particular offense."[178] In contrast,

---

173. *Id.* § 1801(k).

174. *Id.* § 1821(2).

175. *Id.* § 1806(f).

176. *Id.*

177. United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987) (FISA application and related documents "establish that the telephone surveillance of Arocena did not have as its purpose the primary objective of investigating a criminal act").

178. Dalia v. United States, 441 U.S. 238, 255 (1979) (quoting Warden v. Hayden, 387 U.S. 294, 307 (1967)) (holding that the legislature intended to confer power to engage in covert entries under Title III upon a showing of probable cause); *see* 18 U.S.C. §§ 2518(1)(b), 3(a); United States v. Meling, 47 F.3d 1546, 1551 (9th Cir. 1995) (finding that an affidavit for Title III warrant

FISA does not require a showing of criminal probable cause.[179] Instead, the government must only show probable cause that the target is an "agent of a foreign power."[180] The Patriot Act amended FISA's requirement that an executive branch official certify that "the purpose" of the proposed surveillance was foreign intelligence gathering.[181] As amended, foreign intelligence gathering need only be "a significant purpose" of the surveillance.[182] As a result, FISA offers less protection than the traditional Fourth Amendment protections under Title III of the Omnibus Crime Control and Safe Streets Act of 1968.[183]

Under Title III and the Fourth Amendment, the target of the surveillance must receive notice that the government has invaded his privacy.[184] Under FISA, the government does not have to provide notice to the target unless it "intends to enter into evidence or otherwise use or disclose" the FISA evidence in a trial or other official proceeding.[185] In contrast, a target under Title III surveillance may receive copies of the application and order to challenge the constitutionality of the surveillance.[186]

2. Disclosure of the FISA Applications and Orders and an "Agent of a Foreign Power"

According to the legislative history of FISA, disclosure may be necessary under § 1806(f) in cases where compliance with minimization standards and general questions of legality undermine the validity of the surveillance. For example, disclosure may be necessary "where the court's initial review of the application, order, and fruits of the surveillance indicates that the question of legality may be complicated by factors such as 'indications of possible misrepresentation of fact, vague identification of the persons to be

---

contained sufficient probable cause).

179. Motion to Suppress, *supra* note 95, at 8.

180. *Id.*

181. Patriot Act, Pub. L. No. 107-56, § 218, 115 Stat. 291 (codified at 50 U.S.C. §§ 1804(a)(7)(B), 1805(a)(5), 1823(a)(7)(B), 1824(a)(5) (2005).

182. *Id.*

183. 18 U.S.C. §§ 2510–2521 (2005).

184. *Id.* § 2518(8)(d).

185. 50 U.S.C. §§ 1806(c), 1825(d) (2005).

186. 18 U.S.C. § 2518(9).

surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order.'"[187]

In Smith's case, to obtain the FISC orders, the government had to convince FISC that probable cause existed showing that Smith was "an agent of a foreign power."[188] Smith could only have been an "agent of a foreign power" if he "knowingly" assisted Leung's alleged clandestine intelligence activities on behalf of the PRC.[189] Interestingly, neither of the indictments against Smith alleges that Smith "knowingly" assisted Leung. In fact, the indictments only charge Smith with gross negligence in the handling of classified information. Gross negligence does not require that the defendant's conduct be "knowing."[190] Therefore, it is possible that despite the government's allegations that Smith is an "agent of a foreign power," which formed the probable cause upon which FISC issued its orders, the FISC applications contained falsehoods or omissions that were material to and properly influenced FISC's issuance of the orders.[191] However, because the government never disclosed to Smith's counsel the FISC application, Smith's counsel was unable to

187. United States v. Belfield, 692 F.2d 141, 147 (D.C. Cir. 1982) (quoting S. REP. NO. 701, at 64 (1978)); *see* United States v. Ott, 827 F.2d 473, 476 (9th Cir. 1987) (finding that if monitoring agents choose to disregard the minimization standards and thereby acquire evidence of a crime against an overheard party whose conversation properly should have been minimized, that evidence would be acquired in violation of this chapter and would properly be suppressed); *see also* United States v. Duggan, 743 F.2d 59, 77 n.6 (2d Cir. 1984) (holding that to be entitled to a hearing on the validity of the FISA order, the target must make a substantial preliminary showing that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included in the application and that the allegedly false statement was "necessary" to the FISA Judge's approval of the application).

188. *See supra* note 168 and accompanying text; *see also* Motion to Suppress, *supra* note 91, at 8.

189. *See* 50 U.S.C. § 1801(b) (2005) (defining "agent of a foreign power" as requiring knowing action).

190. 18 U.S.C. § 793(f) (2005).

191. *See* Franks v. Delaware, 438 U.S. 154 (1978) (establishing the circumstances under which the target of a search may obtain an evidentiary hearing concerning the veracity of the information contained in a search warrant affidavit); *Duggan*, 743 F.2d at 77 n.6.

conclusively test whether there was adequate probable cause that Smith was an "agent of a foreign power." Nevertheless, Smith's counsel attempted to argue that probable cause did not exist.

Smith's counsel identified at least three large categories that potentially contained material omissions: (1) information supporting Leung's reliability, bona fides, and loyalty to the United States; (2) information about Smith that would materially undercut the government's contention that he knowingly aided and abetted the PRC's clandestine intelligence activities; and (3) information casting doubt on the credibility of informants on whom the government may have relied in the FISA applications.[192]

The motion has seven redacted pages that follow this citation. Presumably, Smith's counsel cited specific instances of each of its three contentions. If defense counsel had information that would have shown that Smith was *not* an "agent of a foreign power," it would have wanted to ensure that FISC, and in turn, Judge Cooper, evaluated the evidence in Smith's favor.

3. Failed Minimization Procedures

In addition, the "surveillance records" produced to Smith's lawyers[193] "include[d] a significant amount of non-foreign intelligence information, calling into question compliance with the minimization standards contained in the order."[194] "The overwhelming majority of the intercepted Smith phone calls and e-mails have no conceivable bearing on foreign intelligence."[195]

The blanket FISA surveillance affected Smith's family as well. "The communications also include a large number of telephone calls that do not involve or relate to Smith—conversations by his wife and son, for example—that have no bearing at all on this case."[196] "[B]etween April 2002 and April 2003 the government intercepted . . . approximately 19,315 total calls to and from Smith's home telephone . . . . [W]e estimate that fewer than 200 of the calls—about 1% of the total . . . could conceivably contain foreign intelligence

192. Motion to Suppress, *supra* note 95, at 28.
193. Motion to Compel, *supra* note 88, at 11–12.
194. *Belfield*, 692 F.2d at 147 (quoting S. Rep. No. 701, at 64 (1978)).
195. Motion to Compel, *supra* note 88, at 12.
196. Motion to Suppress, *supra* note 95, at 38.

information or evidence of a crime."[197]

4. Deficient Certifications to FISC

The government's certifications to FISC may have also been deficient or erroneous. First, "the government presumably certified that 'a significant purpose'. . . of the surveillance was 'to obtain foreign intelligence information. . . .' Because it appears that the government had begun a criminal investigation of Smith well before the FISA surveillance began, there is reason to believe that the surveillance served an overwhelmingly criminal purpose during all or most of its existence."[198]

If the government had asked for a FISA warrant primarily to assist in a criminal investigation that coincidentally had foreign intelligence overtones, then they violated the requirements of FISA.

