# National Security Law Journal

**Excerpt from Vol. 3, Issue 1 – Fall 2014**

Cite as:

Ronald J. Sievert, *Time to Rewrite the Ill-Conceived and Dangerous Foreign Intelligence Surveillance Act of 1978*, 3 NAT'L SEC. L.J. 47 (2014).



ISSN: 2373-8464

The *National Security Law Journal* is a student-edited legal periodical published twice annually at George Mason University School of Law in Arlington, Virginia. We print timely, insightful scholarship on pressing matters that further the dynamic field of national security law, including topics relating to foreign affairs, intelligence, and national defense.

Visit our website at www.nslj.org to read our issues online, purchase the print edition, submit an article, or sign up for our e-mail newsletter.

# TIME TO REWRITE THE ILL-CONCEIVED AND DANGEROUS FOREIGN INTELLIGENCE SURVEILLANCE ACT OF 1978

**Ronald J. Sievert***

*The Foreign Intelligence Surveillance Act's ("FISA") imposition of a civilian criminal law probable cause search standard on what should be recognized as straightforward intelligence collection activity has greatly obstructed our nation's ability to monitor and deter foreign-connected terrorists and agents in the United States. The result has been a protracted, bureaucratic FISA judicial process that has led to failure to uncover several terrorist conspiracies. The Supreme Court specifically exempted foreign-related domestic intelligence interceptions from its decision on intelligence collection, warrants, and traditional probable cause requirements. Further, the Supreme Court's established "special needs" exception to conventional Fourth Amendment warrants applies to intelligence surveillance, and the FISA Court of Review explicitly found that the "special needs" doctrine should apply to such cases. Moreover, a review of the laws related to domestic national security surveillance in several European nations reveals that none of them mandate an evidentiary standard as rigorous as probable cause before authorizing electronic interception in national security cases.*

*Due to these considerations, Congress should modify FISA to permit electronic surveillance where the government has established reasonable suspicion that a target in the United States, or a U.S. citizen overseas, is the subject of an Authorization for Use of Military Force, or is engaged in planning an attack using Weapons of Mass Destruction. Should Congress take this step, any fears that FISA would be used as a substitute for the stricter requirements of*

* Professor, Bush School of Government, and Adjunct Professor, University of Texas School of Law; Author, CASES AND MATERIALS ON U.S. LAW AND NATIONAL SECURITY.

*Title III could be eased by the inclusion of a condition that the product of such surveillance cannot be used in the prosecution of ordinary crimes unrelated to intelligence.*



## INTRODUCTION

The United States regrettably has not been able to dwell in a state of domestic peace and tranquility since the conclusion of World War II. We have instead existed in a state of continuous conflict that daily has threatened to explode in targeted or potentially massive attacks against American citizens. For almost fifty years, we operated under the understanding that the slightest misstep could lead at any moment to a cataclysmic war with the Soviet Union. Then, the 1996

bombing of Khobar towers[1] and the 2000 assault on the USS *Cole*[2] presaged the domestic attacks of a new enemy in 2001 as Al Qaeda directed strikes against our financial, military, and governmental centers of power.[3] Many are not aware of the multiple elements of the continuous onslaught because, thankfully, luck, skill, and, in at least two cases, minor technical mistakes on the part of our adversaries prevented their success.[4] The simultaneous destruction of twelve U.S. planes over the Atlantic in 2006 was averted with the discovery of the liquid explosives plot,[5] planned attacks on John F. Kennedy International Airport and New Jersey oil terminals were uncovered early in 2007,[6] Najibullah Zazi's plan to blow up the New York City subways was disrupted in 2009,[7] Umar Farouk Abdulmuttalab's underwear bomb failed to detonate on a passenger-laden plane over Detroit that same year,[8] and Faisal Shahzad's 2010 Times Square bomb fizzled after preliminary ignition.[9]

---

[1] *Al Qaeda Is Now Suspected in 1996 Bombing of Barracks,* N.Y. TIMES (May 14, 2003), http://www.nytimes.com/2003/05/14/world/al-qaeda-is-now-suspected-in-1996-bombing-of-barracks.html.

[2] CNN Library, *USS Cole Bombing Fast Facts*, CNN WORLD (last updated Oct. 8, 2014, 5:40 PM), http://www.cnn.com/2013/09/18/world/meast/uss-cole-bombing-fast-facts/.

[3] *9/11 Attacks,* HISTORY.COM, http://www.history.com/topics/9-11-attacks (last visited Oct. 24, 2014).

[4] *See* Ben West & Scott Stewart, *Uncomfortable Truths and the Times Square Attack,* STRATFOR GLOBAL INTEL. (May 6, 2010, 3:56 PM), http://www.stratfor.com/weekly/20100505_uncomfortable_truths_times_square_attack; Anahad O'Connor & Eric Schmitt, *Terror Attempt Seen as Man Tries to Ignite Device on Jet*, N.Y. TIMES (Dec. 25, 2009), http://www.nytimes.com/2009/12/26/us/26plane.html.

[5] Peter Wright, *UK 2006 Liquid Explosives Plot Trial Overview*, TRANSP. SEC. ADMIN. (Sept. 8, 2008), http://www.tsa.gov/press/releases/2008/09/08/uk-2006-liquid-explosives-plot-trial-overview.

[6] Cara Buckley & William K. Rashbaum, *Four Men Accused of Plot to Blow Up Kennedy Airport Terminal and Fuel Lines,* N.Y. TIMES (June 3, 2007), http://www.nytimes.com/2007/06/03/nyregion/03plot.html?pagewanted=all&_r=0.

[7] John Marzulli, *Zazi, Al Qaeda pals planned rush-hour attack on Grand Central, Times Square subway stations*, NY DAILY NEWS (Apr. 11, 2010, 11:00 PM), http://www.nydailynews.com/news/crime/zazi-al-qaeda-pals-planned-rush-hour-attack-grand-central-times-square-subway-stations-article-1.167379.

[8] O'Connor & Schmitt, *supra* note 4.

[9] West & Stewart, *supra* note 4.

