NEW YORK UNIVERSITY
JOURNAL OF LAW & LIBERTY

THE FISA WALL AND FEDERAL INVESTIGATIONS

Cedric Logan*

* J.D., New York University School of Law class of 2008. My deep appreciation goes to the professors and students of the Complex Federal Investigations seminar for their helpful critiques, and to the fantastic editors of the Journal of Law & Liberty for their thorough and thoughtful comments. This project would not have been possible without the patience and support of Stephanie and Elliot; my continuing and loving thanks to you both.

INTRODUCTION

The Foreign Intelligence Surveillance Act of 1978 ("FISA") governs federal collection of foreign intelligence information,[1] though there is an ongoing and critical debate about what the law means and how best to implement it.[2] Much of the debate centers on a set of regulations, commonly referred to as "The Wall," which limit the ability of law enforcement officials within the federal government to cooperate with intelligence officials involved in FISA investigations.[3] Congress intended to dismantle The Wall with the USA PATRIOT Act,[4] but one federal court has taken steps that may lead to The Wall being rebuilt.[5]

Rebuilding The Wall would be a mistake. Ample and convincing evidence, largely in the form of government reports investigating specific intelligence failures, shows that The Wall was a disastrous policy. The arguments against The Wall exist mostly in case-study contexts responding to intelligence failures preceding events such as the Wen Ho Lee investigation or the September 11 attacks. This note aims to tie together the varied and isolated statements of government actors who were frustrated with the rules as they existed prior to the USA PATRIOT Act. If Congress rebuilds The Wall or if courts decide that certain aspects of The Wall are constitutionally compelled, they should do so with the knowledge that they will

---

[1] 50 U.S.C. §§ 1801–1862 (1978).

[2] *See, e.g.*, Richard A. Posner, *Privacy, Surveillance, and Law*, 75 U. CHI. L. REV. 245 (2008); William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209 (2007); Susan N. Herman, *The USA PATRIOT Act and the Submajoritarian Fourth Amendment*, 41 HARV. C.R.-C.L. L. REV. 67 (2006).

[3] *See infra* Part II.C.2.

[4] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA PATRIOT Act].

[5] *See generally* Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007) (holding that the USA PATRIOT Act's amendment to §§ 1804 and 1823 are unconstitutional violations of the Fourth Amendment).

be significantly hampering the ability of federal investigators to protect national security.

The scope of this note is limited: I do not assess the constitutionality of the USA PATRIOT Act, nor do I appraise whether or not privacy interests are hindered or promoted by The Wall. Other scholars have done so.[6] Rather, my concern is to provide an accurate assessment of the impact of The Wall on the effectiveness of federal investigations.

Part I traces the development of the FISA Wall, the impact of the USA PATRIOT Act on it, and the responses of the federal courts. Part II categorizes and explains the different ways in which The Wall influences the federal government's counterterrorism capabilities. Part III explores whether or not a compromise is possible that both dismantles The Wall and alleviates the concerns of privacy advocates who argue that The Wall is necessary to protect Fourth Amendment privacy values.

I. THE RISE AND FALL OF THE FISA WALL

A. PRE-FISA FOREIGN INTELLIGENCE GATHERING

The executive has long claimed the inherent authority to conduct warrantless surveillance for the purposes of collecting foreign intelligence. In anticipation of World War II, President Franklin D. Roosevelt directed J. Edgar Hoover to investigate possible sources of threats, including the communists and the Japanese.[7] During the war, Roosevelt authorized Attorney General Robert Jackson to use warrantless wiretaps to investigate threats to the United States,[8]

---

[6] *See, e.g.*, Herman, *supra* note 2; Banks, *supra* note 2.

[7] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT: FINAL REPORT OF THE NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES 74 (Official Gov't ed. 2004); Elizabeth Gillingham Daily, Comment, *Beyond "Persons, Houses, Papers, and Effects": Rewriting the Fourth Amendment for National Security Surveillance*, 10 LEWIS & CLARK L. REV. 641, 644 (2006).

[8] Fletcher N. Baldwin, Jr. & Robert B. Shaw, *Down to the Wire: Assessing the Constitutionality of the National Security Agency's Warrantless Wiretapping Program: Exit the Rule of Law*, 17 U. FLA. J.L. & PUB. POL'Y 429, 435 (2006); *see* Michael A. DiSabatino, Anno-

though Roosevelt asked that Jackson refrain from targeting U.S. citizens.[9] In the 1950s, the FBI broadened its use of warrantless surveillance, taking the position that it could engage in surveillance without any authorization as long as the FBI determined that the "national interest" justified it.[10]

Such searches escaped serious judicial scrutiny as long as the wiretapping devices were physically attached at a point outside the target house or business so that government agents did not physically trespass on the target property. In *Olmstead v. United States*, the Supreme Court held that wiretapping did not constitute a literal search and seizure and thus did not amount to a search under the Fourth Amendment.[11] The Court reasoned that the Fourth Amendment's list of things protected from warrantless search and seizure—"persons, houses, papers, and effects"[12]—constituted "material things"; and since the government could listen to phone conversations via wires that extended far outside a person's house, doing so did not violate a literal reading of the Fourth Amendment.[13]

The *Olmstead* rule survived until 1967, when the Supreme Court revisited it in *Katz v. United States*.[14] The FBI tapped a phone booth used by Katz and then used recorded conversations against him to obtain a conviction for "transmitting wagering information" via telephone.[15] The Court overturned the conviction and overruled *Olmstead*, arguing that "the Fourth Amendment protects people, not places . . . . [W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[16]

---

tation, *Construction and Application of "National Security" Exception to Fourth Amendment Search Warrant Requirement*, 39 A.L.R. FED. 646, § 2[a] (2002).

[9] Daily, *supra* note 7, at 644; Baldwin & Shaw, *supra* note 8, at 435.

[10] Daily, *supra* note 7, at 645.

[11] Olmstead v. United States, 277 U.S. 438, 464 (1928).

[12] U.S. CONST. amend. IV.

[13] *Olmstead*, 277 U.S. at 464 ("The amendment does not forbid what was done here. There was no searching. There was no seizure. The evidence was secured by the use of the sense of hearing and that only. There was no entry of the houses or offices of the defendants.").

[14] Katz v. United States, 389 U.S. 347 (1967).

[15] *Id.* at 348.

[16] *Id.* at 351–52; *see* Daily, *supra* note 7, at 646–47.

Katz continued to recognize exceptions to the Fourth Amendment warrant requirement, such as the "hot pursuit" exception and searches incident to an arrest.[17] The Court, however, expressly declined to decide whether there existed a viable national security exception.[18] Justice White's concurring opinion argued that the president or attorney general could authorize surveillance without a warrant in the interests of national security.[19]

In response to *Katz*, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968 ("Crime Control Act"), which authorized electronic surveillance with a warrant under strict judicial oversight.[20] The act, like *Katz*, expressly declined to touch upon the executive branch's asserted inherent authority to engage in warrantless surveillance for national security purposes.[21]

The Supreme Court tested the national security exception for the first time in *United States v. U.S. District Court* (*Keith*).[22] The defendants, U.S. citizens, were charged with conspiracy to destroy government property, and one of the defendants was charged for bombing a Michigan CIA office.[23] The government did not seek to introduce evidence from a warrantless wiretap, but the defendants moved to compel the government to reveal whether a warrantless wiretap of any of the defendants' conversations took place in order to discover whether that information might lead to the exclusion of other evidence used against the defendants.[24] The government provided an affidavit from Attorney General John Mitchell acknowledging that he approved warrantless wiretaps in this case, but that

---

[17] *Katz*, 389 U.S. at 357–58 & n.19 (listing cases that recognize exceptions).
[18] *Id.* at 358 n.23.
[19] *Id.* at 363–64 (White, J., concurring); *see* Daily, *supra* note 7, at 647.
[20] 18 U.S.C. §§ 2510–2520 (1968); *see* Daily, *supra* note 7, at 647–48 (listing statutory limits and regulations on the ability of government agents to engage in electronic surveillance).
[21] *Id.* § 2511(3) ("Nothing contained in this chapter . . . shall limit the constitutional power of the President . . . to obtain foreign intelligence information deemed essential to the security of the United States . . . .").
[22] United States v. U.S. Dist. Court, 407 U.S. 297 (1972).
[23] *Id.* at 299.
[24] *Id.* at 299–300.

the wiretaps were "employed to gather intelligence information deemed necessary to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."[25] Furthermore, Mitchell certified that disclosure of the conversations could harm national security.[26] The government provided to the district court, under seal, the transcripts from the recorded conversations and records indicating that Mitchell approved the wiretaps.[27] The district court ruled for the defendants, and the Sixth Circuit Court of Appeals affirmed on a writ of mandamus.[28]

The Supreme Court began by dismissing the government's contention that the Crime Control Act recognized the president's ability to conduct national security surveillance without a warrant. The Court noted that the national security caveat was worded negatively—it did not grant the president the authority, but it ensured that any inherent authority would not be interfered with: "[T]he Act shall not be interpreted to limit or disturb such power as the President may have under the Constitution. In short, Congress simply left presidential powers where it found them."[29]

Next, the Court acknowledged that the case did not touch upon the authority of the president to engage in surveillance of foreign entities for the protection of national security; rather, it raised the issue of national security from a purely domestic perspective: "There is no evidence of any involvement, directly or indirectly, of a foreign power."[30]