"Second, the government was required to certify that the foreign intelligence information 'cannot reasonably be obtained by normal investigative techniques,' and to provide a 'statement of the basis for the certification.'"[199] "In the discovery provided to date, we have seen little indication that the government attempted to use 'normal investigative techniques' before resorting to the highly intrusive, blanket surveillance of Smith's cell phone, home phone, fax machine, and e-mail, and to covert physical searches."[200]

5. The Government's Classified Responses and Concern for National Security

In response, the government asked the court to review the materials *ex parte*, which carries a notoriously significant "risk of an erroneous deprivation" of the liberty and property interests at issue. "Additional. . .procedural safeguards," such as access to the FISA materials and an opportunity to address them, carry substantial "probable value."[201]

The Supreme Court has declared that "fairness can rarely be

197. *Id.* at 40–41.

198. *Id.* at 36 (quoting 50 U.S.C. § 1804(a)(7)(B) (2005)).

199. 50 U.S.C. §§ 1804(a)(7)(E), 1823(a)(7)(E); Motion to Suppress, *supra* note 95, at 36–37.

200. *Id.* at 37.

201. Mathews v. Eldridge, 424 U.S. 319, 335 (1976) (three-factor test to determine if due process requires requested disclosure).

obtained by secret, one-sided determination of facts decisive of rights .... No better instrument has been devised for arriving at truth than to give a person in jeopardy of serious loss notice of the case against him and opportunity to meet it."[202] The Ninth Circuit, in a secret evidence case, observed "[o]ne would be hard pressed to design a procedure more likely to result in erroneous deprivations ... [T]he very foundation of the adversary process assumes that use of undisclosed information will violate due process because of the risk of error."[203]

Similarly, in *Franks v. Delaware*,[204] the Court held that "a defendant must be permitted to attack the veracity of the affidavit underlying a search warrant, upon a preliminary showing of an intentional or reckless material falsehood."[205]

> The usual reliance of our legal system on adversary proceedings itself should be an indication that an *ex parte* inquiry is likely to be less vigorous .... The pre-search proceeding will frequently be marked by haste, because of the understandable desire to act before the evidence disappears; this urgency will not always permit the magistrate to make an extended independent examination of the affiant or other witnesses.[206]

As FISC itself has acknowledged, without adversarial proceedings, systematic executive branch misconduct, including submission of FISC applications with "erroneous statements" and "omissions of material facts," goes entirely undetected by the courts until the DOJ chooses to reveal it.[207] In recognition of this problem, "[o]ne FBI agent was barred [subsequently] from appearing before

---

202. United States v. James Daniel Good Real Property, 510 U.S. 43, 55 (1993) (quoting Joint Anti-Fascist Refugee Comm. v. McGrath, 341 U.S. 123, 170–72 (1951) (Frankfurter, J., concurring)).

203. American-Arab Anti-Discrimination Comm. v. Reno, 70 F.3d 1045, 1069 (9th Cir. 1995) (internal quotation marks omitted).

204. 438 U.S. 154 (1978).

205. Motion to Compel, *supra* note 88, at 15 (citing Franks v. Delaware, 438 U.S. 154, 169 (1978)).

206. Franks v. Delaware, 438 U.S. 154, 169 (1978).

207. *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611, 620–21 (Foreign Intelligence Surveillance Ct. 2002), *abrogated by In re* Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Ct. of Review 2002).

the Court as a FISA affiant."[208]

6. Interception of Privileged Communications with Smith's Attorneys and Wife

Beginning on December 10, 2002, when Smith contacted Brian Sun, Smith's lead attorney of record, by cell phone during his interrogation by the FBI, the government intercepted approximately eleven attorney-client communications. At the beginning of one such call, on December 12, 2002, Sun specifically noted that the communication was privileged. In some calls, Smith and Sun discussed the details of Smith's legal strategy.[209]

The extent of the government's intrusion into defense counsel's conversations was not yet revealed. On March 24, 2004, Smith's counsel had identified fifty-three folders containing privileged communications between Smith and his attorney, Sun and/or Murphy.[210] The law has historically regarded attorney-client communications as essential to the vitality of the American judicial process.[211] "The privilege is intended to encourage 'full and frank communication between attorneys and their clients and thereby promote broader public interests in the observance of law and the administration of justice.'"[212] The government's interception of the attorney-client communications between Smith and Sun was inexcusable.

Purportedly, the government implemented measures to guard against the wholesale disregard of the privilege. The government's approach was to submit these calls to review by a "taint team" rather than by the "investigative team."[213] Nevertheless, eight of the conversations were produced to the investigative team and Leung's counsel.[214] Upon hearing these conversations, the government may

208. *Id.* at 621.

209. Motion to Suppress, *supra* note 95, at 43.

210. Paul Murphy was an associate attorney in Sun's firm. Reply in Support of Motion to suppress, *supra* note 110 at 1.

211. *See* Upjohn Co. v. United States, 449 U.S. 383, 389 (1981).

212. Swidler & Berlin v. United States, 524 U.S. 399, 403 (1998) (quoting *Upjohn Co.*, 449 U.S. at 389) (addressing attorney's notes of an interview with a deceased client; holding that they were protected by the attorney-client privilege).

213. *See* Reply in Support of Motion to Suppress, *supra* note 110 at 2.

214. *Id.*

have adjusted their approach to the investigation and to the prosecution, gaining an advantage against Smith while at the same time impeding his ability to mount an effective defense.

In addition, the indictment could have been dismissed due to the government's misconduct. The court considered four factors when determining whether intrusion into the attorney-client privilege violates the Constitution, thus requiring dismissal of an indictment:[215]

> (1) whether evidence to be used at trial was obtained directly or indirectly by the government intrusion; (2) whether the intrusion was intentional; (3) whether the prosecution received otherwise confidential information about trial preparation or defense strategy as a result of the intrusion; and (4) whether the privileged information was used or will be used to the substantial detriment of the defendant . . . .[216]

If the previously discussed FISA motions were factually correct, all four factors would have been met. The first, third, and fourth factors would be satisfied if the government learned details about Smith's conduct or planned defense through his conversations with his attorneys that led it to additional investigative avenues. Furthermore, the invasion of the attorney-client privilege would qualify as intentional if the government did not comply with the minimization procedures required under FISA. Thus, the second factor would also be met.

In addition to intercepting attorney-client communications, the government disregarded another essential privilege—spousal communications. "The FISA surveillance of Smith intercepted, and recorded, without minimizing numerous telephone conversations between Smith and his wife."[217] It is not known what the substance of these conversations was, however, they were privileged and could

---

215. *See* United States v. Neill, 952 F. Supp. 834, 840 (D.D.C. 1997).

216. Supplemental Reply Memorandum in Support of Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived from Foreign Intelligence Surveillance Act Surveillance of Attorney-Client Privileged Communications at 2–3, United States v. James J. Smith, No. CR-03-429-FMC (C.D. Cal. Apr. 19, 2004) (quoting United States v. Neill, 952 F. Supp. 834, 840 (D.D.C. 1997)).

217. Motion to Suppress, *supra* note 95, at 45.

not be offered as evidence.[218]

7. The Outcome

The foregoing discussion demonstrates the absence of reason or basis in fact supporting the FISA warrant. And yet, FISC approved the warrant nonetheless.[219] Since the CIPA motions that Smith's counsel produced were all redacted when released to the public, no one can determine whether the FISC applications omitted or misrepresented classified information that would have shown Smith was not in fact an "agent of a foreign power." However, had the government included information in the FISC applications showing Smith was acting as an "agent of a foreign power" and had the resulting FISA surveillance uncovered additional evidence of "knowing" action by Smith, one can only wonder why the government did not charge Smith with a more egregious violation than gross negligence.