Those who underestimate Al Qaeda in comparison with the Germany and Japan of former times ignore the fact that if Al Qaeda were to acquire Weapons of Mass Destruction ("WMD") it potentially would pose a greater threat than our previous enemies. As Judge Wilkinson stated in *Hamdi v. Rumsfeld*:

> We have emphasized that the 'unconventional aspects of the present struggle do not make its stakes any less grave.' . . . [N]either the absence of set-piece battles nor the intervals of calm between terrorist assaults (should) suffice to nullify the . . . authority entrusted to the executive and legislative branches.[10]

At the same time, looming in the background as a potential threat is China, a nation with unknown intentions that has been highly aggressive in penetrating our cyber infrastructure and defense establishment. The former Chief of Central Intelligence Agency ("CIA") Counter Intelligence noted it is likely that China has dispatched approximately 1,000 State Security Officers to the U.S. in an effort to obtain American military technology by any means possible.[11] "Among the many U.S. citizens implicated in espionage for the [Chinese Ministry of State Security] were Larry Wu-Tai Chin, a CIA employee; Peter Lee, a TRW employee; and James Smith, a special agent for the FBI."[12] In 2014, the Department of Justice ("DOJ") took the unusual step of directly exposing organized action aimed at the U.S. by the Chinese military when it charged five officers of the People's Liberation Army with conducting massive cyber espionage against U.S. interests.[13]

To counter these and other ongoing threats, the United States government has been burdened with the restrictions of the

---

[10] Hamdi v. Rumsfeld, 316 F.3d 450, 464 (4th Cir. 2003) (citation omitted) (internal quotation marks omitted).

[11] JAMES OLSON, FAIR PLAY, THE MORAL DILEMMAS OF SPYING, 242 n.3 (2006); *see also Report: China Stole U.S. Nuke Secrets to 'Fulfill International Agenda,'* CNN (May 25, 1999, 8:13 PM), http://www.cnn.com/US/9905/25/cox.report.02/.

[12] OLSON, *supra* note 11, at 242.

[13] Kimberly Bennett, *US charges five Chinese army officers in cyber espionage case*, JURIST (May 20, 2014, 8:52 AM), http://jurist.org/paperchase/2014/05/us-charges-five-chinese-army-officers-in-cyber-espionage-case.php.

misguided and ill-conceived Foreign Intelligence Surveillance Act of 1978 ("FISA").[14] This statute requires that, in their effort to protect the nation's security, intelligence analysts, agents, and attorneys must produce evidence before members of the federal judiciary that meets the maximum criminal law search standard of probable cause before they can monitor the domestic conversations and emails of agents of a foreign power and terrorist organizations.[15] The procedure created by this statute is both confusing and, in the words of New York City Police Commissioner Raymond Kelly, "an unnecessarily protracted, risk-adverse process that is dominated by lawyers, not investigators and intelligence collectors."[16]

Both the 9/11 Commission[17] and Amy Zegart in her book *Spying Blind*[18] have detailed how FBI agents were stymied in tracking the hijackers before the September 11th attacks because, as a result of FISA interpretations, lawyers in the Department of Justice's "Office of Intelligence and Policy Review, FBI leadership and the FISA Court built barriers between agents—even agents serving on the same squads."[19] This "wall" was breached to some extent with the 2001 PATRIOT Act provisions permitting information sharing,[20] but the statute's basic restrictions and confusion surrounding its interpretation remain. The FBI had detained hijacker Zacarias Moussaoui in Minneapolis days before the 9/11 attacks, but agents were prevented from scanning his computer because a supervisor at

---

[14] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified at 50 U.S.C. Ch. 36).

[15] 50 U.S.C. § 1805 (2010).

[16] *Surveillance and Shahzad*, *Are Wiretap Limits Making it Harder to Discover and Pre-empt Jihadists?*, WALL ST. J. (May 13, 2010, 12:01 AM), http://online.wsj.com/news/articles/SB10001424052748704250104575523844418292496.

[17] *See* NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 78 *passim* (2004).

[18] AMY ZEGART, SPYING BLIND: THE CIA, THE FBI, AND THE ORIGINS OF 9/11 *passim* (2007).

[19] 9/11 COMMISSION REPORT, *supra* note 17, at 79; *see also* Nola Breglio, *Leaving FISA Behind; The Need to Return to Warrantless Intelligence Surveillance*, 113 YALE L.J. 179 at 193-94 (for excellent quotes from various former DOJ officials regarding problems created by the "wall"). The "wall" and its effects are further explained in Ronald J. Sievert, *Patriot 2005-2007: Truth, Controversy and Consequences*, 11 TEX. REV. L. & POL. 319, 322-31 (2007).

[20] *See* Sievert, *supra*, note 19, at 322-28, 331-35.

FBI Headquarters concluded there was not probable cause for a FISA warrant. Meanwhile, according to the DOJ Inspector General's report, the Minneapolis office believed that "probable cause for the warrant was clear" and "became increasingly frustrated with the responses and guidance it was receiving."[21]

The Bush administration initiated the publicly criticized Terrorist Surveillance Program because, even with the PATRIOT Act's modifications, obtaining FISA warrants "incurr(ed) a delay that was unacceptable given the time-sensitivity and sheer volume of intelligence requirements after 9/11."[22] The government apparently knew that 2007 Times Square bomber Faisal Shahzad had "established interaction with the Pakistani Taliban, including bomb making training in Waziristan" and had made "thirteen trips to Pakistan in seven years," yet did not monitor him as he slowly assembled the materials to construct his potentially devastating weapon.[23] This led the *Wall Street Journal* to question whether the failure was due to "restrictions imposed on wiretapping by the Foreign Intelligence Surveillance Act" and to quote officials on the reduced effectiveness and excessive delays of the judicially regulated program.[24] In a very extensive, detailed investigation of the Boston Marathon bombing, Keith Maart further highlighted the confusion endemic to attempts at interpreting FISA.[25] He noted that the Russian Federal Security Service ("FSB") had twice informed the FBI and CIA that Tamerlan Tsarnaev "had contacts with foreign Islamic militants/agents, was visiting jihadist websites and was looking to join jihadist groups" and that he had travelled to Dagestan on an

[21] *See* U.S. DEP'T. OF JUSTICE, OFFICE OF THE INSPECTOR GEN., A REVIEW OF THE FBI'S HANDLING OF INTELLIGENCE INFORMATION RELATED TO THE SEPTEMBER 11 ATTACKS 101-02 (Nov. 2004), *available at* http://www.justice.gov/oig/special/s0606/final.pdf (internal quotations omitted).

[22] John Andrews, *Time of Clear and Present Danger*, PUB. DISCOURSE (Oct. 4, 2010), http://www.thepublicdiscourse.com/2010/10/1659/.

[23] *Surveillance and Shazad*, WALL ST. J. (May 13, 2010, 12:01 AM), http://online.wsj.com/news/articles/SB10001424052748704250104575238444182924962.