Finally, the Court provided a framework for evaluating the Fourth Amendment claims at issue. For the Court, the Fourth Amendment was "not absolute in its terms," and therefore the role of the Court was to weigh the relevant interests at stake to determine whether the government's actions were constitutional.[31] Three issues

---

[25] *Id.* at 300, n.2 (quoting Mitchell Affidavit.).
[26] *Id.*
[27] *Id.* at 300–01.
[28] *Id.* at 301.
[29] *Id.* at 303.
[30] *Id.* at 309.
[31] *Id.* at 314.

deserved special consideration: (1) the government's need for surveillance in order to provide for domestic security; (2) the possibility of violations of privacy and suppression of free expression; and (3) whether imposing a warrant prerequisite would impede the government's ability to protect the country.[32] The Court determined that a warrant requirement would better protect the privacy and free expression interests of the individual.[33] Then the Court rejected each of the reasons the government offered as to why a national security exception was appropriate, holding that the government had not shown a sufficient reason to carve a domestic national security exception into the Fourth Amendment.[34]

B. THE BIRTH OF FISA

Picking up on the Supreme Court's repeated insistence that *Keith* involved a purely domestic organization with no hint of foreign involvement, several federal courts in the years after *Keith* considered whether a national security exception to the Fourth Amendment existed for *foreign intelligence* gathering, almost universally answering in the affirmative.[35] For example, in one case, a defendant was convicted of interstate transportation of a firearm while under felony indictment; after the trial, the government revealed to the defense that the government possessed certain recordings of the defendant.[36] According to the district court judge, who reviewed the tapes in camera, the warrantless wiretap at issue was properly authorized by the attorney general for the purposes of collecting foreign intelligence.[37] The defendant was not a target of the wiretap; rather, the defendant had simply conversed with the targets at the location where they were under surveillance. In any event, the recorded conversation did not

---

[32] *Id.* at 314–15.
[33] *Id.* at 316–18.
[34] *Id.* at 320–21.
[35] *See* William Funk, *Electronic Surveillance of Terrorism: The Intelligence/Law Enforcement Dilemma – A History*, 11 LEWIS & CLARK L. REV. 1099, 1110 n.55 (2007) (collecting cases).
[36] *See* United States v. Brown, 484 F.2d 418, 424 (5th Cir. 1973).
[37] *Id.* at 425.

bear upon the government's case against the defendant in any way. The Court of Appeals held that the warrantless wiretaps were lawful in this case "because of the President's constitutional duty to act for the United States in the field of foreign relations, and his inherent power to protect national security in the context of foreign affairs."[38] The Court also cited pre-*Keith* Supreme Court cases stating the proposition that courts should give deference to the executive branch's need for secrecy in the realm of foreign affairs. For example, in 1948, the Supreme Court argued that

> [t]he President, both as Commander-in-Chief and as the Nation's organ for foreign affairs, has available intelligence services whose reports neither are not and ought not to be published to the world. It would be intolerable that courts, without the relevant information, should review and perhaps nullify actions of the Executive taken on information properly held secret.[39]

Minority authority, however, argued against granting a foreign intelligence national security exception to the Fourth Amendment. In *Zweibon v. Mitchell*, a plurality on the D.C. Circuit sitting en banc reversed a *Bivens*[40] action involving the Jewish Defense League, finding that—though the group engaged in international terrorism—it was a domestic organization and thus, under *Keith*, the government should not have wiretapped them without a warrant.[41] The plurality argued in dicta that even if the League did have foreign ties, the Fourth Amendment should still protect them from warrantless surveillance.[42]

---

[38] *Id.* at 426.
[39] Chicago & S. Air Lines v. Waterman S.S. Corp., 333 U.S. 103, 111 (1948), *cited in Brown*, 484 F.2d 418.
[40] Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971).
[41] *See* Zweibon v. Mitchell, 516 F.2d 594 (D.C. Cir. 1975) (en banc).
[42] *See id.* at 613.

The indeterminate legal landscape surrounding warrantless wiretaps was only one of the many forces existing in the 1970s that motivated Congress to create a statutory framework designed to regulate the collection of foreign intelligence information. First, Christopher Pyle, a former Army intelligence officer, made headlines when he alleged that the military engaged in virtually unregulated surveillance of the civilian population. This accusation resulted in a Senate inquiry and greater public and congressional awareness of clandestine intelligence operations being conducted against U.S. citizens.[43]

Second, President Nixon's Watergate scandal led to the formation of the Church Committee, which revealed that Nixon used warrantless surveillance in the name of national security to investigate U.S. citizens who were more of a political threat to Nixon than a criminal threat to anyone.[44] The Church Committee revealed more Nixon misdeeds, but also informed the public that the problem was deeper than Nixon: President Kennedy, for example, wiretapped *sans* warrant both Martin Luther King, Jr. and Jimmy Hoffa.[45] The Church Committee also fully investigated Pyle's allegations that the Army was infiltrating civil rights and anti-war groups.[46] Moreover, the Committee exposed the infamous FBI Counterintelligence Operations (COINTELPRO), which had used national security as a smokescreen to suppress domestic political dissent.[47] According to the Church Committee:

> Many of the techniques used would be intolerable in a democratic society even if all of the targets had been involved

---

[43] *See, e.g.*, Christopher M. Ford, *Intelligence Demands in a Democratic State: Congressional Intelligence Oversight*, 81 TUL. L. REV. 721, 737–38 (2007).

[44] *See* Michael P. O'Connor & Celia Rumann, *Going, Going, Gone: Sealing the Fate of the Fourth Amendment*, 26 FORDHAM INT'L L.J. 1234, 1255 (2003).

[45] *See* Evan Tsen Lee, *The Legality of the NSA Wiretapping Program*, 12 TEX. J. C.L. & C.R. 1, 39 n.142 (2006), (citing S. REP. NO. 94-755 (1976); Editorial, *Court Warrants for Traps and Stings*, N.Y. TIMES, July 5, 1990, at A16).

[46] *See id.* at 38.

[47] *See* Michael German, *Trying Enemy Combatants in Civilian Courts*, 75 GEO. WASH. L. REV. 1421, 1432 (2007).

> in violent activity, but COINTELPRO went far beyond that. The unexpressed major premise of the programs was that a law enforcement agency has the duty to do whatever is necessary to combat perceived threats to the existing social and political order.[48]

One scholar commented on the report:

> No one outside the Bureau was supposed to know that COINTELPRO existed. The lack of oversight inherent with all secret government programs allowed this program to spin out of control and expand far beyond its national security purpose. But with the lack of oversight there also came a lack of accountability, and FBI officials interviewed by the Church Committee expressed their belief that many of the COINTELPRO programs were ultimately ineffective in achieving the FBI's goal of protecting national security.[49]

Third, the telephone company (AT&T) threatened to cease cooperating with law enforcement officials for wiretapping purposes because they were worried that such cooperation could make the company vulnerable to civil lawsuits.[50]

Following Nixon's resignation and the release of the Church Committee report, the political climate was ripe for congressional action. Senator Edward Kennedy and President Gerald Ford's attorney

---

[48] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, SUPPLEMENTARY DETAILED STAFF REPORTS ON INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755, at 3 (1976), *quoted in* German, *supra* note 47, at 1432).

[49] *See* German, *supra* note 47, at 1432 (internal quotation marks omitted).

[50] Diane C. Piette & Jesselyn Radack, *Piercing the "Historical Mists": The People and Events Behind the Passage of FISA and the Creation of the "Wall,"* 17 STAN. L. & POL'Y REV. 437, 448 (2006) ("While the executive branch continued to believe it had inherent authority to conduct wiretaps, it had to face the reality that neither the telephone company nor any government official was willing to approve an electronic wiretap—without a Title III warrant—for fear of the potential legal consequences.") (internal citations omitted). This debate echoes the recent "telecom amnesty" debate in Congress. *See, e.g.*, Eric Lichtblau, *Senate Votes to Expand Spy Powers*, N.Y. TIMES, Feb. 13, 2008.

general, Edward Levi, cooperated to write what would become FISA.[51] The Senate considered the bill during the months leading up to the elections of 1976, though the final bill would not be sent to President Jimmy Carter until 1978.[52]

C. FROM FISA TO THE WALL

The preceding sections framed FISA in its historical context. The following section describes the FISA machinery as it existed upon its enactment in 1978. Subsequent sections trace FISA's evolution through the build up and, ultimately, the destruction of The Wall.

1. FISA Prior to The Wall

FISA is a complex statute. At its most basic level, it defines the procedures needed to conduct electronic surveillance to obtain foreign intelligence. Significantly, these procedures do not require getting a warrant as one would do in a criminal investigation under Title III of the Crime Control Act, the other avenue for federal officials to legally wiretap.[53] Federal officials in counterterrorism efforts may attempt to acquire a Title III warrant or a FISA warrant, which have unique requirements and have different levels of secrecy.

Title III of the Crime Control Act requires, *inter alia*, that a law enforcement officer submit to a judge a written application stating the following: the "facts and circumstances" that lead the officer to believe a serious crime[54] "has been, is being, or is about to be committed"; a description of the location "where the communication is to be intercepted"; "a particular description of the type of communications sought to be intercepted"; "the identity of the person, if

---

[51] *See* Funk, *supra* note 35, at 1112–13.

[52] *Id.* at 1113.