The indictment against Smith alleged that Leung surreptitiously took documents from Smith's unlocked briefcase and copied them.[220] So, why did the government abandon its argument that Smith was an "agent of a foreign power" who *knowingly* assisted Leung in her efforts, to adopt the position that Smith was guilty of no more than gross negligence? There is no evidence that the government applied for a Title III warrant of Smith at the beginning of the investigation. Nor is there any evidence that the government had a source who tipped them off to the possibility of Leung's and Smith's misconduct. If there was in fact an informant who led the government to open an investigation, then Smith was denied the opportunity to test the informant's reliability under the *Aguilar-*

218. *See* Trammel v. United States, 445 U.S. 40, 47–53 (1980); *see also In re* Grand Jury Investigation, 745 F.2d 863, 864 (9th Cir. 1985); *In re* Grand Jury Investigation, 603 F.2d 786, 787–88 (9th Cir. 1979).

219. Notice of Motion and Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived From Foreign Intelligence Surveillance Act Surveillance, Memorandum in Support, and Declaration of John D. Cline at 1, United States v. James J. Smith, No. CR 03-429-FMC, (C.D. Cal. January 28, 2004).

220. First Superseding Indictment at 16–17, United States v. James J. Smith, No. CR 03-429(A)-FMC (C.D. Cal. Feb. 24, 2004).

Spinelli line of cases[221] and their progeny, such as *Illinois v. Gates*.[222]

In addition to the shortcomings of the system to protect the rights of targets of surveillance, FISA offers a convenient means of circumventing the traditional Title III and search warrant processes.[223] Under FISA, the executive's certification concerning the purpose of the surveillance or search is only subject to minimal scrutiny by the courts. "The FISA Judge, in reviewing the application, is not to second-guess the executive branch official's certification that the objective of the surveillance is foreign intelligence information."[224] Even subsequent *ex parte* review of the FISA Judge's determination adds little protection for the defendant, considering that the "reviewing court is to have no greater authority to second-guess the executive branch's certifications than has a FISA Judge."[225]

According to the Attorney General's annual reports, from 1979 to 2002 FISC approved 15,256 applications or extensions authorizing FISA surveillance or searches. On four occasions it modified an application before granting approval, and only on one occasion did

---

221. Aguilar v. Texas, 378 U.S. 108 (1964) (search violated Fourth Amendment since the affidavit did not contain a sufficient basis for probable cause, such as information that the unidentified informant spoke with personal knowledge of the facts or any informant for the unidentified source's belief); Spinelli v. United States, 393 U.S. 410 (1969) (probable cause not supportable on an informant's tip alone, because the affidavit did not set forth reasons for informant's reliability or personal knowledge).

222. 462 U.S. 213 (1983).

223. *See generally* 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 (2003) (discussing Title II of the USA Patriot Act and how it violates American civil liberties); Joshua L. Dratel, *Ethical Issues in Defending a Terrorism Case: How Secrecy and Security Impair the Defense of a Terrorism Case*, 2 CARDOZO PUB. L. POL'Y & ETHICS J. 81 (2003) (addressing the unique issues faced by attorneys defending those faced with terrorism charges); Grayson A. Hoffman, *Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment*, 40 AM. CRIM. L. REV. 1655 (2003) (discussing why a comparison of FISA Title III procedures are problematic).

224. United States v. Duggan, 743 F.2d 59, 77 (2d Cir. 1984); *see In re* Grand Jury Proceedings, 347 F.3d 197, 204–205 (7th Cir. 2003) (citing *Duggan* as authority).

225. *Duggan*, 743 F.2d at 77.

FISC deny the application.[226] Basic division shows that FISC approved an average of almost three applications per day over the 1979 to 2002 period.[227]

The trend is only increasing. In 2003, the Justice Department applied for a record 1,754 FISA warrants,[228] or on average, almost seven warrants a day.[229]

No more than once has FISC rejected an application. Nor has any district court suppressed the results of a FISA surveillance or search.[230] Nor has any appeals court reversed a decision where the district court denied a motion to suppress FISA information.[231]

The underwhelming number of occasions in which FISC actually rejected FISA warrant applications suggests that the rights of the targets of the surveillance are not adequately considered. The deck is stacked against the target from the beginning of the process, and the Fourth Amendment becomes an afterthought in the proceedings. There is no meaningful standard of review guiding FISC, the district court, or defense counsel.

The government responds to these critiques by citing the usual generalized interest in avoiding damage to "national security." However the government makes no effort to demonstrate that disclosure of FISA materials would cause such damage.

---

226. Foreign Intelligence Surveillance Act, http://fas.org/irp/agency/doj/fisa (last visited Apr. 6, 2006).

227. Assuming that the FISC sits for all five weekdays of the 52 weeks a year to consider applications, this means that there are 260 days a year in which the FISC can sit and consider applications. The period in question covers 23 years. Therefore, the FISC sat for 5980 days over the period from 1979 to 2002. If there were 15,264 applications divided by 5980 days total, then the FISC considered almost three applications a day. The number is likely much higher when you consider federal holidays, vacations, and a likely three or four day work-week.

228. Devlin Barrett, *Wiretaps in U.S. Jump in 19 Percent in 2004*, Associated Press, Apr. 28, 2005; Richard Schmitt, *Covert Searches Are Increasing Under Patriot Act*, L.A. TIMES, May 2, 2004, at A29.

229. Assuming 260 days in which the FISC can sit and consider applications, 1,754 total applications divided by 260 days a year equals 6.75 warrants, or almost seven a day.

230. *See* Foreign Intelligence Surveillance Act, *supra* note 226.

231. *In re* Sealed Case, 310 F.3d 717 (Foreign Intelligence Surveillance Ct. of Review 2002).

Specifically, in the *Smith* case, the government merely stated that "[d]efense counsel have Top Secret/SCI security clearances and an obvious 'need to know' the information. Smith himself, as the government has repeatedly acknowledged, possesses an extraordinary range of classified information," without demonstrating how disclosing the FISA material would affect national security.[232] Thus, the Smith case illustrated that the government's argument that further disclosure of FISA materials would harm national security is tenuous at best.

The *Smith* case would have been the perfect case to test the limits of the FISA statutes. Everyone involved with the case was cleared to view the applications and orders, and there would have been no risk to national security. The court could have conducted an *in camera* review and revealed the review only to Smith, his lawyers, and government counsel. Smith had already been arrested and presumably, since classified information was involved, was under strict pre-trial protective orders not to discuss the case with anyone. If he exposed any of the FISA information or methods, he could have easily been rearrested and charged with intentional exposure of classified material. If appealed, the case would have gone to the Ninth Circuit, and, regardless of the outcome, it could have been appealed to the Supreme Court, which appears to be uneasy with the abandonment of the Fourth Amendment and its protections.[233]

IV. BROADER DEVELOPMENTS IN DOMESTIC SPYING TECHNIQUES AND AUTHORITY

"[I]t appears that the only way to make [FISC] more convenient would be to install a drive-through window."[234] To people familiar with the *Smith* case, problems with balancing defendants' rights with the government's interest in protecting national security are no surprise. However, the government's zeal to protect national security does not merely extend to the FISA context. The government has gone farther than ever before in its quest to protect

232. Motion to Compel, *supra* note 88, at 20.

233. United States v. James Daniel Good Real Property, 510 U.S. 43, 123 (1993) (quoting Joint Anti-Fascist Refugee Committee v. McGrath, 341 U.S. 123, 170–72 (1951) (Frankfurter, J., concurring)).