[24] *Id.*

[25] Keith Maart, *The Boston Marathon Bombing One Year Later: A Detailed Look*, VETERANSTODAY.COM (Apr. 13, 2014), http://www.veteranstoday.com/2014/04/13/the-boston-marathon-bombing-one-year-later-a-detailed-look/.

unknown mission.[26] Maart offered that it would certainly appear there was "sufficient probable cause to obtain FISA warrants that would allow . . . more encompassing surveillance."[27] However, the FBI had apparently come to a contrary conclusion.[28]

By adhering to FISA, we are weakening our intelligence collection capabilities rather than strengthening our ability to prevent catastrophic attacks by those who do not hesitate to target and inflict mass casualties on innocents. At the same time, we are overreacting to the government's access to the limited information contained in metadata that has been routinely collected by telephone companies for decades.[29] This Article will explain how FISA was an excessive response to the Supreme Court's decision in *U.S. v. U.S District Court (Keith)*[30] and the Watergate era, and demonstrate why, because of the foreign affairs power and the Supreme Court's decisions on public safety searches, it is not constitutionally required.[31] Furthermore, this Article will show that most of our foreign partners in the supposedly sophisticated, privacy-protecting nations of Europe do not restrain their security forces in a similar manner in intelligence cases. This is due to the obvious reason that national security investigations involve threats that endanger the lives of thousands of people and potentially imperil the very existence of the nation, unlike the far more constrained menace of ordinary

[26] *Id.*
[27] *Id.*
[28] *Id.*
[29] *See* Smith v. Maryland, 442 U.S. 735, 742 (1979) ("First, we doubt that people in general entertain any actual expectation of privacy in the numbers they dial. All telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed. All subscribers realize, moreover, that the phone company has facilities for making permanent records of the numbers they dial, for they see a list of their long-distance (toll) calls on their monthly bills. In fact, pen registers and similar devices are routinely used by telephone companies 'for the purposes of checking billing operations, detecting fraud, and preventing violations of law.'") (quoting United States v. New York Tel. Co., 434 U.S. 159, 174-75).
[30] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297 (1972).
[31] See quotes from *Keith*, as well as numerous public safety cases discussed in this article.

crime.[32] It is well recognized that the arguments contained here are directly opposed to those who are demanding more, not fewer, government regulation in the wake of the revelations attributed to Edward Snowden.[33] Accordingly, this Article will also address why our recent media, political, and judicial reactions might once again lead to restrictions that are not constitutionally required, and that could further undermine the government's reasonable efforts to provide security for the American people.

## I. THE CREATION OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

### A. *United States v. U.S. District Court (Keith)*

The Foreign Intelligence Surveillance Act traces back to legislative hearings held immediately following the Supreme Court's decision in *United States v. U.S. District Court (Keith)* in 1972.[34] The Court's opinion in *Keith* related to electronic surveillance conducted against an entirely domestic conspiracy to bomb the CIA office in Ann Arbor, Michigan.[35] The Court held that the government should obtain a warrant from a neutral, detached magistrate before intercepting the conversations of wholly "domestic organizations."[36]

---

[32] This will be discussed in great detail later in the Article. Several excellent sources are Daniel Saperstein, *The European Counterterrorist as the Next Cold Warrior*, 32 FORDHAM INT'L L. J. 1947 (2009); WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENT ACCESS TO DATA IN THE CLOUD (May 23, 2012), *available at* http://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf; MAXWELL & WOLF, A SOBER LOOK AT NATIONAL SECURITY ACCESS TO DATA IN THE CLOUD, (May 22, 2013), *available at* http://www.hldataprotection.com/2013/05/articles/international-eu-privacy/white-paper-cloud-national-security; PRIVACY INT'L, UNITED STATES OF AMERICA (2006), *available at* https://www.privacyinternational.org/resources/reports/united-states-of-america.

[33] Katherine Jacobsen & Elizabeth Barber, *NSA Revelations, A Timeline of What's Come Out Since Snowden Leaks Began*, CHRISTIAN SCI. MONITOR (Oct. 16, 2013), http://www.csmonitor.com/USA/2013/1016/NSA-revelations-A-timeline-of-what-s-come-out-since-Snowden-leaks-began/June-5-8-2013.

[34] Diane Carraway Piette & Jesselyn Radack, Symposium, *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, 441-52 (2006).

[35] *See Keith*, 407 U.S. at 299.

[36] *Id.* at 316 n.8.

This phrase was defined as a group "composed of citizens of the United States which has no significant connection with a foreign power, its agents or agencies."[37] Recognizing that intelligence investigations such as the one at issue concerned long range attempts to prevent subversive actions, spanned long periods of time, and involved information "less precise" than in ordinary crime cases, the Court invited Congress to pass legislation that would be less restrictive than Title III (18 U.S.C. § 2510-2522).[38] Title III was passed in 1968 to control criminal investigations.[39] It required the government to establish, before a court, probable cause that a specific communication facility was being used to further an ongoing or imminent crime. Wiretaps would not be approved without a court finding of probable cause.[40] The Court stated with respect to purely domestic intelligence matters:

> In determining whether there is probable cause to issue a warrant for that inspection . . . the need for the inspection must be weighed in terms of the reasonable goals of (Code) enforcement. It may be that Congress, for example, would judge that the application and affidavit showing probable cause need not follow the exact requirements of Section 2518 but should allege other circumstances more appropriate to domestic security cases.[41]

Thus the Court held that there should be warrants for entirely domestic security cases but even these warrants need not follow the same strictures applied to ordinary crime.[42] Even more importantly for purposes of this Article, the Court repeatedly emphasized that "this case involves only the domestic aspects of national security."[43] No opinion was expressed "as to the issues which may be involved with respect to the activities of foreign

---

[37] *Id.*
[38] *Id.* at 322.
[39] Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. 90-351, §§ 801-02, 82 Stat. 197; *see also* 18 U.S.C. §§ 2510-13, 2515-22.
[40] 18 U.S.C. § 2518(3) (1998).
[41] *Keith,* 407 U.S. at 323.
[42] *See id.* at 322-24.
[43] *Id.* at 321.

powers or their agents."[44] However, the Court hastened to add a footnote citing numerous sources, including the American Bar Association's standards on electronic surveillance, supporting "the view that warrantless surveillance . . . may be constitutional where foreign powers are involved."[45]

The Court's emphasis that it was not imposing a probable cause warrant requirement in foreign intelligence cases was grounded in legal and factual precedent. As the Court noted, President Roosevelt authorized Attorney General Robert Jackson to utilize wiretaps for national defense in 1940, Attorney General Tom Clark advised President Truman of the necessity of such wiretaps,[46] and Attorney General Herbert Brownell advocated their employment by President Eisenhower.[47] Furthermore, in the landmark case of *Katz v. United States*,[48] holding that wiretaps in ordinary crime cases required warrant authorization, Justice White stressed the Court's acknowledgement

> that there are circumstances in which it is reasonable to search without a warrant. In this connection, in footnote 23 the Court points out that today's decision does not reach national security cases. Wiretapping to protect the security of the Nation has been authorized by successive Presidents. The present Administration would apparently save national security cases from restrictions against wiretapping.[49]

Accordingly, when Congress passed Title III in 1968, it inserted a special provision that the statute did not limit the constitutional power of the President

> to take such measures as he deems necessary to protect the Nation against actual or potential attack or other hostile acts of a foreign power, to obtain foreign intelligence information deemed essential to the security of the United States, or to

[44] *Id.* at 322.
[45] *Id.* at 322 n. 20.
[46] *Id.* at 311 n. 10.
[47] *Keith*, 407 U.S. at 311.
[48] Katz v. United States, 389 U.S. 347 (1967).
[49] *Id.* at 363 (White, J., concurring).