[53] For a comprehensive and user-friendly account of FISA procedures, see Funk, *supra* note 35, at 1114–16. *See also* David S. Kris, *The Rise and Fall of the FISA Wall*, 17 STAN. L. & POL'Y REV. 487, 489–94 (2006). For an explanation of Title III warrant procedures, see Kevin S. Bankston, *Only the DOJ Knows: The Secret Law of Electronic Surveillance*, 41 U.S.F. L. Rev. 589, 592 (2007); 18 U.S.C. §§ 2510–2520 (1968).

[54] The list of serious crimes is too long to reprint here, but may be found at 18 U.S.C. § 2516(1) (2008).

known, committing the offense and whose communications are to be intercepted";[55] and "a full and complete statement as to whether or not other investigative procedures have been tried and failed or why they reasonably appear to be unlikely to succeed if tried or to be too dangerous."[56] The judge may require more information from the applying officer.[57] If the judge is convinced that there is probable cause to believe a crime was, is, or will be committed; that there is probable cause to believe communications about the crime will be intercepted at the requested location; and that other investigative techniques will fail or are too dangerous, then the judge may authorize an agency to intercept the targeted communications for a period of up to thirty days with extensions possible if the officer submits another application.[58] The target must be notified of the surveillance within ninety days.[59]

Like Title III, FISA authorizes electronic surveillance, but FISA covers a narrower range of circumstances. The targeted entity must be a foreign power[60] or an agent of a foreign power (hereinafter simply "foreign power").[61] The targeted communications must relate to "the ability of the United States to protect against"[62] a foreign power's efforts to engage in attack, sabotage,[63] international terrorism,[64] or clandestine intelligence activities.[65] If the intelligence information concerns a "United States person,"[66] the information must be *necessary* to prevent an attack, sabotage, etc., and not just "relate" to the United States' ability to do so.[67]

---

[55] 18 U.S.C. § 2518(1)(b) (2008).
[56] *Id.* § 2518(1)(c).
[57] *Id.* § 2518(2).
[58] *Id.* §§ 2518(3), (5).
[59] *Id.* § 2518(8)(d).
[60] *Id.* § 1801(a).
[61] *Id.* § 1801(b).
[62] *Id.* § 1801(e).
[63] *Id.* § 1801(d).
[64] *Id.* § 1801(c).
[65] *Id.* § 1801(e)(1)(C).
[66] *Id.* § 1801(i).
[67] *Id.* § 1801(e)(2).

There are two sets of procedures that the government may use in order to collect foreign intelligence without a warrant. Under the first set of procedures, the attorney general may authorize surveillance for up to one year if the attorney general certifies in writing under oath that (1) the surveillance is solely directed at communications between foreign powers and (2) there is no substantial likelihood that communications of U.S. persons will be intercepted.[68]

The second set of procedures cover any circumstances other than those covered by the first set of procedures, and they are substantially more comprehensive.[69] The attorney general must submit an application to the Foreign Intelligence Surveillance Court ("FISC"), a court created by FISA and consisting of federal district court judges appointed by the Chief Justice of the United States Supreme Court.[70] The application must contain the following items, inter alia, which a FISC judge may supplement with additional requirements:[71] (1) the identity or description of the target and how long surveillance will be necessary; (2) the facts that justify the belief that the target is a foreign power or an agent of a foreign power, and that the facilities targeted are or will be used by a foreign power or an agent of a foreign power;[72] (3) the minimization procedures to be used; (4) a description of the type of communications and information sought by the surveillance; and (5) a certification from the Assistant to the President for National Security Affairs stating that the "purpose of the surveillance is to obtain foreign intelligence

---

[68] *Id.* § 1802(a)(1)(A)–(B).
[69] *See id.* § 1802(b).
[70] *Id.* § 1803.
[71] *See generally id.* § 1804.
[72] "Essentially, a foreign power includes foreign governments (e.g., the government of Russia), factions of foreign governments not substantially comprised of U.S. persons (e.g., the PLO), entities directed and controlled by foreign governments (e.g., OPEC), a group engaged in or preparing to engage in international terrorism (e.g., al-Qaeda), and foreign-based political organizations not substantially comprised of U.S. persons (e.g., foreign political parties)." Kris, *supra* note 53, at 490–91 (citations omitted).

information"[73] and that "such information cannot reasonably be obtained by normal investigative techniques."[74]

The FISA judge must issue the warrant if he or she determines that there is probable cause to believe that the target is a foreign power and that the facilities targeted will be used by that foreign power.[75] The warrant may authorize surveillance of a foreign power for one year and may authorize surveillance of an agent of a foreign power for up to ninety days, with extensions possible for both.[76]

FISA also provides for the establishment of a Foreign Intelligence Surveillance Court of Review (FISCR) in the event that a FISC ruling is challenged. The FISCR did not convene until the first appeal, *In re Sealed Case*, occurred in 2002.[77]

In sum, FISA grants broader authority than Title III, but under a narrower range of circumstances. A Title III application may be made to any United States District Court judge, whereas a FISA application must be made to a specially appointed FISA judge. A Title III warrant must be disclosed to the target within ninety days, whereas a FISA warrant is kept secret. In order to benefit from this higher level of secrecy, the government bears a burden of showing that there is probable cause to believe that the target is a foreign power and that the targeted information relates to the ability of the United States to protect against spying or terrorism. Furthermore, FISA requires a high level Justice Department official to certify the application; these requirements are not present in Title III.

2. The Development of The Wall

The Wall is a metaphor used to describe the inability of federal law enforcement officials and intelligence officials to coordinate, advise, and share information with each other pursuant to procedures adopted by the Justice Department in 1995 (hereinafter "the

---

[73] 50 U.S.C. § 1804(a)(7)(B).
[74] *Id.* § 1804(a)(7)(E)(ii).
[75] *Id.* § 1805(a)(3).
[76] *Id.* § 1805(e).
[77] *See In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

1995 Procedures").[78] It is (almost) universally acknowledged that the original FISA statute did not contain The Wall, at least not to its fullest extent.[79] Few people outside the legal world were aware of The Wall's existence until the weeks following September 11, 2001, when some people attributed to The Wall intelligence failures that allowed the terrorist attacks to happen.[80] This section covers the events that contributed to the development of The Wall between the enactment of FISA in 1978 and the jurisprudence surrounding the USA PATRIOT Act.

The story of The Wall largely depends upon who is speaking. After the events of September 11, 2001, explanations for The Wall proliferated, each with an emphasis on a different historical event. Andrew McCarthy, a former federal prosecutor in the Southern District of New York who led the prosecution against Sheik Omar Abdel Rahman for his involvement in the first World Trade Center terrorist attack, pointed his finger at Deputy Attorney General Jamie Gorelick for both writing a 1995 memo that advocated wall-like restrictions and for her instrumental role in writing and convincing

---

[78] *See* OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS (NOVEMBER 2004) 26 (2006), *available at* http://www.fas.org/irp/agency/doj/oig/fbi-911/index.html [hereinafter OIG REPORT] (arguing that Richard Scruggs advocated a "Chinese Wall" between criminal and intelligence investigators—the first time the word "wall" was used in this context); Memorandum from Janet Reno, Attorney Gen. of the U.S., on Procedures for Contacts Between the FBI and the Criminal Div. Concerning Foreign Intelligence and Foreign Counterintelligence Investigations to Assistant Attorney Gen. of the Criminal Div., the Dir. of the FBI, Counsel for Intelligence Policy, and U.S. Attorneys (July 19, 1995), *available at* http://www.fas.org/irp/agency/doj/fisa/1995procs.html [hereinafter 1995 Procedures].

[79] *See, e.g.*, Piette & Radack, *supra* note 50, at 452 (arguing that The Wall did not exist at least until after Mary Lawton died); Andrew C. McCarthy, *The Wall Truth*, NAT'L REV. ONLINE, Apr. 19, 2004, http://www.nationalreview.com/mccarthy/mccarthy200404190849.asp (arguing that Jamie Gorelick was instrumental in creating The Wall during the Clinton Administration). *But see* Jamie S. Gorelick, *The Truth About 'the Wall,'* WASH. POST, Apr. 18, 2004, at B07 (implying that The Wall was inherent in FISA and was slowly built up over time).

[80] *See* Tung Yin, *The Impact of the 9/11 Attacks on National Security Law Casebooks*, 19 ST. THOMAS L. REV. 157, 167 n.46 (2006) (collecting citations to media articles linking The Wall to 9/11).

Attorney General Janet Reno to adopt the 1995 Procedures. Gorelick, meanwhile, argued that The Wall was compelled by judicial decisions interpreting FISA.[81] The FISCR decision and the Justice Department Inspector General's review of the FBI's treatment of intelligence information prior to September 11, 2001 highlighted the role of the decision in *United States v. Truong* and implied that The Wall had existed since the early 1980s.[82] Former Associate Deputy Attorney General David Kris placed blame on all three branches of the federal government. Scholars Diane Piette and Jesselyn Radack offered a novel explanation for the development of The Wall: the untimely death of the Office of Intelligence Policy and Review ("OIPR") chief Mary Lawton and the resulting turf wars between entities battling to fill the gap she left.[83] A comprehensive evaluation of these different narratives is beyond the scope of this note, though I draw upon all of them in attempting to reconstruct a historically accurate account of the development of The Wall. This section, therefore, focuses on key events that inarguably assisted in the creation of The Wall.

a. United States v. Truong

Truong was wiretapped by the FBI, without a warrant, pursuant to the attorney general's authorization that such surveillance was necessary to acquire foreign intelligence information.[84] Truong had given classified information to Vietnamese government officials.[85] Ultimately, the government decided to criminally prosecute Truong. The defense objected on Fourth Amendment grounds to

---

[81] *See* Gorelick, *supra* note 79.