234. Tim Rutten, *Paranoia on the Left and the Right*, L.A. TIMES, Dec. 24, 2005, at E1.

Americans from terrorism. In an extension of the techniques and abilities granted under the Patriot Act's revision of the FISA statutes,[235] the government created a secret National Security Agency ("NSA") domestic spying program that was revealed in late 2005.[236]

The NSA is a super secret monitoring agency whose mission is to spy on communications abroad.[237] On December 16, 2005, after withholding a story for an entire year due to security concerns, the New York Times published an article revealing that President Bush authorized the NSA to monitor the international phone calls and emails of hundreds, perhaps thousands, of people inside the United States, all without warrants.[238] The Times stated that some NSA officials were so concerned about the validity of the program that they refused to participate.[239] The Times also stated that most people

---

235. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56 (2001).

236. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1. Details of the program are sketchy at best. However, the Times reported that when the Central Intelligence Agency ("CIA") began capturing Al Qaeda operatives overseas, agents seized the terrorists' computers, cell phones and personal phone directories. *Id.* This information was sent to the NSA and, during their monitoring of the original numbers and email addresses, it also monitored others linked to them, creating an expanding chain. *Id.* Hundreds of these numbers and addresses were located in the United States. *Id.* However, in order to target the recipients of the messages in the United States, the government previously had to first obtain a court order from the FISC. *Id.* In addition, the FBI is traditionally responsible for the application to the FISC, not the NSA. *Id.*

237. Traditionally, the NSA can target phone calls or emails on foreign soil, even if the recipient of those messages is in the United States. *Id.*

238. *Id.* Additionally, new disclosures stemming from an American Civil Liberties Union ("ACLU") FOIA lawsuit alleging improper FBI surveillance of protest and social groups show that the FBI was monitoring, among others, an Indianapolis "Vegan Community Project," Greenpeace, the Catholic Workers' for exhibiting a "semi-communistic ideology," and a People for the Ethical Treatment of Animals ("PETA") protest over the use of llama fur. Eric Lichtblau, *F.B.I. Watched Activist Groups, New Files Show*, N.Y. TIMES, Dec. 20, 2005, at A1. The FBI argued that their monitoring was driven by evidence of criminal or violent activity at public protests or disruptive activities. *Id.*

239. *Id.* In opposition to the program, the federal judge who oversees the FISC, Judge Colleen Kollar-Kotelly, helped spur a temporary suspension of certain aspects of the program in mid-2004. *Id.* She questioned whether

targeted under the NSA program have never been charged with a crime.[240]

Additional facts regarding the government's surveillance of U.S. targets continue to come to light. The Pentagon's newest counterintelligence agency, the Counterintelligence Field Activity ("CIFA"), grew from a coordinating agency between the military and the Pentagon to an analytical and operational organization in just under three years.[241] Included in the agency's activities is the "surveillance of potentially threatening people or organizations inside the United States."[242] A former senior counterterrorism official has referred to CIFA as the "militarization of counterterrorism."[243]

In a surprising move, on December 21, 2005, one of FISC's judges, U.S. District Judge James Robertson, resigned from his position in protest over President Bush's surveillance program, stating that the NSA program is legally questionable and may have tainted FISC's work.[244] In addition, Judge Robertson expressed concern that information gathered under President Bush's warrantless surveillance program could have been used to obtain FISC warrants.[245]

Continuing the call for disclosure, on December 22, 2005, presiding FISC Judge Colleen Kollar-Kotelly arranged for a classified briefing for FISC to address FISC's concern about the legality of President Bush's domestic spying program.[246] Judge

---

information gathered under the NSA program was being improperly used as the basis for FISA wiretap requests from the Justice Department. *Id.* As a result, she insisted that any material gathered under the NSA program not be used in seeking wiretap warrants from her court. *Id.* To date, her question has not been answered and it is not clear whether her request has been honored. *Id.*

240. *Id.*

241. Walter Pincus, *Pentagon's Intelligence Authority Widens*, WASH. POST, Dec. 19, 2005, at A10.

242. *Id.*

243. *Id.*

244. Carol D. Leonnig & Dafna Linzer, *Spy Court Judge Quits In Protest*, WASH. POST, Dec. 21, 2005, at A1.

245. *Federal Judge Quits Foreign-Intelligence Court; A critic of tactics in the war on terrorism, he was reportedly troubled by reports that citizens were being monitored without warrants*, L.A. TIMES, Dec. 22, 2005, at A30.

246. Carol D. Leonnig & Dafna Linzer, *Judges on Surveillance Court To Be*

Kollar-Kotelly expects top-ranking officials from the NSA and the DOJ to outline the details of the program to FISC.[247] The judges could also demand that the officials prove that FISC warrants were not tainted by information gathered through President Bush's program.[248] In addition, a judge stated that members of the FISC could disband the court in light of President Bush's assertion that he can bypass FISC.[249]

On another front, defense lawyers in prominent terror cases plan to bring legal challenges to determine whether the NSA used illegal wiretaps against several dozen Muslim men tied to Al-Qaeda.[250] The expected legal challenges will center on the question of whether the defendants in these cases were in fact monitored under the NSA program and whether the government withheld critical information or misled judges and defense lawyers about how and why the defendants were singled out.[251] Specifically, the Bush administration has cited the NSA program as a "critical" part in at least two cases that led to convictions of Al-Qaeda associates. The first case involved Iyman Faris of Ohio, who admitted in taking part in a failed plot to destroy the Brooklyn Bridge. The second case involved Mohammed Junaid Babar of Queens, New York, who was implicated in a plot to bomb British targets.[252] The first expected challenge is likely to come as early as January 2006 in the case of two men charged with Jose Padilla,[253] the dirty bomb suspect held for three years without an indictment as his detention wound its way through the courts.[254] To date, lawyers for Smith and Leung have not filed similar motions to discover whether information gained from the NSA domestic spying program provided the factual basis for the FISA surveillance conducted during the investigations.

Briefed on Spy Program, WASH. POST, Dec. 22, 2005, at A1.

247. *Id.*

248. *Id.*

249. *Id.*

250. Eric Lichtblau & James Risen, *Defense Lawyers in Terror Cases Plan Challenges Over Spy Efforts*, N.Y. TIMES, Dec. 28, 2005, at A1.

251. *Id.*

252. *Id.*

253. *Id.*

254. Eric Lichtblau, *In Legal Shift, U.S. Charges Detainee in Terrorism Case*, N.Y. TIMES, Nov. 23, 2005, at A1.

The first official lawsuits seeking to end the NSA spying program were filed on January 17, 2006 in federal court.[255] The lawsuits, one filed in New York by the Center for Constitutional rights[256] and the other in Detroit by the ACLU,[257] challenge the program on the basis that it bypasses monitoring safeguards required by FISA.[258] The lawsuits name President Bush, the head of the NSA and the various heads of the other major security agencies as parties to the lawsuit.[259]

V. SUGGESTED CHANGES TO FISA TO SECURE DEFENDANTS' RIGHTS

If it were enough to avoid the Fourth Amendment warrant and probable cause requirements merely that an electronic surveillance or physical search had some "significant" connection to foreign intelligence, federal criminal investigators could use those highly intrusive techniques for "virtually any purpose."[260]

The FISA Court of Review conceded that the "constitutional question presented by [*U.S. v. Smith*]—whether Congress' disapproval of the primary purpose test is consistent with the Fourth Amendment—has no definitive jurisprudential answer."[261]

It is apparent that the government increasingly views FISA as the cure-all to the annoyance of due process and Fourth Amendment protections of traditional Title III warrants. Through FISA, the government can easily obtain a secret warrant, allowing an invasion of one's privacy that is almost entirely insulated from any meaningful Fourth Amendment scrutiny or analysis.