> protect national security information against foreign intelligence activities.[50]

*Keith* demonstrates the Court believed that surveillance of an exclusively domestic organization was an entirely different matter, requiring at least some type of judicial warrant because it potentially infringed on the First Amendment right to dissent at home. As Justice Powell stated for the majority:

> As I read it—and this is my fear—we are saying that the President, on his motion, could declare—name your favorite poison—draft dodgers, Black Muslims, the Ku Klux Klan, or civil rights activists to be a clear and present danger to the structure or existence of the Government.
>
> The price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society.[51]

Justice Douglas followed this up in his concurring opinion by writing that "the recurring drive of reigning officials to employ dragnet techniques to intimidate their critics lies at the core of that (Fourth Amendment) prohibition."[52]

The holding and reasoning of *Keith* is clear. The irony is that, after extensive legislative hearings for the next six years, Congress ultimately reacted by passing a statute that greatly restricted and imposed probable cause requirements on *foreign intelligence surveillance*. Congress completely failed to enact a law providing guidance for wholly *domestic security surveillance* as suggested by the Court. How did we get there from *Keith*?

---

[50] 18 U.S.C. § 2511(3) (1967); *see also Keith*, 407 U.S. at 302 (citing the 1967 version of 18 U.S.C. § 2511(3)).
[51] *Keith*, 407 U.S. at 314 (internal citation omitted).
[52] *Id.* at 327 (Douglas, J., concurring).

*B. Post-Keith Developments*

Just ten days after the Supreme Court's decision in *Keith*, Senator Edward Kennedy chaired hearings on its implications before the Senate Judiciary Subcommittee on Administrative Priorities and Procedure.[53] His first witness was Deputy Assistant Attorney General Kevin Maroney of the DOJ's Internal Security Division. Kennedy's questioning of Maroney demonstrated that the Senator had a firm grasp on the exact scope of the *Keith* decision and revealed the Congressional response he hoped to obtain. Conceding that the Court did not prohibit collections targeted at agents of a foreign power,[54] Kennedy noted that the Court nevertheless rejected the Government's arguments that obtaining warrants in security cases could expose sensitive information and that determining probable cause in such cases involved complex and subtle factors beyond the competence of the judiciary.[55] In addition, he expressed his opinion that "there can be domestic groups with some significant foreign connection" which should still "retain their primarily domestic character for purpose of the First and Fourth Amendment."[56] Therefore, he asked Maroney if the case did not "affect your thinking about the legitimacy of (the government's) arguments (against warrants) in the foreign field?"[57] The Deputy Assistant Attorney General responded with a clear articulation of justice department policy, stating that "when you get into the area of foreign intelligence, the Court has recognized the President's Constitutional authority in the area of foreign affairs to protect the nation."[58] He noted that in such situations there are not "presently

[53] *Warrantless Wiretapping: Practices and Procedures of the Dept. of Justice for Warrantless Wiretapping and Other Electronic Surveillance, Hearing before the Subcomm. on Admin. Practice & Procedure of the S. Comm. on the Judiciary*, 92d Cong. 2 (1972) (statement of Sen. Edward M. Kennedy, Chairman, Subcomm. on Admin. Practice & Procedure) [hereinafter Kennedy Statement].
[54] *Id.* at 2-3, 8-9, 20-23.
[55] *Id.* at 2-3.
[56] *Id.* at 21.
[57] *Id.* at 9, 21.
[58] *Id.* at 10.

competing first amendment rights [as regards domestic dissent] that the Court found quite heavy in the Keith case."[59]

The Government's position prevailed and the President's ability to conduct foreign intelligence searches without probable cause warrants might have continued to this day if not for Watergate and the perceived abuses of the Vietnam era highlighted by the 1976 Church Committee report.[60] In the years immediately following *Keith*, four separate federal circuit courts "readily accepted the existence of a foreign intelligence exception to the warrant requirement based on the legal and policy arguments put forth by the Executive."[61] The Fifth Circuit, in *United States v. Brown*, upheld the legality of government-authorized warrantless surveillance that was targeted at the object of a genuine foreign intelligence investigation and incidentally acquired the communications of black activist, H. Rap. Brown.[62] The Third Circuit held, in *United States v. Butenko*, that warrantless surveillance, whose "primary purpose" was to obtain foreign intelligence information concerning the activities of foreign powers within the United States, was lawful even when conversations of American citizens were acquired.[63] The court noted that in foreign intelligence matters officials should not be required to interrupt their operations to "rush to the nearest available magistrate."[64] The Ninth Circuit, in *United States v. Buck*, held that electronic surveillance of foreign powers and their agents was considered a "recognized exception to the general warrant requirement of the fourth amendment."[65] The Fourth Circuit, in *United States v. Truong*, debated the issue of when an investigation

[59] Kennedy Statement, *supra* note 53, at 9 (1972).
[60] SELECT COMM. TO STUDY GOVERNMENTAL OPERATIONS, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, S. REP. NO. 94-755 (1976).
[61] Americo R. Cinquegrana, *The Walls (and Wires) Have Ears: The Background and First Ten Years of the Foreign Intelligence Surveillance Act of 1978*, 137 U. PA. L. REV. 793, 804 (1989).
[62] United States v. Brown, 484 F.2d 418 (5th Cir. 1973), *cert. denied,* 415 U.S. 960 (1974).
[63] United States v. Butenko, 494 F.2d 593, 606-08 (3d Cir. 1974), *cert. denied sub nom.* Ivanov v. United States, 419 U.S. 881 (1974).
[64] *Id.* at 605.
[65] United States v. Buck, 548 F.2d 871 (9th Cir. 1977), *cert. denied*, 434 U.S. 890 (1977).

becomes a search for evidence of a crime rather than an intelligence gathering effort, but clearly recognized a warrant exception flowing from the Executive's presumed expertise in the foreign intelligence area.[66] Typical of the reasoning of these courts was the Third Circuits' en banc opinion in *Butenko*:

> In the present case, too, a strong public interest exists: the efficient operation of the Executive's foreign policy-making apparatus depends on a continuous flow of information. A court should be wary of interfering with this flow . . .
>
> Also, foreign intelligence gathering is a clandestine and highly unstructured activity, and the need for electronic surveillance often cannot be anticipated in advance. Certainly occasions arise when officers, acting under the President's authority, are seeking foreign intelligence information, where exigent circumstances would excuse a warrant. To demand that such officers be so sensitive to the nuances of complex situations that they must interrupt their activities and rush to the nearest available magistrate to seek a warrant would seriously fetter the Executive in the performance of his foreign affairs duties.[67]

At the same time, in 1975 Congress had commissioned the Library of Congress to do a comparative study of wiretapping laws in major foreign countries. The report found that, without exception, in national security matters the executive authority could authorize electronic surveillance without either probable cause or a judicial warrant.[68] In France, General Instruction 500-78 required telephone companies to comply with demands for wiretaps originating from military authorities, public prosecutors, or department prefects acting in matters of state security.[69] The German Federal Constitutional Court had held that "the exclusion of recourse to courts with respect to ordering and carrying out surveillance is compatible with the Basic Law [Constitution]" with the exception of provisions that might prevent the disclosure to those surveilled after

[66] United States v. Truong, 629 F.2d 908 (4th Cir. 1980).
[67] *Butenko*, 494 F.2d, at 605.
[68] *See* LIBRARY OF CONG. LAW LIBRARY, COMPARATIVE STUDY ON WIRETAPPING AND ELECTRONIC SURVEILLANCE LAWS IN MAJOR FOREIGN COUNTRIES *passim* (1975).
[69] *Id.* at France-5.

a point it would not interfere with the investigation.[70] According to the German Court, "[i]n the final analysis, prosecutorial surveillance requires a judicial order whereas intelligence surveillance needs only an order of an administrative agency."[71] In the United Kingdom, the Home Secretary had absolute authority to issue a surveillance warrant upon request of any governmental authority.[72] His power traced to the Crown's duty to "preserve the safety of the state and maintain order" or, historically, the "common law right of the Crown to safeguard the safety of the realm."[73]

However, after evidence of Presidential assassination plots and surveillance of domestic anti-government organizations emerged, Idaho Senator Frank Church convened the Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities and the Rights of Americans.[74] As reflected by the Committee's name, "the congressional mood at this time was one of antagonism towards the Executive because of Watergate and the disclosures in 1975 and 1976 of a broad range of perceived abuses of authority, especially in the area of intelligence and national security related activities."[75] Frederick Schwarz, Jr., Church's Chief Counsel at the hearings, recently recounted that the Committee found "shocking conduct by numerous agencies including the FBI, CIA, and NSA."[76] For example, the FBI targeted Martin Luther King, Jr., "the CIA enlisted the Mafia in its attempts to assassinate Fidel Castro, and the NSA obtained copies of most telegrams leaving America for a period of thirty years."[77] Exemplifying mission creep,

[70] *Id.* at FRG-3.
[71] *Id.* at FRG-13.
[72] *Id.* at Great Britain-2.
[73] *Id.* at Great Britain-1.
[74] S. REP NO. 94-465 at 1 (1976); S. REP. NO. 94-755, bk. II, at v (1976).
[75] Cinquegrana, *supra* note 61, at 806.
[76] Frederick A.O. Schwarz Jr., *Why We Need a New Church Committee to Fix Our Broken Intelligence System*, THE NATION (Mar. 31, 2014), http://www.thenation.com/article/178813/why-we-need-new-church-committee-fix-our-broken-intelligence-systeem.
[77] *Id.*

"the NSA trained its sights on anti-Vietnam War protesters and civil rights activists."[78]

Although not often reported in today's literature, many of these investigations were based on FBI documents indicating Communist connections and possible Soviet financing of some aspects of the Civil Rights and anti-war movements.[79] This is not to say that there were not government abuses, or that both movements did not have legitimacy on their own completely independent of Communist exploitation. Regardless of the Government's justifications for this surveillance and the foreign intelligence connections that existed, the Committee attributed what they perceived as domestic abuses in these foreign intelligence-related cases to the absence of clear congressional or judicial standards. Consequently they "urged a statutory framework restricting electronic surveillance for intelligence purposes within the United States to that conducted by the FBI pursuant to a judicial warrant."[80] The report and its recommendations "appeared to persuade many in Congress" that legislation was needed to remove national security collection in the United States from the sole discretion of the Executive,[81] irrespective of the fact that the surveillance involved foreign powers and their agents. Instead of fighting this position based on the practical arguments and presidential foreign affairs power highlighted in the numerous previously cited court opinions,[82] the incoming President, Georgia governor and Washington outsider Jimmy Carter, supported it. As Senator Birch Bayh stated in a 1978

[78] *Id.*

[79] For a revelation of FBI documents reflecting communist connection with these movements see AFRICAN AMERICAN INVOLVEMENT IN THE VIETNAM WAR, *Protest on the Homefront, Martin Luther King, Jr., The Backlash*, http://www.aavw.org/protest/homepage_king_backlash.html (last visited Oct. 25, 2014); *see also* 129 CONG. REC. 26,870-78 (1983) (for the full text of the remarks of Senator Jesse Helms). Although the far right reputation of Senator Helms is well recognized, the documents speak for themselves.

[80] *See* Cinquegrana, *supra* note 61, at 807 (citing S. REP. NO. 97-755, bk. II, at 29, 320, 325, 327-28 (1976)).

[81] *Id.* at 807-08.

[82] In addition to *Keith* and the Appellate Court cases cited after, for historical opinions on the foreign affairs power see United States v. Curtis Wright Exp. Co., 299 U.S. 304 (1936), and for Presidential protective power see *In re* Neagle 135 U.S. 1 (1890).

hearing before the Senate Select Intelligence Committee's Subcommittee on Intelligence and the Rights of Americans:

> For the first time, to my knowledge, in history we have a President of the United States, who does not claim implied authority, but sends his right arm, the Attorney General of the United States, up here to support and indeed to help in drafting of legislation which governs the exclusive means by which Presidential authority may be exercised in this very controversial yet critical area.[83]

The result of the Church Committee report and President Carter's support was the Foreign Intelligence Surveillance Act of 1978.

## II. FOREIGN INTELLIGENCE SURVEILLANCE ACT

The statutory framework that Congress adopted to control foreign intelligence surveillance relies essentially on the same legal concept applied to criminal wiretaps in Title III of the Omnibus Safe Streets and Crime Control Act of 1968, but with some key modifications.[84] First, the statute is intended to provide procedures to obtain "foreign intelligence information" which is "information necessary to the national defense or security of the United States" or "the conduct of the foreign affairs of the United States."[85] Second,

---

[83] *Foreign Intelligence Surveillance Act of 1978*: *Hearing on S. 1566 Before the Subcomm. on Intelligence and the Rights of Americans of the S. Select Comm. on Intelligence*, 95th Cong. 3 (1978) (statement of Sen. Birch Barh, Chairman, S. Subcomm. on Intelligence).