[82] *See In re* Sealed Case, 310 F.3d 717, 725 (FISA Ct. Rev. 2002); OIG REPORT, *supra* note 78, at 23–24.

[83] Piette & Radack, *supra* note 50, at 467 ("[Immediately after Lawton's death,] [t]he jockeying for power began in earnest. When the dust settled two years later, the Truong analysis and the 'wall' were viewed as official [Justice] Department policy.") (internal citations omitted).

[84] *See* United States v. Truong Dinh Hung, 629 F.2d 908, 912 (4th Cir. 1980). *Truong* is a case in which the warrantless surveillance at issue was conducted prior to the enactment of FISA and was therefore judged according to pre-FISA law.

[85] *Id.* at 911.

the government's use of evidence derived from warrantless surveillance, while the government argued that the foreign intelligence exception created in the aftermath of the Supreme Court's *Keith* decision permitted the surveillance. The district court split the difference, holding that once criminal prosecution became the "primary purpose" of the surveillance, a warrant was required. Since the court could not read minds to determine when the purpose of the surveillance changed, the court held that the date that the federal prosecutors with the Justice Department became involved was the watershed moment when the investigation ceased being "primarily" to obtain foreign intelligence information and began being "primarily" for criminal prosecution.[86] The Court of Appeals for the Fourth Circuit affirmed, holding that:

> [O]nce surveillance becomes primarily a criminal investigation, the courts are entirely competent to make the usual probable cause determination, and because, importantly, individual privacy interests come to the fore and government foreign policy concerns recede when the government is primarily attempting to form the basis for a criminal prosecution.[87]

Truong's impact is a matter of historical dispute. According to the FISCR decision, the Justice Department read *Truong*'s "primary purpose" standard into FISA at some point during the 1980s.[88] Piette and Radack argue, however, that the Justice Department never regarded *Truong* as influencing Department policy because the enactment of FISA made the question moot.[89] Piette and Radack

---

[86] *Id.* at 916.
[87] *Id.* at 915.
[88] *In re* Sealed Case, 310 F.3d 717, 727 (Foreign Intelligence Surveillance Ct. Rev. 2002).
[89] *See* Piette & Radack, *supra* note 50, at 461 ("Contrary to the FISCR's assertion, *Truong* was a standard embraced by defense attorneys, but viewed as a non-factor at the Justice Department (and particularly within OIPR) when it came to electronic surveillance during the 1980s.").

interviewed several officials from the 1980s Justice Department, who confirmed that, in the words of the first OIPR chief Kenneth Bass, "[f]rom the beginning of FISA there was always communication and interaction between the two divisions [law enforcement and intelligence]."[90] Piette and Radack also cite to an internal Justice Department memo reviewing the Los Alamos National Laboratory investigation ("Bellows Report"), which confirms that Mary Lawton allowed until her death, as a matter of unwritten policy, the routine interaction of intelligence and law enforcement officials.[91] Piette and Radack's argument, if true, casts substantial doubt on Jamie Gorelick's account of The Wall, which claims The Wall was compelled by judicial decisions. It is critical to note, however, that Piette and Radack's argument hinges on unverified interviews and telephone conversations with Justice Department officials, and it is therefore possible that they did not interview a representative sample of Justice Department officials or that they did not accurately construe the substance of their interviewees' opinions. Piette and Radack's methods are arguably justified due to a lack of written record of the Lawton era (due to Lawton's apparent practice of leaving unwritten the regulation of law enforcement and intelligence official communication). The gravamen of Piette and Radack's argument, however—that Lawton allowed more communication than later regulations—has yet to be criticized in the legal academic literature.

It is uncontested that the "primary purpose" standard as applied to FISA continued to evolve in the federal courts throughout the 1980s and early 1990s; the exact nature of the evolution, however, is difficult to trace due to two factors. First, every federal court to consider a defendant's motion to suppress FISA evidence on the grounds that the purpose of the search was to obtain a criminal

---

[90] Piette & Radack, *supra* note 50, at 461 (quoting Interview by Diane Carraway Piette & Jesselyn Radack with Kenneth C. Bass, III, former Counsel for Intelligence Policy at the U.S. Dep't of Just. (July 29, 2003)).

[91] Piette & Radack, *supra* note 50, at 464 (citing DEP'T OF JUSTICE, ATT'Y GEN.'S REV. TEAM ON THE HANDLING OF THE LOS ALAMOS NAT'L LAB. INVESTIGATION, FINAL REPORT, 711 (May 2002), *available at* http://www.usdoj.gov/ag/readingroom/bellows.htm [hereinafter BELLOWS REPORT]).

prosecution, not foreign intelligence information, either held or assumed that the primary purpose of a FISA search must be to obtain foreign intelligence information.[92] Second, and somewhat paradoxically, no federal court ever found that the "primary purpose" standard had been breached, and—consequently—no federal court ever suppressed FISA-derived evidence on the grounds that the purpose of the investigation was not primarily to obtain foreign intelligence information.[93] In sum, it is difficult to pinpoint whether the exact wording of the "primary purpose" standard was in dispute—every time a court was presented with the situation, the evidence was admissible under the stricter standard anyway. According to one scholar, "[m]any courts simply assumed such a requirement [the "primary purpose" standard], probably because the government did not contest the issue."[94]

Much later, the FISCR expressed dismay that courts did not subject their gradual shift to the "primary purpose" standard to greater scrutiny:

> It is almost as if [the cases] assume that the government seeks foreign intelligence information . . . for its own sake—to expand its pool of knowledge—because there is no discussion of how the government would use that information outside criminal prosecutions. That is not to say that the government could have no other use for that information. The government's overriding concern is to stop or frustrate the agent's or the foreign power's activity by any means, but if one considers the actual ways in which the government would foil espionage or terrorism it becomes apparent that criminal prosecution analytically cannot be placed easily in a separate response category.[95]

---

[92] *See* Funk, *supra* note 35, at 1123–24 nn.135–39 (collecting cases).
[93] *See id.*
[94] *Id.* at 1123.
[95] *In re* Sealed Case, 310 F.3d 717, 727 (FISA Ct. Rev. 2002).

In sum, the *Truong* progeny was not a series of dramatic wins for defendants in which the "primary purpose" standard was definitively articulated. Rather, the cases did not appear to impact the Department of Justice; Mary Lawton consistently permitted law enforcement and intelligence officials to cooperate on investigations until her death. The FISCR said that the historical origins of The Wall are "shrouded in historical mist[s]."[96] If Piette and Radack, as well as Andrew McCarthy, are to be believed, however, then there is no mystery: Jamie Gorelick built The Wall in 1995.

b. The Gorelick Memo and the 1995 Procedures

Upon the unexpected death of Mary Lawton in 1993, Attorney General Janet Reno appointed Richard Scruggs—whom she knew from her work in Florida and who had little national security experience—to be the head of OIPR.[97] Scruggs was worried about the lack of formal, written procedures governing the relationship of criminal investigators and intelligence officials (Lawton believed that FISA required flexibility, and therefore her procedures were unwritten).[98] Scruggs issued memoranda instructing intelligence and criminal officials that any contact between the two groups must be approved by OIPR.[99] The FBI and the Criminal Division within the Department of Justice rebelled against Scruggs, and Reno was caught in the middle.[100] She appointed Jamie Gorelick to head a group that would propose procedures for regulating the relationship of criminal and intelligence officials, as well as the role of OIPR as a conduit on information between the two.[101] Gorelick's memo suggested written regulations, which were formally adopted in the 1995 Procedures.[102] According to Gorelick, her procedures "exceeded

---

[96] *Id.*
[97] *See* Piette & Radack, *supra* note 50, at 471.
[98] *See id.* at 472.
[99] *See id.* at 473–74; Funk, *supra* note 35, at 1126.
[100] *See* Piette & Radack, *supra* note 50, at 474.
[101] *See id.* at 466.
[102] *See id.* at 480–81; 1995 Procedures, *supra* note 78.

the requirements of FISA and then-existing federal case law" in regulating information sharing.[103]

The 1995 Procedures turned the "primary purpose" standard into written Justice Department policy and ultimately had the effect of limiting the coordination between intelligence and criminal officials who wanted to avoid the appearance that a foreign intelligence investigation was becoming a criminal investigation.[104] By their own terms, the 1995 Procedures did not totally ban the sharing of information between criminal and intelligence officials; they simply heavily regulated that communication. However, the procedures for passing information "over the wall"—the slang phrase for transferring information between intelligence and criminal officials—were often so burdensome or complicated that officials simply chose not to share information.[105]

The Wall grew "higher" in 2000 when the FISC issued a new rule requiring FBI officials who received FISA information to sign a certification declaring that they understood the requirements of The Wall.[106] According to one source in the FBI, the new requirement "'shut down' the flow of information in the FBI."[107] The OIG Report quoted FBI agents saying the "walls were viewed as a 'maze' that no one really understood or could easily navigate."[108]

D. THE USA PATRIOT ACT

The terrorist attacks of September 11, 2001, spawned the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("USA PATRIOT Act"), which considerably dismantled The Wall.[109] This section reviews the significance of the USA PATRIOT Act changes.