---

255. Larry Neumeister, *Groups File Lawsuit Over Eavesdropping Program*, Associated Press, Jan. 17, 2006.

256. *See* Complaint, Center for Constitutional Rights v. Bush, No. 06-CV-00313 (S.D.N.Y. Jan 17, 2006).

257. *See* Complaint for Declaratory and Injunctive Relief, American Civil Liberties Union v. National Securitiy Agency, No. 2:06-CV-10204 (E.D. Mich. Jan. 1, 2006).

258. *Id.*

259. *Id.*

260. Motion to Suppress, *supra* note 95, at 23.

261. *In re* Sealed Case, 310 F.3d 717, 746 (Foreign Intelligence Surveillance Ct. of Review 2002). And yet, in spite of this startling admission, the Court of Review upheld the constitutionality of the warrant *without* addressing the murkiness of the Fourth Amendment question. *See id.*

A. Congressional Oversight

According to the FISA statutes, the U.S. Senate's Select Committee on Intelligence[262] and the House Permanent Select Committee on Intelligence[263] have jurisdiction over FISC and the executive branch officials submitting FISA applications when the Attorney General authorizes covert surveillance without a court order.[264] A quick glance at the Senate Committee's hearings[265] of the 109th Congress reveals that many of the hearings are closed to the public for obvious national security reasons, making the concern over public opinion against secret search and seizure warrants a moot point. Senators on the committee can say that they give FISA warrants the attention they deserve, while in reality, they accept the testimony of government officials before the committee at face value without further investigation.[266]

The only requirements as to the content of the Attorney General's report to the Committees are statistical in nature.[267] The

263. U.S. Senate Committee on Intelligence—Jurisdiction http://intelligence.senate.gov/juris.htm, (last visited Apr. 6, 2006) (emphasis added).

263. Permanent Select Committee on Intelligence: Home Page, http://intelligence.house.gov/default.aspx (last visited Apr. 6, 2006).

264. 50 U.S.C. § 1802(a)(2) (2001) ("An electronic surveillance authorized by this subsection may be conducted only in accordance with the Attorney General's certification and the minimization procedures adopted by him. The Attorney General shall assess compliance with such procedures and shall report such assessments to the House Permanent Select Committee on Intelligence and the Senate Select Committee on Intelligence under the provisions of *section 1808*(a) of this title.").

265. U.S. Senate Committee on Intelligence—Hearings, http://intelligence.senate.gov/hr109.htm (last visited Apr. 6, 2006).

266. *See infra* text accompanying note 265.

267. According to 50 U.S.C. § 1871(a):

> On a semiannual basis, the Attorney General shall submit to the Permanent Select Committee on Intelligence of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Committees on the Judiciary of the House of Representatives and the Senate, in a manner consistent with the protection of the national security, a report setting forth with respect to the preceding 6-month period—
>
> (1) the aggregate number of persons targeted for orders issued under this chapter . . .

Attorney General need only give the Committee a brief description of each case brought under FISA, and an indication of which cases ultimately involved use of FISA evidence at trial.

As the *Smith* case demonstrates, when an executive branch official applies for a FISA warrant against a U.S. citizen,[268] the only Executive Branch review comes from the Attorney General. But the Attorney General is the person who ordered the FISA warrant in the first place, and the Attorney General can only grant review upon written request from specific executive branch individuals.[269] The FBI Director, presumably after consultation with the DOJ and the Attorney General, directs his officials to apply for a FISA warrant. The FBI Director, after getting approval from the Attorney General, is expected to review the same FISA warrant and ask the Attorney General to review it for any mistakes. It is safe to say that neither the Attorney General nor the FBI Director will review the FISA warrant once it has been secured from the FISC. None of the other three executive officials listed in the statute[270] would know what the FBI and DOJ investigations entailed, so their written requests would not likely be forthcoming.

The protections from within the Executive and Legislative Branches are weak, if not toothless. The author understands the need to protect national security. Furthermore, the author agrees that opening the hearings in the House and Senate would expose to the public information regarding intelligence gathering and targets of surveillance. This would likely bring about the calamitous threat to national security the government fears. We cannot have intelligence information broadcast for all to hear, giving our nation's enemies

---

> (3) the number of times that the Attorney General has authorized that information obtained under this Act may be used in a criminal proceeding or any information derived therefrom may be used in a criminal proceeding . . . .

50 U.S.C. § 1871(a) (2005).

268. 50 U.S.C. § 1801(b)(2)(A).

269. *Id.* § 1804(e)(1)(A) ("Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, or the Director of National Intelligence, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801(b)(2) of this title.").

270. Namely, the Secretary of Defense, Secretary of State, or the Director of National Intelligence. *See id.*

additional ammunition in their fight against us.

However, the expectation that the Attorney General and other executive branch officials will review every FISA application for proper procedures is unrealistic and naïve—especially after the FBI Director and the DOJ confer over the need for a FISA warrant. They cannot be expected to review almost two thousand applications a year. Therefore, we cannot look to the Legislative or Executive Branches for help. That leaves us with one Branch to turn to for aid: the Judicial Branch.

B. Criminal and Civil Remedies

Under the FISA statutes, there are criminal sanctions that can be brought against the agents conducting electronic surveillance and physical searches.[271] However, case law precludes a suit against the Attorney General and FBI Agents acting at his behest.[272] Citing a

---

271. 50 U.S.C. § 1809 (2005) provides:

> (a) Prohibited activities
>
> A person is guilty of an offense if he intentionally—
>
> (1) engages in electronic surveillance under color of law except as authorized by statute; or
>
> (2) discloses or uses information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance not authorized by statute.
>
> (b) Defense
>
> It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction.
>
> (c) Penalties
>
> An offense described in this section is punishable by a fine of not more than $10,000 or imprisonment for not more than five years, or both.
>
> (d) Federal jurisdiction
>
> There is Federal jurisdiction over an offense under this section if the person committing the offense was an officer or employee of the United States at the time the offense was committed.

50 U.S.C. § 1809; *see* § 1827 (physical searches).

272. Chagnon v. Bell, 642 F.2d 1248, 1251 (D.C. Cir. 1980) (appellants arguing, among other claims, that the defendants did not have probable cause

possibility of abuse if a remedy were granted,[273] the Court in *Chagnon v. Bell* denied relief to plaintiffs, stating that "the broad authority of federal executive officials to direct their subordinates carries with it the danger that such power will be abused . . . ."[274] The Court has further found that "FBI officers [are] entitled to act in reliance on an official statement of the law by the Attorney General of the United States."[275]

However, an exception to this immunity exists. A public official loses immunity if he knows or reasonably should know that an action within his sphere of official responsibility "would violate the constitutional rights of the [individual] affected. . . ."[276] Immunity is also inappropriate where the public official acts with the "malicious intention to cause a deprivation of constitutional rights or other injury . . . ."[277]

Next, "when a defendant interposes a good-faith defense to a charge of official misconduct, the court must determine as a matter of law whether the charge states a violation of a right that has been authoritatively declared."[278] In *Chagnon*, the court hedged its bets, stating that the state of the law in 1978–1979 was still unsettled, and therefore, the claim of immunity should stand.[279]

However, in *Zweibon I*, the court stated:

---

to believe that the target of the wiretap was the agent of a foreign power, and that this should overcome any assertion of immunity).