[84] *See generally* ELIZABETH B. BRAZAN, CONG. RESEARCH SERV., RL30465, THE FOREIGN INTELLIGENCE SURVEILLANCE ACT: AN OVERVIEW OF THE STATUTORY FRAMEWORK AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT AND U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT OF REVIEW DECISIONS 5, 89-94 (2007) (discussing the Court of Review's comparison of the procedures in Title III with those in FISA, and finding in some respects that Title III had higher standards, while in others FISA included additional safeguards); *see also* Nicholas J. Whilt, *The Foreign Intelligence Surveillance Act: Protecting the Civil Liberties that Make Defense of Our Nation Worthwhile*, 35 SW. U. L. REV. 361, 371-83 (2006) (comparing FISA and Title III provisions to demonstrate the similarities between the two Acts and that Congress recognized the need to clearly distinguish foreign intelligence surveillance from criminal surveillance).

[85] 50 U.S.C. §§ 1801(e)(2)(A)-(B) (2012).

rather than establishing probable cause the target is committing a specific crime, the government must demonstrate probable cause to believe that the subject of the proposed surveillance is a foreign power or agent of a foreign power, which includes an international terror organization.[86]

To reduce the chance that FISA surveillance could interfere with the rights of U.S. persons, FISA requires "minimization procedures" that the Attorney General must adopt in order to prevent acquisition and retention and to prohibit dissemination of nonpublic information about U.S. persons.[87] In essence, FISA forbids disclosing information obtained from FISA surveillance except as provided in the minimization procedures,[88] although "information that is evidence of a crime which has been, is being, or is about to be committed can be retained or disseminated for law enforcement purposes."[89]

Subsequent amendments to the original legislation permitted physical searches according to a process parallel to electronic surveillance,[90] pen registers, trap and trace and business records acquisition,[91] interception of international communications that passed through the United States, and monitoring of "lone wolf" terrorists.[92] Another amendment imposed a requirement for a specially created FISA Court (also known as "FISC") approval before U.S. citizens could be targeted, even when outside the United States.[93] The amendment that caused the most angst among academics, scholars, and special interest groups, however, was a 2001 PATRIOT

[86] 50 U.S.C. §§ 1801(a)(4), 1805(2)-(3).
[87] 50 U.S.C. §§ 1801(h)(1), 1805(a)(4).
[88] *Id.* at § 1806(a).
[89] *Id.* at § 1801(h)(3); *see also* William C. Banks, *The Death of FISA*, 91 MINN. L. REV. 1209, 1231 (2007).
[90] Counterintelligence and Security Enhancements Act of 1994, Pub. L. No. 103-359, § 301(5), 108 Stat. 3423 (2001).
[91] Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, § 601, 112 Stat. 2396 (1998).
[92] 50 U.S.C. § 1801 (b)(1)(c).
[93] Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008, Pub. L. No. 110-261, § 702, 122 Stat. 2436.

Act change, which stated that only a "significant" intelligence purpose was required before a FISA order could be approved.[94]

Although no specific purpose was delineated in the original FISA legislation, the Fourth Circuit in *United States v. Truong*,[95] and subsequent DOJ practice, mandated that the "primary" purpose of FISA surveillance be intelligence collection.[96] This evolved into DOJ and FBI procedural requirements and interpretations that dictated there be virtually no communication between agents working towards a criminal prosecution and those concerned with obtaining foreign intelligence, even in an espionage or terrorism case.[97] As noted earlier in this Article, the 9/11 Commission highlighted the major problems in information sharing created by this "wall."[98] The PATRIOT Act brought the wall down by requiring the government to certify only that a "significant purpose" of the surveillance was intelligence collection,[99] leaving open the possibility that another purpose could be criminal prosecution. This in turn led to strenuous objections by FISA Court judges, the American Civil Liberties Union ("ACLU"), and the National Association of Criminal Defense Attorneys ("NACDA").[100] Their argument, in essence, was that the new FISA statute did not comply with the Fourth Amendment because it did not demand that the government show probable cause a crime was being committed, or a statement particularly describing

---

[94] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) of 2001, Pub. L. No. 105-56, § 218, 115 Stat. 272; 50 U.S.C. § 1804(6)(b). *See, e.g.,* David Hardin, Note, *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, 294 (2003); Joshua Pike, Note, *The Impact of a Knee-Jerk Reaction: The Patriot Act Amendments to the Foreign Intelligence Surveillance Act and the Ability of One Word to Erase Established Constitutional Requirements*, 36 HOFSTRA L. REV. 185, 185 (2007).

[95] United States v. Truong, 629 F.2d 908, 914-15 (4th Cir. 1980).

[96] Banks, *supra* note 89, at 1237.

[97] *Id.* at 1238.

[98] 9/11 COMMISSION REPORT, *supra* note 17, at 79; Breglio, *supra* note 19, at 193-94; Sievert, *supra* note 19, at 323-28, 331-35.

[99] USA PATRIOT Act. The Act also permitted law enforcement and intelligence to coordinate; *see* 50 U.S.C. § 1806(k)(1).

[100] *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002); brief for ACLU & NACDA as Amici Curiae, *In re* Sealed Case, 310 F.3d 717.

what was to be seized.[101] Agents could use the theoretically lesser standard, probable cause that a surveillance target is the agent of a foreign power, to get around the stricter requirements of the Title III criminal surveillance standard.[102]

The phrase "theoretically lesser standard" is utilized above because, as a former DOJ attorney very familiar with both forms of surveillance, the author can attest that it was in practice more difficult to get FISA approval than Title III authorization. FBI Director and former U.S. Attorney and Deputy Attorney General James Comey confirmed this in an address at Yale when he stated that it was a misconception that the standards for obtaining FISA warrants are lower, as in most cases it is easier to establish that a target is involved in criminal activity than to prove that the target is an agent of a terrorist organization. Furthermore, the bureaucratic review process for FISA and Title III warrants at DOJ is "something above probable cause."[103] Obtaining surveillance approval is hardly a cakewalk for the government, as it can take experienced lawyers up to a week to prepare the paperwork and the documents are "like mortgage applications in their complexity."[104]

Regardless, the specially-appointed FISA Court of Review (also known as the "FISA Appellate Court") rejected the ACLU's, NACDA's, and FISA judges' challenges to the "significant purpose" test by finding (1) FISA required a neutral and detached magistrate, (2) probable cause that someone is an agent of a foreign power is defined in terms of criminal activity to include any person knowingly engaging in espionage, sabotage, or terrorism,[105] (3) to the extent there are limited "particularity" requirements, *Keith* had found that different standards could be appropriate in national security surveillance, and (4) FISA, as amended to authorize surveillance