---

[103] *See* McCarthy, *supra* note 79.
[104] Kris, *supra* note 53, at 502–03.
[105] *See* OIG REPORT, *supra* note 78, at 280.
[106] *Id.* at 344.
[107] *Id.*
[108] *See id.* at 345.
[109] *See* USA PATRIOT Act, *supra* note 4.

First, the USA PATRIOT Act changed the FISA requirement that a government official certify that *the* purpose of the surveillance was to collect foreign intelligence information—*a significant* purpose to do so would suffice.[110] After the original FISA, courts had interpreted "the purpose" to mean "the primary purpose." This meant that prior to the USA PATRIOT Act, evidence derived from FISA surveillance after law enforcement became the purpose of the surveillance could be excluded.[111] Since it is difficult to tell exactly when the purpose of surveillance changes, *Truong* had held that the watershed date was when criminal investigators became involved in the investigation; FISA evidence gathered after that date, then, could theoretically be suppressed.[112] Upon the adoption of the 1995 Procedures, prosecutors and law enforcement officials were virtually banned from assisting or advising intelligence officials engaged in FISA surveillance.[113] By changing "the purpose" to "a significant purpose," the USA PATRIOT Act knocked out the foundation for The Wall. According to Sen. Dianne Feinstein, these changes were necessary to make it

> easier to collect foreign intelligence information under . . . FISA. Under current law, authorities can proceed with surveillance under FISA only if the primary purpose of the investigation is to collect foreign intelligence.
>
> But in today's world things are not so simple. In many cases, surveillance will have two key goals—the gathering of foreign intelligence, and the gathering of evidence for a criminal prosecution. Determining which purpose is the "primary" purpose of the investigation can be difficult, and

---

[110] Section 218 of the PATRIOT Act reads, in its entirety: "Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking 'the purpose' and inserting 'a significant purpose'." USA PATRIOT Act, *supra* note 4, § 218.

[111] *See supra* Part II.C.2.a.

[112] *See supra* Part II.C.2.a.

[113] *See supra* Part II.C.2.b.

> will only become more so as we coordinate our intelligence and law enforcement efforts in the war against terror.[114]

Later, the FISCR decision argued that this USA PATRIOT Act provision was unnecessary because—for FISA—"the purpose," aside from the interpretation given to it by the 1995 Procedures, never meant that foreign intelligence information could not be shared with law enforcement officials.[115] In other words, The Wall was a creation of Gorelick's 1995 Procedures, not an inherent piece of the original FISA legislation.

The USA PATRIOT Act's second major change to FISA took direct aim at the 1995 Procedures. The USA PATRIOT Act provided that, with respect to both physical searches and electronic surveillance, federal officers executing a FISA warrant "may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against": (1) "actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power"; (2) "sabotage or international terrorism by a foreign power or an agent of a foreign power"; or (3) "clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power."[116]

Furthermore, the USA PATRIOT Act said that such consultation "shall not preclude" the required certification stating that a significant purpose of the surveillance is to obtain foreign intelligence information.[117] According to David Kris, this section of the USA PATRIOT Act provided that "by definition, coordination authorized by [the USA PATRIOT Act] must further a purpose to protect against the threats specified in the definition of 'foreign

---

[114] *In re* Sealed Case, 310 F.3d 717, 732–33 (FISA Ct. Rev. 2002) (quoting 147 CONG. REC. S10591 (2001) (statement of Sen. Feinstein)).

[115] *See id.* at 727 ("In sum, we think that the FISA as passed by Congress in 1978 clearly did *not* preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution.").

[116] USA PATRIOT Act, *supra* note 4, § 504 (creating 50 U.S.C. §§ 1806(k)(1), 1825(k)(1)).

intelligence information.' Accordingly, authorized coordination cannot 'preclude' a purpose to obtain foreign intelligence information—on the contrary, it is affirmative evidence of that purpose."[118]

E. IN RE SEALED CASE

The parts of the USA PATRIOT Act mentioned above led to three unprecedented events in the history of FISA. First, after the Ashcroft Justice Department submitted their proposed regulations ("the 2002 Procedures")[119]—which implemented the USA PATRIOT Act and repudiated much of the 1995 Procedures—to the FISC for review, the FISC struck down and rewrote much of the proposal.[120] This was the first time the government appealed the FISC's decision. Second, and again for the first time, the FISC released its opinion to the public.[121] Third, since the government never appealed before, the FISCR had never convened.[122] When it did so, the FISCR strongly rejected the FISC's attempt to rebuild The Wall.[123] This section examines how the FISA courts and Justice Department wrangled over the implementation of the USA PATRIOT Act.

The Justice Department's proposed procedures implementing the USA PATRIOT Act in the early months of 2002 contained three major differences vis-à-vis the 1995 Procedures.[124] First, the procedures restated the USA PATRIOT Act change from "the purpose" to "a significant purpose."[125] The procedures explained that the change

---

[117] *Id.*
[118] Kris, *supra* note 53, at 509.
[119] Memorandum from John Ashcroft, Attorney Gen. of the U.S. on Intelligence Sharing Procedures for Foreign Intelligence and Foreign Counterintelligence Investigations Conducted by the FBI to Director of the FBI, Assistant Attorney Gen. for the Criminal Div., Counsel for Intelligence Policy, and U.S. Attorneys (Mar. 6, 2002), *available at* http://www.fas.org/irp/agency/doj/fisa/ag030602.html [hereinafter 2002 Procedures].
[120] *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. Rev. 2002).
[121] *See* Piette & Radack, *supra* note 50, at 439.
[122] *Id.* at 440.
[123] *See In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).
[124] *See* 2002 Procedures, *supra* note 119.
[125] *Id.* at Part I.

"allow[ed] FISA to be used *primarily* for a law enforcement purpose, as long as a significant foreign intelligence purpose remain[ed]."[126]

Second, the procedures instructed the FBI to inform the Criminal Division and OIPR of all information necessary to protect the United States from terrorism,[127] including information that a crime "has been, is being, or is about to be committed."[128] Thus, a major part of The Wall was dismantled: information could be given to law enforcement officials without bit-by-bit review.[129]

Third, the procedures allowed the FBI, Criminal Division, and OIPR to consult and advise each other (with all or any combination of the three present) on any open foreign intelligence investigations.[130] Contrary to the 1995 Procedures, the 2002 Procedures allowed consultation and advice on a wide scope of issues in an investigation, including "the strategy and goals for the investigation; the law enforcement and intelligence methods to be used in conducting the investigation; the interaction between intelligence and law enforcement components as part of the investigation; and the initiation, operation, continuation, or expansion of FISA searches or surveillance."[131]

Upon submission of the procedures, the FISC permitted some of the procedures but struck down and rewrote the provision allowing criminal investigators to advise and coordinate with intelligence officials.[132] The court allowed some contact between law enforcement and intelligence officers, but not on the expansive scope of issues called for in the procedures. For example, the procedures called for law enforcement advice on "the initiation, operation, continuation, or

---

[126] *Id.*

[127] As well as "foreign attack," "sabotage," and "clandestine intelligence activities." *Id.* at Part II.A.

[128] *Id.*

[129] *See* Kris, *supra* note 53, at 510–11 (explaining the significance of Part II.A of the 2002 Procedures).

[130] 2002 Procedures, *supra* note 119, at Part II.B.

[131] *Id.*

[132] *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (FISA Ct. Rev. 2002).

expansion of FISA searches or surveillance."[133] The FISC deleted that paragraph and added a significantly stricter one stating that

> [L]aw enforcement officials shall *not* make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances. Additionally, the FBI and the Criminal Division shall ensure that law enforcement officials do not direct or control the use of the FISA procedures to enhance criminal prosecution, and that advice intended to preserve the option of a criminal prosecution does not inadvertently result in the Criminal Division's directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives.[134]

Furthermore, the FISC demanded that the OIPR be present at all meetings between intelligence and law enforcement officials, a provision David Kris, the Justice Department lawyer who argued the case before the FISC, termed a "chaperone" requirement.[135] This requirement harkened back to the 1995 Procedures, which mandated that the FBI give an opportunity for the OIPR to participate in meetings between intelligence and law enforcement officials and required the FBI to give the OIPR a summary of the substance of the meeting if the OIPR did not participate.[136]

The government appealed the FISC decision. Since the government was the only party to the FISC case, the FISCR permitted the ACLU and the National Association of Criminal Defense Lawyers to submit briefs in opposition to the government.[137] When it became apparent that the constitutionality of the USA PATRIOT Act changes

---

[133] 2002 Procedures, supra note 119, at Part II.B.
[134] *See In re* All Matters Submitted to the Foreign Intelligence Surveillance Court, 218 F. Supp. 2d, at 626–27 (emphasis added).
[135] *Id.*; *see* Kris, *supra* note 53, at 511–12.
[136] *See* 1995 Procedures, *supra* note 78.
[137] *In re* Sealed Case, 310 F.3d 717, 719 (FISA Ct. Rev. 2002).

was a major issue, the FISCR called for further briefing from all parties.[138] After oral argument, the FISCR released its decision.

First, the FISCR expressed concern about whether the FISC had the authority to rewrite the procedures, since that authority appeared to belong to the Department of Justice.[139] The real issue, then, was whether FISA or the Fourth Amendment compelled the court to strike down the procedures.