273. *Id.* at 1252.

274. *Id.* at 1255.

275. *Id.* at 1255 n.9.

276. *Id.* at 1257

277. *Id.*

278. *Id.* at 1258.

279. *Id.* ("Each of the alleged issues of material fact upon which appellants relied in opposing summary judgment is in essence a claim that the Attorney General 'knew or should have known' that the Truong surveillance violated appellants' constitutional rights. As we have explained, absent malice, such a claim defeats an immunity defense only in an area of 'clearly established' law. Whether evaluated by reference to Supreme Court and other judicial precedent, to presidential practice, or to then existing congressional legislation, the state of the law with respect to electronic surveillance of foreign agents of foreign powers was, at best, unsettled in 1977–1978, the period of the Truong wiretap." (footnotes omitted)); *see also id.* at 1256. ("[I]t is plain that the Supreme Court in *Keith* left unanswered the question whether a foreign agent exception to the warrant requirement exists.").

> [A] warrant must be obtained before a wiretap is installed on a domestic organization that is neither the agent of nor acting in collaboration with a foreign power. Thus, read in its broadest light, *Zweibon I* restricted the potential reach of the foreign agent exception by explicitly eliminating from its purview surveillance aimed at *individuals or domestic organizations not acting on behalf of a foreign power.*[280]

This could spell victory for Smith and others like him. As the highest ranking law enforcement official in the federal government, the Attorney General "must be held to know the relevant law."[281] However, case law also makes such a claim extraordinarily hard to prove.

> [W]hen the foreign agent exception is invoked to justify warrantless surveillance, courts must be alert to the possible pretextuality of the claim. Here the good faith defense based on a presumed foreign agent exception succeeds because this record demonstrates a "direct link between the wiretap target and a foreign interest as a justification for surveillance' and because the surveillance was 'reasonably intended to guard national security data from foreign intelligence agencies.'"[282]

In *Smith*, both factors of the good faith defense fail. First, since the affidavit against Smith only charged him with gross negligence, there is serious reason to doubt that Smith was directly linked to a foreign interest. Second, while the initial FISA application could be reasonably viewed as an attempt to determine if national security data was in fact passing from Smith to Leung, initial FISA surveillance and interviews with Leung would have given the investigators no indication that Smith was in fact knowingly passing national security data to Leung on a continuous basis. In light of these arguments, it is possible that Smith could defeat a claim of immunity in the face of criminal charges by the Attorney General.

However, not all is well for Smith. FISA provides for an

---

280. *Chagnon*, 642 F.2d at 1259 (second emphasis added) (internal quotation omitted).

281. *Id.* at 1257.

282. *Id.* at 1260 (quoting Halperin v. Kissinger, 606 F.2d 1192, 1204 (D.C. Cir. 1979)).

additional defense to the potential criminal charges.[283] Since no one has ever defeated the immunity that federal officers enjoy, no case exists that tests the limits of the defense built into the statute. However, by the plain text of the statute, it is clear that the Attorney General, the FBI Director, and any FBI Agent involved with the FISA surveillance can easily be defined as a "law enforcement or investigative officer engaged in the course of his official duties."[284] Also, since "the electronic surveillance was authorized by and conducted pursuant to a search warrant . . . of a court of competent jurisdiction,"[285] namely FISC, every federal official who had a hand in the FISA surveillance can rest easy. If arrested under the FISA statute, they have a rock-solid defense. Smith has no recourse under the criminal penalties section of FISA. No federal official will ever be held judicially accountable for the likely abuses of Smith's Fourth Amendment rights. Meanwhile, Smith remains convicted of a felony punishable by up to five years in prison.[286]

Not surprisingly, the same result and its reasoning[287] apply to the civil remedies sections of FISA.[288] However, the statutes do not

283. 50 U.S.C. § 1809(b) (2005) ("It is a defense to a prosecution under subsection (a) of this section that the defendant was a law enforcement or investigative officer engaged in the course of his official duties and the electronic surveillance was authorized by and conducted pursuant to a search warrant or court order of a court of competent jurisdiction."); *see id.* § 1827(b).

284. 50 U.S.C. § 1809(b)

285. *Id.*

286. 18 U.S.C. § 1001 (2005) (stating the maximum sentence for making a false statement to a federal agency).

287. *See* Chagnon, 642 F.2d 1248.

288. 50 U.S.C. § 1810 states:

> 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) . . ., respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 1809 . . . shall have a cause of action against any person who committed such violation and shall be 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.

include the defense provided in the criminal remedies section of FISA. The government conceded that Smith was an "aggrieved person" in one of their motions,[289] so Smith has overcome that particular hurdle should he decide to sue. The remaining obstacle, is the same issue that was before the *Smith* court: is Smith an "agent of a foreign power" under FISA definitions?[290]

This would require an examination of the underlying FISC application, along with any evidence that tended to show Smith was not an agent of a foreign power. Again, no court has ever mandated disclosure of a FISA application. However, Smith and his counsel are the perfect parties to break new legal ground. As discussed above, all parties have the requisite security clearances. Moreover, the government's *only* defense to a civil case under this statute is to disclose the application and show that they had probable cause to believe Smith was an "agent of a foreign power." Assuming Smith can overcome a claim of immunity, the government would have no choice but to disclose the application unless it chose to avoid litigation through a settlement accepted by Smith.

Additionally, on the issue of damages, Smith stands to recoup monetarily.[291] Smith's case appears to be the perfect test case. Only

---

50 U.S.C. § 1810 (2005); *see also id.* § 1828 (stating the civil remedies for an illegal FISA physical search).

289. Reply in Support of Motion of Defendant James J. Smith to Suppress Evidence Obtained or Derived from Foreign Intelligence Surveillance Act Surveillance, United States v. James J. Smith, No. CR-03-429-FMC (C.D. Cal. Apr. 12, 2004).

290. 50 U.S.C. § 1804(a)(4)(A); *see id.* § 1823(a)(4)(A) (same requirement for a physical search).

291. *See* 50 U.S.C. § 1810(a)–(c) (defining electronic surveillance damages); *see id.* § 1828(1)–(3) (defining physical searches damages). Under 50 U.S.C. § 1810(a), assuming that Smith was surveilled every day for an entire year, Smith can sue for $100 for each day he was under surveillance. That comes to a total of $365,000. Now, under subsection (c), assume that Smith's two attorneys conservatively charged an hourly rate of $350. Now, assume they spent eight hours a day for 6 months' worth of work total on Smith's case. Assuming that there are thirty days a month times six months, that would equal 180 days worth of work. Multiply that by the eight hours worked per day times $350 an hour, equaling $504,000 for *one* attorney's efforts. All told, a conservative estimate would equal $1,008,000 in attorney's fees. The real amount is likely much higher. Finally, consider subsection (b), which allows plaintiffs to seek punitive damages. How can a price be placed on the loss of

time will tell if he and his lawyers believe they have a credible cause of action against the government for their likely abuse. However, any speculation as to recovery for victims of FISA abuse *without* security clearances is extremely unlikely. Even though the Legislature added a promising legal remedy for a wronged FISA target to pursue, the courts promptly rendered it almost useless. Nearly insurmountable immunities and factual requirements imposed by the court would make many victims of FISA abuse throw up their hands in despair. Many, if not all, of the targets of FISA surveillance do not have the luxury of a security clearance, and would not have the ability to argue that disclosure would not damage national security. Therefore, as a remedy, the Legislature seems to have failed to provide a workable and feasible remedy, both in the criminal and civil arenas.