[101] *Id.* at 38 *et. seq*.
[102] Omnibus Crime Control and Safety Street Acts of 1968, Pub. L. No. 90-351, tit. III, §2518(3), 82 Stat. 197, 219.
[103] Breglio, *supra* note 19, at 189 (quoting James Comey).
[104] Richard Lacayo, *Has Bush Gone Too Far? The President's Secret Directive to Let the National Security Agency Snoop on American Citizens Without Warrants Sets Off a Furor*, TIME, Jan. 9, 2006, at 7.
[105] 50 U.S.C. § 1801(e)(1).

where one purpose might be criminal prosecution was, therefore, "reasonable" under the Fourth Amendment.[106]

The FISA Appellate Court's holding was not well received by many who had objected to the change. One District Court refused to follow it,[107] and law review articles reflected continuous attacks on the modified statute.[108] National security scholar William Banks acknowledged that FISA may have collapsed under its own weight because of its "complex formulations regarding who the government may target, how the government must construct the applications, and how the government must minimize its dissemination of information collected."[109] *In re Sealed Case*, however, in Banks' opinion, had eliminated its core requirements and central premise and effectively helped kill the statute.[110]

What is interesting for purposes of this Article is that *In Re Sealed Case* highlighted that:

> The *Truong* court, as did all the other courts to have decided the issue, held that the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information. It was incumbent upon the court, therefore, to determine the boundaries [used in a criminal prosecution] of that constitutional authority in the case before it. We take for granted that the President does have that authority and, assuming that is so, FISA could not encroach on the President's constitutional power.[111]

The Court followed this interesting explanation by summarizing prior Supreme Court holdings on "Special Needs," stating, "[T]he distinction between ordinary criminal prosecutions and extraordinary situations underlies the Supreme Court's approval of entirely warrantless and even suspicionless searches that are

---

[106] *In re* Sealed Case, 310 F.3d 717, 737, 740, 746 (FISA Ct. Rev. 2002).
[107] Mayfield v. United States, 504 F. Supp. 2d 1023, 1041 (D. Or. 2007).
[108] *See, e.g.,* Banks, *supra* note 89; Hardin, *supra* note 94; Pike, *supra* note 94.
[109] Banks, *supra* note 89, at 1211.
[110] *Id.* at 1214-15.
[111] *In re* Sealed Case, 310 F.3d at 742 (brackets added by the author for clarification as consistent with the context of the case and the court's discussion).

designed to serve the government's special needs beyond the normal need for law enforcement."[112]

That is, in the author's interpretation, Congress had imposed the requirement that there be probable cause to believe that the target was an agent of a foreign power before a FISA warrant could be granted. This understanding would make sense if the government knew at the time FISA was enacted that it would want to use the surveillance for criminal prosecution as contemplated by *Truong*. This does not mean, however, that establishing probable cause before a judge is constitutionally mandated any time the government wants to conduct surveillance in the United States against an agent of a foreign power, because the President has inherent foreign affairs authority to obtain foreign intelligence.

This of course also raises the interesting question whether FISA was at the start essentially an unconstitutional legislative infringement on the president's foreign affairs and commander-in-chief powers. That was certainly suggested by the Bush administration when the *New York Times* caused an uproar by disclosing that the government was conducting domestic surveillance of a few Al Qaeda suspects under the Terrorist Surveillance Program without going through the FISA Court.[113] After that revelation, Senator Pat Roberts stated, "Congress, by statute, cannot extinguish a core constitutional authority of the president."[114] Congress relied on the Commerce Clause, the Necessary and Proper Clause, and its regulation of the Department of Defense to pass the statute.[115] An earlier case, *Youngstown*, maintained that Congress could not encroach on the president's *fundamental* constitutional powers.[116] Although *Youngstown* and the more recent Supreme Court decision

[112] *Id.* at 745.
[113] James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES (Dec. 16, 2005), http://www.nytimes.com/2005/12/16/politics/16program.html?pagewanted=all&_r=0.
[114] Pete Yost, *Senate Intelligence Chairman: Bush Can Spy*, U-T SAN DIEGO (Feb. 3, 2006, 1:22 PM), http://legacy.utsandiego.com/news/nation/terror/20060203-1322-domesticspying.html.
[115] U.S. CONST. art. I, § 8, cl. 3; Banks, *supra* note 84, at 1279.
[116] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585-89 (majority opinion), 635, 637-38 (Jackson, J., concurring) (1952).

in *Hamdan v. Rumsfeld*[117] have been cited for the proposition that Congress can act to limit the president's authority with a statute like FISA, especially absent a declaration of war,[118] it is highly questionable whether, as the administration contended, the general Authorization for Use of Military Force ("AUMF") of 2001[119] would be a blanket grant of surveillance authority in the United States, especially in the face of the more specific FISA statute.[120]

The administration suspended the Terrorist Surveillance Program and there are no known cases before the Supreme Court challenging it or the original constitutionality of FISA. Thus FISA still stands today, and for the foreseeable future, as legislation mandating that the government demonstrate probable cause to believe a citizen or alien in the United States is an agent of a foreign power before electronic surveillance can be conducted against him for intelligence purposes.

## III. FISA AND PROBABLE CAUSE

When Congress decided to require that the government show a court probable cause before it could electronically surveil an agent of a foreign power, it took a long-established criminal law standard and applied it to the completely different field of foreign intelligence collection. Although this standard may make a little more sense today, as surveillance conducted for a "significant purpose" has the potential to be used in a subsequent criminal case, the fact remains that the essence of FISA is intelligence gathering, not criminal prosecution. Title III was and continues to be the primary vehicle for criminal cases and no one, to the author's knowledge, has made a serious claim to the contrary.[121] As will be further discussed, in many other situations where there are substantial safety and security reasons for the search, the Supreme Court has consistently

[117] Hamdan v. Rumsfeld, 548 U.S. 557 (2006).
[118] Banks, *supra* note 89, at 1211.
[119] *See* Authorization for of Use of Military Force, Pub. L. No. 107-40, 115 Stat. 224 (2001).
[120] Banks, *supra* note 89, at 1278-80.
[121] *See* 18 U.S.C. § 2510 (2002).

held that the standard of probable cause does not apply, regardless of the possibility of a later criminal indictment.