The FISCR held that the procedures were consistent with both the Constitution and FISA. For the statutory argument, the court reviewed the history of the "primary purpose" test and concluded that despite its seeming popularity, no federal court had fully explained its decision to adopt the test, nor had they grounded their adoption of the test in any constitutional or statutory language.[140] According to the court, previous cases endorsing the "primary purpose" test simply assumed, without explanation, that intelligence operations were conducted simply to learn information, not to interfere or file charges against targets.[141] In sum, the FISCR did not find the prior case law on the "primary purpose" test—nor the FISC's reliance on that case law—persuasive. Nothing in FISA—nor the USA PATRIOT Act modifications—compelled any conclusion contrary to the 2002 Procedures.[142]

The court went on to hold that the 2002 Procedures implementing the USA PATRIOT Act did not violate the Fourth Amendment due to the fact that the government's need for flexibility in the area of foreign intelligence, combined with the safeguards inherent in FISA, rendered the procedures "reasonable" under the standard

---

[138] *Id.* at 719.
[139] *Id.* at 731–32 (*stating* "[t]he FISA court asserted authority to govern the internal organization and investigative procedures of the Department of Justice which are the province of the Executive Branch (Article II) and the Congress (Article I). Subject to statutes dealing with the organization of the Justice Department, however, the Attorney General has the responsibility to determine how to deploy personnel resources.").
[140] *Id.* at 726–27.
[141] *Id.* at 727.
[142] *Id.* at 736.

articulated by the Supreme Court in *Keith*.[143] *Keith*, as stated above,[144] weighed the government's need for the information against the risk of the deprivation of an individual's privacy rights, along with the ability of the government to acquire the information another way.[145] While the amici argued that *Truong* was strong authority on the constitutional necessity of the "primary purpose" test, the FISCR agreed with the government that the newly created "significant purpose" test was constitutionally satisfactory.[146]

According to the court, *Truong*'s distinction between surveillance for intelligence and law enforcement purposes was both analytically arbitrary and difficult to administer. It was arbitrary, the court wrote, because the government can have more than one purpose—the government can maintain its foreign policy purpose while becoming increasingly concerned with charging the target of the surveillance with a crime.[147] The *Truong* standard was difficult to administer as well because inquiring into the subjective motivations of complex government actors is a difficult task; indeed, *Truong* had to use a crude proxy for intent, i.e., the involvement of law enforcement officials in the investigation.[148] This turned a difficult standard into a bad standard because it gave the government "perverse organizational incentives" to exclude the

---

[143] The FISC did not explicitly strike down the procedures as violative of the Fourth Amendment, but rather, the FISC repeatedly invoked privacy rights as the driving force of the their decision. The FISCR, therefore, felt compelled to address the Fourth Amendment arguments, which is why it called for supplemental briefing from the government and *amici*. *Id.*at 737; *see* discussion *supra* Part I.A (discussing *Keith*).

[144] *See supra* text accompanying notes 31–34.

[145] *See* discussion *supra* Part II.A.

[146] *In re* Sealed Case, 310 F.3d 717, 742–44 (FISA Ct. Rev. 2002).

[147] *Id.* at 743 (*stating* "[t]he false premise [in *Truong*] was the assertion that once the government moves to criminal prosecution, its 'foreign policy concerns' recede. . . . [T]hat is simply not true as it relates to counterintelligence. In that field the government's primary purpose is to halt the espionage or terrorism efforts, and criminal prosecutions can be, and usually are, interrelated with other techniques used to frustrate a foreign power's efforts.").

[148] *Id.*

valuable experience of law enforcement officials in foreign intelligence investigations.[149]

F. MAYFIELD V. UNITED STATES

Courts continued to hear challenges to the USA PATRIOT Act in the years after the FISCR decision, and the courts upheld the changes to FISA until *Mayfield v. United States* in 2007.[150]

Soon after the Madrid train bombings of 2004, the Spanish government obtained a fingerprint from a bag containing detonators.[151] The Spanish authorities sent the fingerprint to the FBI, which ran it through an automated computer system and identified possible suspects but failed to find an exact match. The fingerprint was then analyzed by the FBI's own fingerprint specialists as well as an independent contractor, both of whom concluded that the fingerprint matched one of the suspects, Brandon Mayfield, who was a U.S. citizen and an attorney.[152] The FBI began to watch Mayfield and his family and then applied for a FISA warrant.[153] After surveillance, a federal judge issued a warrant to have Mayfield arrested as a material witness.[154] Mayfield claimed he was innocent and that he had not been out of the country in years, so the judge appointed a fingerprint expert chosen by Mayfield's counsel to evaluate the government's evidence. The expert confirmed that the fingerprint found in Spain matched Mayfield's.[155] The judge then issued search warrants, and federal officials seized papers in Mayfield's home and office.[156] After Mayfield spent two weeks in detention, the Spanish authorities notified the FBI

---

[149] *Id.* (citing the BELLOWS REPORT, *supra* note 91, at 723–26).
[150] *Mayfield*, 504 F. Supp. 2d 1023 (D. Or. 2007). For cases upholding the USA PATRIOT Act, see, for example, United States v. Wen, 477 F.3d 896, 898 (7th Cir. 2007); United States v. Damrah, 412 F.3d 618 (6th Cir. 2005); United States v. Holy Land Found. for Relief and Dev., 2007 WL 2011319 (N.D. Tex. 2007); United States v. Mubayyid, 521 F. Supp. 2d 125 (D. Mass. 2007).
[151] *Mayfield*, 504 F. Supp. 2d at 1026–27.
[152] *Id.* at 1027–28.
[153] *Id.* at 1028.
[154] *Id.*
[155] *Id.* at 1029.
[156] *Id.*

that they had arrested an Algerian suspect who matched the fingerprint found on the bag of explosives.[157]

Mayfield was then released. He filed a *Bivens*[158] claim against the government and asked the court to declare that certain FISA provisions were unconstitutional.[159] Mayfield settled with the government for the arrest, but the court ruled he had standing to challenge FISA because the government continued to possess copies of FISA-derived surveillance of him and his family.[160]

The court struck down FISA as violative of the Fourth Amendment's traditional requirements of notice and particularity.[161] The court suggested that FISA was constitutional prior to the USA PATRIOT Act because it met the Supreme Court's "special needs" exception, but after the USA PATRIOT Act replaced the "primary purpose" test and allowed FISA warrants as long as obtaining foreign intelligence information was a "significant purpose," then the traditional Fourth Amendment standards applied.[162]

The *Mayfield* court appeared cognizant of the fact that the government was dissatisfied with The Wall and that the "primary purpose" standard was the foundation of The Wall. The court, however, assured the government that *Mayfield* would not rebuild The Wall because the other Wall-related USA PATRIOT Act provision, section 504 (the consultation provision),[163] was not challenged in this case.[164]

---

[157] *Id.*

[158] *See* Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971).

[159] *Mayfield,* 504 F. Supp. 2d 1029.

[160] *Id.* at 1034. One scholar has expressed doubt that the Court's standing analysis will survive on appeal. *See* Posting of Orin Kerr to The Volokh Conspiracy, http://www.volokh.com/archives/archive_2007_09_23-2007_09_29.shtml#1190858591 (Sept. 27, 2007, 11:59 EST).

[161] *Mayfield*, 504 F. Supp. 2d. at 1039–41.

[162] *Id.* at 1041–42.

[163] USA PATRIOT Act, *supra* note 4, at § 504.

[164] *Mayfield*, 504 F. Supp. 2d at 1041. The Court addressed The Wall in only one sentence of the decision: "However, a provision of the Patriot Act, unchallenged by

II. THE IMPACT OF THE WALL ON FEDERAL INVESTIGATIONS

The previous Parts traced the evolution of foreign intelligence gathering from pre-FISA practices to the litigation surrounding implementation of the USA PATRIOT Act. This Part commences the normative analysis, arguing that The Wall hampered the effectiveness of federal investigations. Critics of the USA PATRIOT Act have defended The Wall largely on privacy grounds but have not undertaken a serious look at what a renewed Wall would mean for national security.[165] Opponents of The Wall are plentiful and passionate, but their literature is largely confined to reports evaluating The Wall in response to specific counterintelligence failures as opposed to a general and systematic evaluation of The Wall en toto.[166] This section attempts to fill this gap by providing a more comprehensive critique of The Wall.

The arguments against The Wall tend to fall into three separate themes. First, The Wall is so confusing that when it attempts to control the flow of intelligence information, it actually bans it. Second, excluding criminal law officials from intelligence investigations is unwise because the tools and expertise of these officials is an invaluable resource in most investigations. Third, the separation of criminal and intelligence officials leads to duplicative investigations, wasting resources. These themes are not meant to be completely analytically distinct; rather, they are general categories of complaints that may "feed" off each other. For example, when agents are confused about The Wall's requirements, they may spend valuable time and resources seeking legal advice on how to comply with the regulations instead of actively conducting an investigation.[167] This Part concludes with a case study of The Wall's

---

plaintiffs here, eliminates the DOJ 'wall' and with it the 'dangerous confusion' and 'perverse organizational incentives' referred to and relied on by the FISCR." *Id.*

[165] *See, e.g.*, Herman, *supra* note 2; Banks, *supra* note 2.

[166] *See, e.g.*, OIG REPORT, *supra* note 78 (responding to the 9/11 attacks); BELLOWS REPORT, *supra* note 91 (responding to the Wen Ho Lee investigation).

[167] *See infra* Part III.D (outlining the FBI's pursuit of 9/11 hijacker al-Mihdhar).

impact on the botched Al-Mihdhar investigation prior to the September 11 attacks.