C. FISA Public Defenders

"[T]he United States has a difficult history which testifies to the fact that in times of emergency and crisis, precisely at the time when democracy is tested, there is a tendency to violate human rights unnecessarily, a violation which is not rectified by the courts but which is on occasion actually given effect, starting with Korematsu and ending with the Patriot Act."[292]

A basic search in the LEXIS database for law review articles dealing with FISA produced more than two hundred entries. Of those, approximately fifty were on topic. Most of the articles argued that the amendments to FISA are unconstitutional,[293] while very few

---

reputation, lost wages, marital and familial strife and likely harassment by the media that the Smith family must have suffered? Again, conservatively, a figure in the millions is not out of the question. Under 50 U.S.C. § 1828(1), there is no way to know how many physical searches were conducted at the Smith home or how many times the Smith's belongings were searched unless the FISC application is disclosed. The same math would apply as above, however, the total amount would be much less since it is likely that the searches numbered in the range of dozens and not hundreds.

292. Emanuel Gross, *The Influence of Terrorist Attacks on Human Rights in the United States: The Aftermath of September 11, 2001*, 28 N.C.J. INT'L L. & COM. REG. 1, 78 (2002) (footnote omitted).

293. *See, e.g.*, Jennifer C. Evans, *Hijacking Civil Liberties: The USA Patriot Act of 2001*, 33 LOY. U. CHI. L.J. 933 (2002).

argued that the changes withstood Fourth Amendment analysis.[294] While many of the articles focused on the language of the amendments and the accompanying case law, not one author offered a solution to the inherent problems of FISA such as this paper suggests.

The FISA application process itself must be fundamentally altered to ensure the rights of U.S. citizens who are potential targets of FISA surveillance. In order to ensure that *all* facts, both inculpatory and exculpatory, are brought to the FISC's attention, this Note proposes that Congress amend FISA to ban *ex parte* applications, except in times of emergency.[295] Of course, this means that we need government attorneys whose sole job would be to review and argue against a FISA application if it lacks probable cause to believe the target is an "agent of a foreign power."[296]

Since all solutions to problems involve money, let us engage in some hypothetical hiring. Let us assume that the number of FISA applications for 2005 totals 2,000 applications. Of those applications, assume that seventy-five percent of those are either targeting foreign powers or reapplying for continuing surveillance. That leaves us with 500 applications remaining of U.S. citizens. If we also assume that there are 260 working days per year, that means that each day, only two applications and accompanying evidence need be reviewed. A team of three or four attorneys, along with a support staffer for each, would easily meet the burden of reviewing the applications.

This is hardly difficult in terms of money and logistics. The added expense of three or four attorneys and support staff would be

---

294. *See, e.g.*, Lance Davis, *The Foreign Intelligence Surveillance Court's May 17 Opinion: Maintaining a Reasonable Balance Between National Security and Privacy Interests*, 34 MCGEORGE L. REV. 713 (2003).

295. Of course, the emergency exception should be written so that only valid emergencies would be allowed under the statutes. For example, if in the course of a terrorist investigation it becomes apparent that an attack is imminent, and the FBI reasonably believes it can gain invaluable information by surveilling a particular group of people using electronics to communicate, the author has no problem allowing that type of surveillance to occur. However, as in *Smith*, it was apparent that the documents had already been purloined and that no information was continually flowing from Smith to Leung.

296. *See supra* note 288 and accompanying text.

negligible in the entire Federal Public Defenders' Office budget, and security clearances for employees should be relatively easy to procure. Existing Public Defender's Offices could be restructured to have a secure floor with a SCIF for the accompanying classified information and applications. In addition to adding a layer of adversarial process for targets of surveillance, it would actually improve FBI investigations since it would force FBI Agents to plan out their investigations, allowing them prepare a more thorough affidavit for a FISA warrant.

Targets could rest easy knowing that *someone* is advocating and reviewing their Fourth Amendment rights. District Courts could be relieved of much of the burden from FISA suppression motions litigation regarding the validity of the FISA applications and government mistake or misconduct. Since FISA public defenders would have to argue truthfully before FISC, and since they would have to present all evidence *against* the approval of a FISA application or bring exculpatory evidence to FISC regarding an *existing* FISA application, targets could be assured that the warrant was vigorously litigated and tested. A federal judge would receive *all* of the facts, not just the ones beneficial to the government's case. The Fourth Amendment would be alive and well—even in the foreign intelligence arena. The government could be confident knowing that the additional safeguards pose no threat to national security, and government investigations would not be seriously hampered by unreasonable restrictions on agents' investigative powers in times of emergency.

Critics of this proposal may argue that exposure of classified intelligence gathering methods and classified materials would seriously endanger national security. However, there is a direct precedent for such a process that has existed for years that has balanced the need for national security against defendants' access to classified materials. Under the Uniform Code of Military Justice ("UCMJ"), classified information is directly defined in the opening section.[297] Military courts-martial are designed to try defendants who

297. "The term 'classified information' means (A) any information or material that has been determined by an official of the United States pursuant to law, an Executive order, or regulation to require protection against unauthorized disclosure for reasons of national security, and (B) any restricted data, as defined in section 11(y) of the Atomic Energy Act of 1954 (42 U.S.C.

are accused of spying[298] or who engaged in espionage.[299] Naturally, these charges often involve matters of the highest national security since they may deal with classified information regarding, among other topics: nuclear weaponry, military spacecraft and satellites, early warning systems, war plans, and communications intelligence.[300] These charges may also involve many different forms of information storage or transmission.[301]

In these cases, both attorneys need to know the background and extent of the charges against the accused. Thus, military courts-martial provide a system currently in place that deals specifically with the production of classified information. Under the Military Rule of Evidence ("M.R.E.") 505(a), a privilege against the disclosure of classified materials exists at all stages of the proceedings.[302] The M.R.E. specifically states that the person claiming the privilege may authorize a witness or trial counsel to

---

2014(y))." 10 U.S.C. § 801(15) (2005).

298. *Id.* § 906.

299. *Id.* § 906(a)(1).

300. The specific language of the act reads:

> Any person subject to this chapter [10 USCS §§ 801 et seq.] who, with intent or reason to believe that it is to be used to the injury of the United States or to the advantage of a foreign nation, communicates, delivers, or transmits, or attempts to communicate, deliver, or transmit, to any entity described in paragraph (2), either directly or indirectly, anything described in paragraph (3) shall be punished as a court-martial may direct, except that if the accused is found guilty of an offense that directly concerns (A) nuclear weaponry, military spacecraft or satellites, early warning systems, or other means of defense or retaliation against large scale attack, (B) war plans, (C) communications intelligence or cryptographic information, or (D) any other major weapons system or major element of defense strategy, the accused shall be punished by death or such other punishment as a court-martial may direct.

Id. § 906(a)(1).