A. CONFUSION

The 1995 Procedures did not aim to ban information sharing, merely regulate it. Yet this produced a system that was so complex that government officials tended to simply not share information at all given the level of training they received and the number of personnel and resources at their disposal. Many government officials thought The Wall was so unnecessarily complicated that it was not worth their time to pass information over it.[168] For example, the National Security Agency (NSA) was notified that it needed to classify its counterterrorism information as either FISA-derived or not so that non–FISA-derived information could be passed to criminal investigators. The NSA processed so much information, however, it determined that such piece-by-piece classification would be impossible without a massive increase in personnel and resources.[169] Therefore, the NSA classified *all* information as FISA-derived and passed none to criminal investigators.[170]

Additionally, the complexity of the 1995 procedural rules gave criminal officials such significant disincentives against giving advice to intelligence officials that, in practice, no advice was given. While the procedures only banned law enforcement officials from "'directing or controlling the [. . .] investigation toward law enforcement objectives,'" few understood this clearly, therefore most opted to play it safe and not give any advice.[171] Compounding this problem, the deputy director of the FBI informed agents that violation of the 1995 Procedures was a "career stopper";[172] individual officials, therefore,

---

[168] *See supra* Part II.C.2.
[169] *See* OIG REPORT, *supra* note 78, at 280.
[170] *Id.*
[171] Kris, *supra* note 53, at 505 (quoting the 1995 Procedures, *supra* note 78).
[172] Piette & Radack, *supra* note 50, at 475.

faced significant incentives to not test the limits of the procedures.[173] According to the OIG Report, an FBI unit chief "stated that FBI Headquarters employees became worried that any misstep in handling FISA information could result in harm to their careers."[174]

It is important to note that The Wall was at least indirectly responsible for these confusions within the system as it then existed. While it is possible that more training and resources could have potentially averted the confusion, no scholar has yet undertaken a project to study whether The Wall could be a more efficient policy if government officials are given more resources to navigate The Wall's complexities. It suffices for this section, however, to note that government officials became frustrated with The Wall and were confused as to its application; as a response, information sharing was significantly hampered.

B. LAW ENFORCEMENT PERSONNEL IN INTELLIGENCE INVESTIGATIONS

The Wall's virtual ban on the participation of law enforcement personnel in FISA investigations had three bad effects. First, intelligence officials were deprived of the expertise of criminal investigators who could advise intelligence officials on the optimal way to proceed with the investigation. Government officials identified this criticism even before the creation of The Wall. According to the OIG Report, "[t]he Criminal Division and the FBI wrote position papers opposing [an early version of the 1995 Procedures]."[175] The Criminal Division, in particular, argued that "it was imperative for any procedures to allow for potential criminal prosecutions to be protected through early evaluation and guidance."[176] Piette and Radack quote an internal Justice Department memo from Mary Jo White,

---

[173] *See* OIG REPORT, *supra* note 78, at 34, 345 (concluding that concerns by FBI agents that violating The Wall would harm their carriers was one of the primary factors that killed the flow of intelligence within the FBI).
[174] *Id.* at 344–45.
[175] *Id.* at 26.
[176] *Id.* (internal quotations omitted).

the United States Attorney for the Southern District of New York, written to Gorelick a month before the 1995 Procedures took effect:

> It is hard to be totally comfortable with instructions to the FBI prohibiting contact with the United States Attorneys' Offices when such prohibitions are not legally required. Our experience has been that the FBI labels of an investigation as intelligence or law enforcement can be quite arbitrary, depending upon the personnel involved and that the most effective way to combat terrorism is with as few labels and walls as possible.[177]

The Justice Department attempted to deal in various ways with internal resistance to The Wall in the years following the 1995 Procedures.[178] A 1997 Justice Department working group addressed the lack of communication inherent in the 1995 Procedures, yet no changes resulted.[179] The 1999 OIG Report criticized the procedures, but this did not lead to changes, either.[180] Further criticism occurred with the release of the Bellows Report, which concluded that the 1995 Procedures had "significant, and potentially disastrous effects" on the Wen Ho Lee investigation.[181] According to Bellows, "[u]nfortunately, the practice of excluding the Criminal Division from [Foreign Counterintelligence] investigations was not an isolated event confined to the Wen Ho Lee matter. It has been a way of doing business for OIPR, acquiesced in by the FBI, and inexplicably indulged by the Department of Justice."[182] Again, however, no changes occurred.

---

[177] Charles Hurt & Stephen Dinan, *Memos Show Gorelick Involvement in 'Wall,'* WASH. TIMES, Apr. 29, 2004, at A01, *quoted in* Piette and Radack, *supra* note 50, at 481 n.294.
[178] *See* BELLOWS REPORT, *supra* note 91, at 709 ("It should be noted at the outset that this is not a new problem, but one that has persisted from the time that the July 1995 memorandum was promulgated.").
[179] *Id.*
[180] OIG REPORT, *supra* note 78, at 33.
[181] BELLOWS REPORT, *supra* note 91, at 708.
[182] *Id.*

Second, because criminal investigators were not aware of the status or content of intelligence investigations, they did not know what priority to attach to targets of criminal investigations. For example, two of the September 11 hijackers actually *lived* with an FBI informant. Had the FBI law enforcement personnel been aware that intelligence officials had identified the hijackers as possible jihadists, the FBI could have monitored the hijackers.[183] According to the OIG Report, "[t]he most critical breakdown in the [hijacker] case was the failure of the FBI to learn from the CIA critical information about them." The complaints about lack of coordination were not merely theoretical: the OIG Report found that "the FBI dramatically reduced its consultations with the Criminal Division after the 1995 Procedures were issued."[184]

Third, The Wall's virtual ban on participation by criminal investigators in intelligence investigations denied the intelligence officials access to the criminal investigators' expertise and use of traditional law enforcement tools such as grand jury subpoenas.[185] The OIG Report states that the investigation into targets who would become September 11 hijackers was severely hampered because key FBI law enforcement personnel were screened from the investigation because they wanted to pursue a criminal investigation.[186] David Kris argues that traditional law enforcement tools should be used in tandem with modern intelligence techniques in order to best protect national security:

> When we identify a spy or a terrorist, we have to pursue a coordinated, integrated, coherent response. We need all of our best people, intelligence and law enforcement alike, working together to neutralize the threat. In some cases, the best protection is prosecution—like the recent prosecution of Robert Hanssen for espionage. In other cases, prosecution is

---

[183] *See* OIG REPORT, *supra* note 78, at 306.
[184] OIG REPORT, *supra* note 78, at 32.
[185] Kris, *supra* note 53, at 520–21.
[186] OIG REPORT, *supra* note 78, at 343–44.

> a bad idea, and another method—such as recruitment—is called for. Sometimes you need to use both methods. But we can't make a rational decision until everyone is allowed to sit down together and brainstorm about what to do.[187]

The divide between intelligence and criminal agents is probably the feature of The Wall that both the OIG Report and the Bellows Report hit hardest upon when explaining some of the most significant intelligence failures of the past few decades.

C. RESOURCE MISALLOCATION

The general separation of criminal and intelligence officials led to unwise allocations of resources. Because criminal and intelligence investigations proceeded separately, investigations could theoretically take place in which similar officials for the same agency would investigate the same target under different labels. Even if investigators realized that they were pursuing the same target, they would waste resources arguing about whether to open an investigation as a "criminal" or an "intelligence" case.[188] The OIG Report concluded that the FBI had "systematic deficiencies" in counterterrorism cases which included "a narrow and conservative interpretation of FISA, inadequate analysis of whether to proceed as a criminal or intelligence investigation . . . and a disjoined and inadequate review of potential FISA requests by FBI attorneys."[189]

Resources were wasted because OIPR became the conduit through which all information had to pass before going over The Wall. According to Kris, the 1995 Procedures allowed OIPR to "interpose[] itself between the FBI and the Criminal Division . . . [and

---

[187] Kris, *supra* note 53, at 522 (quoting testimony he offered to the Senate Judiciary Committee in 2002).
[188] *See, e.g.*, OIG REPORT, *supra* note 78, at 307–08 (explaining that several agents spent time prior to September 11 arguing about whether to open the matter as an "intelligence" or a "criminal" case).
[189] *Id.* at 378.

the OIPR] sought to limit advice giving between intelligence and law enforcement [officials]."[190]

Scheduling became a problem, too. Again, according to Kris, "OIPR's desire to attend meetings between the FBI and the Criminal Division created substantial delays in scheduling. OIPR understood that it was limiting coordination, but it believed that such limits were necessary to avoid violations."[191]

D. THE AL-MIHDHAR INVESTIGATION

The OIG Report places significant, but by no means all, blame for the September 11 terrorist attacks on The Wall, concluding that the FBI failed to capture at least some of the hijackers because of Wall-related distractions.[192] This section discusses how The Wall hindered the investigation of Khalid al-Mihdhar prior to the attacks.

In August 2001 personnel in the FBI Usama Bin Laden Unit ("UBLU") became aware that al-Mihdhar, a suspected terrorist alleged to have participated in the U.S.S. Cole bombing and an associate of Bin Laden, had traveled to the United States; they decided that locating Mihdhar should be a top priority.[193] The UBLU intelligence official in charge of the investigation, a person the OIG Report calls "Donna," telephoned "Chad," an agent in the FBI's New York field office who had worked on the U.S.S. Cole case and was therefore aware of Mihdhar's significance.[194] Donna and Chad agreed that finding Mihdhar was critical. Donna wrote a formal memorandum laying the basis for the UBLU's suspicion of Mihdhar and asking the New York field office to open a full field investigation in order to discover Mihdhar's location.[195] Chad forwarded the memorandum to his supervisor, Jason, who then forwarded it on to "Scott," a criminal investigator for the FBI involved with the U.S.S.