301. "A thing referred to in paragraph (1) is a document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, note, instrument, appliance, or information relating to the national defense." *Id.* § 906(a)(3).

302. "Classified information is privileged from disclosure if disclosure would be detrimental to the national security. As with other rules of privilege this rule applies to all stages of the proceedings." MIL. R. EVID. 505(a).

assert the privilege on his behalf.[303]

However, the M.R.E. does not specifically state that only the prosecuting attorney may assert the privilege. When the accused requests access to the classified materials prior to the beginning of trial, and counsel asserts the privilege against disclosure, the convening authority may, among other options,[304] "[p]rovide the document subject to conditions that will guard against the compromise of the information disclosed to the accused . . . ."[305] If the privilege has been asserted with respect to "classified information that apparently contains evidence that is relevant and necessary . . . and is otherwise admissible in evidence . . . the matter shall be reported to the convening authority."[306]

If the information is not provided to the court-martial within a reasonable time and proceeding with the case without such information would materially prejudice a substantial right of the accused, the military judge shall dismiss the charges to which the classified information specifically relates.[307]

If the government agrees to disclose the information to the accused, the military judge is required to draft a protective order,[308]

---

303. *Id.* R. 505(c).

304. Rule 505(d) provides that:

> Prior to referral of charges, the convening authority shall respond in writing to a request by the accused for classified information if the privilege in this rule is claimed for such information. The convening authority may:
>
> (1) Delete specified items of classified information from documents made available to the accused;
>
> (2) Substitute a portion or summary of the information for such classified documents;
>
> (3) Substitute a statement admitting relevant facts that the classified information would tend to prove;
>
> (4) Provide the document subject to conditions that will guard against the compromise of the information disclosed to the accused; or
>
> (5) Withhold disclosure if actions under (1) through (4) cannot be taken without causing identifiable damage to the national security.

Id. R. 505(d).

305. *Id.* R. 505(d)(4).

306. *Id.* R. 505(f).

307. *Id.* R. 505(f)(4).

308. *Id.* R. 505(g).

which may include the authorization of specific information by the judge,[309] specific storage procedures,[310] controlling access to the material,[311] requiring security clearances,[312] requiring logs for all who view the material,[313] regulating notes taken from the classified material[314] and assigning security personnel to the government storage facilities.[315]

If the government does not wish to disclose the classified material, the military judge is authorized to conduct an *in camera* hearing to determine whether the information needs to be disclosed to secure the rights of the accused.[316] During the hearing, "[c]lassified information is not subject to disclosure . . . unless the information is relevant and necessary to an element of the offense or a legally cognizable defense and is otherwise admissible in evidence."[317] If the judge finds that disclosure is warranted, and the government continues to object, the judge may, among other options, dismiss all charges.[318]

Criticism of this article's proposal is blunted by the existence of these procedures, especially in light of the fact that they have existed since 1957. Under these procedures, both the prosecuting and defense counsel have the opportunity to request and review classified materials in order to protect both the interests of the government in protecting national security and the interest of securing a fair trial against the accused. These procedures have been in place for forty-eight years, and there has been no outcry over potential damage to national security, and the information potentially disclosed under these procedures is much more sensitive than surveillance techniques or information intercepted using these techniques.

309. *Id.* R. 505(g)(1)(A).
310. *Id.* R. 505(g)(1)(B).
311. *Id.* R. 505(g)(1)(C).
312. *Id.* R. 505(g)(1)(D).
313. *Id.* R. 505(g)(1)(E).
314. *Id.* R. 505 (g)(1)(F).
315. *Id.* R. 505(g)(1)(G).
316. *Id.* R. 505(i).
317. *Id.* R. 505(i)(4)(B).
318. *Id.* R. 505(f).

V. CONCLUSION

The current debate over the Patriot Act's effect on FISA must include its effects on real cases and on real people. The changes made to FISA mean that defendants are easily ensnared in criminal investigations through the secret surveillance of every corner of their lives. Defendants have no remedy, either while undergoing prosecution or after the case concludes. This paper has endeavored to show the devastating impact FISA can have on defendants and to show how the government uses this incredibly broad tool to pursue criminal convictions.

James Smith, a veteran of the Armed Forces and a dedicated thirty-year Special Agent and Supervisory Agent of the FBI, fell prey to an Executive Branch run amok. In its zeal to ensure that Smith was not another Robert Hanssen or Aldrich Ames, the government violated his and his family's Fourth Amendment rights. Using a constitutionally questionable statute, a secret court, and information possibly gathered through a constitutionally questionable NSA domestic spying program, the FBI was able to invade every aspect of Smith's life. Ultimately, the FBI ruined Smith's reputation as a defender of the United States and likely destroyed his familial relationships, all without giving Smith a chance to defend the claims against him. The government's victory is a guilty plea to a single charge of lying to a federal officer about an affair and Smith's resulting probation and three-month house arrest.

Smith's sentence means more than restrictions placed on a felon. He will likely never work again in any meaningful capacity, and his talent and experience as a veteran counterintelligence officer will be wasted. He has likely lost many of his friends and family members' respect, and his name will likely be used on Capitol Hill as political fodder, showing Congress that the FBI can police their own.

The pulse of the Fourth Amendment is thready at best. Congress has allowed the Executive Branch to take the events of September 11, 2001, and steamroll the protections of the Fourth Amendment. Targets of surveillance cannot examine the underlying probable cause forming the basis for the invasion of the most private aspects of their lives. The lawyers for the defendants cannot see the government's applications to examine them for proper probable cause, and the judges do not get to ensure that the rights of the defendants were not abused in the application process. The

Executive Branch holds all of the cards and is never held accountable for mistakes or misconduct at any point during or after the FISA application process.

Criminal and civil remedies are completely ineffective due to the Executive Branch's immunity from prosecution or lawsuit. Even that rare exception, such as Smith, has an uphill battle ahead of him should he decide to sue to recover the losses he and his family suffered. Congress' oversight fails to protect the rights of U.S citizens under the Fourth Amendment. Further, unlike Smith, citizens without security clearances have even more limited ability to argue that national security will not be damaged if the applications are produced, even *in camera*.

The only way to guarantee protection of U.S. citizens' Fourth Amendment rights is by ensuring that each FISA application involving U.S. citizens is subjected to vigorous litigation through the adversarial process. To this end, a small group of dedicated and objective individuals whose sole mission is the protection of U.S. citizens could be created through the Federal Public Defenders' Office. For forty-eight years, this country has maintained a system under which both sides in a court-martial can obtain access to classified materials so that crimes involving such materials can be adequately litigated. If it is good enough for the military and has withstood the test of time, why should U.S. citizens not have the same protections in the FISA context?

Without oversight of FISA applications, the Fourth Amendment, a bedrock principle of the Bill of Rights, is in danger of becoming obsolete in the context of FISA. If Smith cannot prevail in federal court in a civil lawsuit, then we will have lost a powerful deterrent to secret invasions of our private lives, and our government will have become the thing we fear the most: an enemy of freedom.

*Kelly J. Smith**

---

* J.D., Loyola Law School, May 2006; B.A., Claremont McKenna College, 2001. Thanks to the editors and staff of the Loyola Law Review for their guidance and suggestions. I would also like to thank Professor Laurie Levenson for her guidance, wisdom, support and humor. Without you, this paper would not have completed. Special thanks to my friends and family. Finally, this paper is dedicated to Mom and Dad. I owe everything to you.