---

[190] Kris, *supra* note 53, at 505.
[191] *Id.*, at 506 (internal quotations and citations omitted).
[192] OIG REPORT, *supra* note 78, at 370.
[193] *Id*. at 301–02.
[194] *Id*. at 303.
[195] *Id*. at 304–05.

Cole investigation.[196] When Donna became aware that her memorandum had been distributed to a criminal investigator, she contacted Scott and told him to delete it because it had not been approved for criminal investigators.[197] Scott, Donna, and others had a conference call on August 28, 2001 to debate how to proceed with the Mihdhar investigation. According to the OIG:

> Scott . . . argued that the investigation should be opened as a criminal investigation due to the nexus to the Cole investigation and the greater investigative resources that could be brought to bear in a criminal investigation. Scott explained that more agents could be assigned to a criminal investigation due to the squad designations. He also asserted that criminal investigation tools, such as grand jury subpoenas, were far quicker and easier to obtain than the tools available in an intelligence investigation, such as a national security letter.
>
> Donna [said] that the information on Mihdhar was received through intelligence channels and, because of restrictions on using intelligence information, could not be provided directly to criminal agents working the Cole investigation. . . . She stated that without the intelligence information on Mihdhar, there would have been no potential nexus to the Cole investigation and no basis for a criminal investigation.[198] Donna also stated that, due to The Wall, Scott would be unable to interview Mihdhar if he was ever found.

Subsequently, Scott contacted the FBI's National Security Law Unit ("NSLU") "for a legal opinion . . . [on] whether the investigation should be opened as a criminal matter relating to the Cole criminal investigation" and whether a criminal agent could be present at an

---

[196] *Id.* at 305.
[197] *Id.*
[198] *Id.* at 306.

interview with Mihdhar.[199] Donna also contacted the NSLU, and one of their attorneys told her that the investigation should be conducted as an intelligence matter and that a criminal agent could not be present at in interview with Mihdhar.[200]

Donna sent an e-mail to Scott, telling him of the NSLU attorney's statement. She wrote:

> Per NSLU, if Al-Mihdar [sic] is located the interview must be conducted by an intel agent. A criminal agent CAN NOT be present at the interview. This case, in its entirety, is based on intel. If . . . information is developed indicating the existence of a substantial federal crime, that information will be passed over the wall according to proper procedures and turned over for follow-up criminal investigation.[201]

Scott responded to Donna, writing:

> [W]here is the wall defined? Isn't it dealing with FISA information? I think everyone is still confusing this issue . . . [S]omeday someone will die—and wall or not—the public will not understand why we were not more effective and throwing every resource we had at certain 'problems.' Let's hope the National Security Law Unit will stand by their decisions then, especially since the biggest threat to us now, UBL, is getting the most 'protection.'[202]

The FBI began work on an intelligence investigation to locate Mihdhar on September 4, 2001 but was unable to locate him before September 11, 2001, when he and others crashed an airplane into the Pentagon.[203] The OIG Report concluded that "the wall . . . had

---

[199] *Id.* at 307.
[200] *Id.*
[201] *Id.* at 308.
[202] *Id.*
[203] *Id.* at 312.

resulted in a nearly complete separation of intelligence and criminal investigations within the FBI. This separation greatly hampered the flow of information between FBI personnel and intelligence investigations, including information concerning Hazmi [another hijacker] and Mihdhar in the summer of 2001."[204]

The OIG Report stops short of concluding that, had The Wall not existed, the federal government would have captured Mihdhar and prevented the terrorist attacks. It does, however, repeatedly place significant blame on The Wall for intelligence failures that at least contributed to the federal government's failure to prevent the September 11 attacks.

III. THE MAYFIELD COMPROMISE

Before concluding this note, it is important to comment on whether there is a compromise that might protect the Fourth Amendment concerns stated in *Mayfield* and numerous law review articles, as well as provide for the destruction of The Wall. I am skeptical that such a compromise is possible.[205]

Mayfield argued that—despite striking down part of the USA PATRIOT Act—there is no danger The Wall will be judicially rebuilt because another USA PATRIOT Act provision sufficiently dismantles it.[206] The other USA PATRIOT Act section referred to by *Mayfield* provides that intelligence officials "may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against" a variety of catastrophes.[207] Though *Mayfield* does not explain its argument, it assumes that one could maintain this provision while still demanding that intelligence officials have the collection of foreign intelligence information as their "primary purpose."

---

[204] *Id*. 343–44.

[205] David Kris makes a different argument that civil libertarians and privacy advocates should embrace the Patriot Act changes to FISA instead of challenging them. *See* Kris, *supra* note 53, at 523–27. An evaluation of Kris's argument is beyond the scope of this paper.

[206] *See* Mayfield v. United States, 504 F. Supp. 2d 1023, 1041 (D. Or. 2007).

[207] USA PATRIOT Act, *supra* note 4, at § 504.

A regime such as the one *Mayfield* describes would renew the uncertainty of the *Truong* era and ultimately rebuild The Wall. Recall that *Truong* acknowledged that the court could not read minds to determine when the primary purpose of a search had switched from foreign intelligence to law enforcement, and so the court used as a proxy the date when Criminal Division personnel became involved.[208] *Mayfield* does not suggest a way to overcome this problem. This means that any time law enforcement personnel participate in an intelligence investigation, courts could point to the beginning of that participation and say it was the *exact* moment when the purpose of the investigation switched. Faced with such a rule, the coordination provision of the USA PATRIOT Act could not give sufficient comfort to the government to allow law enforcement personnel to participate; rather, the government would be worried that such involvement would risk switching the purpose of the investigation in the eyes of a court or a FISA judge. If law enforcement personnel were allowed to participate, courts could exclude subsequent evidence, or a FISA judge could deny a request to extend the period of surveillance.[209] The events leading up to 9/11 evidence this potential problem: for example, when the FBI identified one of the hijackers as a person of interest, criminal agents were prevented from participating because the FBI wanted to avoid "any activities that the FISA Court or OIPR could later deem 'too criminal' and could use as a basis to deny a FISA application."[210] While it is possible that courts could choose a different test to determine when the purpose of the investigation switches, what would that test look like? *Truong* is the most on-point authority, and no other court or academic paper proposes an alternative test.

---

[208] United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980).
[209] *In re* Sealed Case, 310 F.3d 717, 743 (FISA Ct. Rev. 2002).
[210] OIG REPORT, *supra* note 78, at 343; *see* Stewart Baker, *Wall Nuts*, SLATE, Dec. 31, 2003, http://www.slate.com/id/2093344 (*stating* "[w]e couldn't find al-Mihdhar and al-Hazmi in August 2001 because we had imposed too many rules designed to protect against privacy abuses that were mainly theoretical. We missed our best chance to save the lives of 3,000 Americans because we spent more effort and imagination guarding against these theoretical privacy abuses than against terrorism.").

Ultimately, it is not merely due to metaphorical consistency that David Kris called the "primary purpose" requirement the "foundation" of The Wall.[211] The government did not decide *sua sponte* to prohibit officials working down the hall from each other from speaking to each other. Rather, criminal investigators were excluded because their involvement risked changing the "purpose" of the investigations and thus risked exclusion of the evidence.[212] The OIG Report noted that:

> [C]oncerns were raised that if intelligence investigators consulted with prosecutors about the intelligence information or provided the information to criminal investigators, this interaction could affect the prosecution by allowing defense counsel to argue that the government had misused the FISA statute and it also could affect the intelligence investigation's ability to obtain or continue FISA searches or surveillances.[213]

Contrary to *Mayfield*'s assertion otherwise, The Wall's fate seems tied to the "primary purpose" test.

IV. CONCLUSION

The Wall systematically obstructed federal investigations from 1995 to 2001. At a time when balancing privacy and security is critical, policymakers should cautiously analyze how regulations impact counterterrorism. The history of The Wall detailed in Part II shows how federal courts and even the Department of Justice either assumed or uncritically decided that the "primary purpose" standard was constitutionally mandatory. The fact that the great weight of constitutional authority pointed in the other direction makes this assumption even more incredible. Following Mary Lawton's death, Jamie Gorelick's 1995 Procedures codified The Wall, if they did not outright invent it. While the USA PATRIOT Act destroyed The

---

[211] Kris, *supra* note 53, at 499.
[212] OIG REPORT, *supra* note 78, at 21.
[213] *Id.*

Wall, *Mayfield*, perhaps unintentionally, could lead to The Wall's reconstitution if the decision survives on appeal and if other courts find it persuasive. There is no reason to think that The Wall would be any less disastrous today than it was in the previous decade. By preventing law enforcement officials and intelligence officials from communicating about the most important national security investigations, The Wall significantly impedes the ability of government actors to protect the national security.

I do not argue that *Mayfield* was wrongly decided (nor do I endorse it); I simply point out that The Wall poses such a major security threat that it deserved more than a single sentence out of a forty-four page opinion. This is especially true given the *Keith* Court's mandate to balance privacy interests, the government's need for the information at issue, and whether obstacles to obtaining that information would prevent the government from acquiring it. In short, courts should carefully balance the interests at stake. *Mayfield* did not appear to take this balancing seriously.