Probable cause is not simply a criminal law search standard, but the highest prerequisite for any search in U.S. law. The government can obtain a target's phone, financial, medical, and other records with a Grand Jury subpoena[122] or court order,[123] based only on the fact that the records are "relevant" to a federal investigation. If challenged, the court will uphold the government's authority unless "there is no reasonable possibility that the category of materials that the government seeks will produce information relevant to the general subject" of the investigation.[124] Police may stop your vehicle[125] or conduct a frisk of your person[126] based on "reasonable suspicion," meaning "specific and articulable facts . . . taken together with rational inferences from those facts" that suggest that criminal activity has occurred or is imminent.[127]

Searches of your home or the content of your communications in ordinary criminal cases are generally based on probable cause. This standard comes from the language of the Fourth Amendment:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[128]

Although, as will be discussed later, there is a very strong argument that the Fourth Amendment requires only "reasonable

[122] *See* FED. R. CRIM. P. 17(c)(1).
[123] 50 U.S.C. § 1861(d).
[124] United States v. R. Enters., 498 U.S. 292, 301 (1991).
[125] United States v. Arviza, 534 U.S. 266, 276-77 (2002).
[126] Terry v. Ohio, 392 U.S. 1, 30 (1968).
[127] *Id.* at 21.
[128] U.S. CONST. amend IV.

searches,"[129] and there are many exceptions to the probable cause rule, the Supreme Court has held as a general proposition that searches conducted without a probable cause warrant are unreasonable.[130] As the Court stated in *Chambers v. Maroney*, "[I]n enforcing the Fourth Amendment's prohibition against unreasonable searches and seizures, the Court has insisted upon probable cause as a minimum requirement for a reasonable search permitted by the Constitution."[131]

Probable cause can be defined as circumstances leading a reasonably cautious person to believe that certain facts are probably true,[132] or, in the words of the Supreme Court, there is a "fair probability" of their truth.[133] The Court has resisted efforts to define this in terms of a statistical percentage. "In dealing with probable cause . . . we deal with probabilities . . . The process does not deal with hard certainties."[134]

It would be helpful if the Supreme Court had addressed the exact meaning of probable cause in the context of national security. If the Court had articulated such a definition, it would be clear that probable cause in national security cases is a lesser standard than criminal law probable cause. The *Keith* Court certainly suggested this when it stated that a standard other than Title III may be compatible with the Fourth Amendment in a domestic security case.[135] The Court alluded to this concept decades later in dicta in a stop and frisk case, writing that "we do not say that the report of a person carrying a bomb need bear the same indicia of reliability we demand for the report of a person carrying a firearm before the police can constitutionally conduct a frisk."[136] The FISA Court of

[129] *See* Riley v. California, 134 S. Ct. 2473, 2482 (2014) (noting that "the ultimate touchstone of the Fourth Amendment is reasonableness") (internal quotations omitted).
[130] Chambers v. Maroney, 399 U.S. 42, 51 (1970).
[131] *Id.*
[132] BALLENTINE'S LAW DICTIONARY 431 (Legal Assistant ed. 1994).
[133] Illinois v. Gates, 462 U.S. 213, 238 (1983).
[134] *Id.* (quoting, in part, Brinegar v. United States, 338 U.S. 160, 176 (1949) and United States v. Cortez, 449 U.S. 411, 418 (1981)).
[135] United States v. U.S. Dist. Court (*Keith*), 407 U.S. 297, 322-23 (1972).
[136] Florida v. J.L., 529 U.S. 266, 273-74 (2000).

Review echoed this sentiment in *In Re Sealed Case*, stating that the "threat to society" should be a factor in determining the reasonableness of a search.[137] But the FISA Appellate Court also had to acknowledge that the Supreme Court, while conceding the need for "appropriately tailored roadblocks to thwart an imminent terrorist attack," cautioned in *Indianapolis v. Edmound* that in search cases "the gravity of the threat alone cannot be dispositive."[138]

Such language and speculation, while helpful for formulating a future approach, is far too vague to serve as concrete guidance to the police officer, federal agent, prosecutor, magistrate, or FISA judge who must make probable cause decisions on a daily basis. It should come as no surprise then that practitioners have come to focus on the word probable as meaning "more likely than not," so that

> [f]or practical purposes probable cause exists when an officer has trustworthy information sufficient to make a reasonable person think it more likely than not that the proposed arrest or search is justified. In math terms this implies that the officer or magistrate is more than 50 percent certain that the suspect has committed the offense or that the items can be found in a particular place.[139]

James Comey, when he was Deputy Attorney General, even stated that for FISA and Title III applications the government generally goes "beyond probable cause" to establish and maintain credibility with the courts.[140]

As noted at the beginning of this Article regarding the inability to obtain FISA warrants in the Moussaoui, Times Square Bomber, and Boston Marathon cases, this standard has created great difficulty in obtaining intelligence to defend the security of the United States. Terrorists and spies often operate in a loosely connected cell structure that can be hard to identify. They are well trained in avoiding detection, and their schemes can be quiet and

---

[137] *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002).
[138] Indianapolis v. Edmond, 531 U.S. 32, 42-44 (2000).
[139] ROLANDO V. DEL CARMEN, CRIMINAL PROCEDURE LAW AND PRACTICE 68 (9th ed. 2014).
[140] *See* Breglio, *supra* note 19, at 189.

nascent before suddenly erupting with devastating consequences. A DOJ internal report prior to 9/11 strongly suggested that the failure to obtain these warrants hindered the FBI in the Wen Ho Lee and Aldrich Ames espionage investigations which involved the transfer of enormously damaging national security information to our potential enemies.[141]

Attorney General Alberto Gonzales defended the Administration's much-criticized warrantless Terrorist Surveillance Program against Al Qaeda suspects in the United States on the basis that the FBI needed more "speed and agility" in meeting the threat.[142] National Security Agency ("NSA") Director Michael Hayden amplified Gonzales' comment in noting that the FISA probable cause standard was "too onerous."[143] Testifying about the number of man-hours required to do the paperwork for a FISA application, Director of National Intelligence Mike McConnell stated that "the current statutory requirement to obtain a court order based on probable cause, slows, and in some cases prevents altogether, the Government's efforts to conduct surveillance of communications it believes are significant to the national security."[144] In his opinion, this standard required "substantial expert resources towards preparing applications . . . (diverting them) from the job of analyzing collection results and finding new leads."[145]

---

[141] David A. Vise & Vernon Loeb, *Justice Study Faults FBI in Spy Case; Wen Ho Lee Probe Too Slow and Sloppy, Report Says,* WASH. POST, May 19, 2000, at A1, *available at* 2000 WLNR 10706687 (West).

[142] Alberto R. Gonzales, Att'y Gen of the United States, Prepared Remarks for Att'y Gen. Alberto R. Gonzales at the Georgetown University Law Center (Jan. 24, 2006), *available at* http://www.justice.gov/archive/ag/speeches/2006/ag_speech_0601241.html.

[143] Glenn Greenwald, *The Administration's New FISA Defense is Factually False*, UNCLAIMED TERRITORY (Jan. 24, 2006, 4:11 PM), http://glenngreenwald.blogspot.com/2006/01/administrations-new-fisa-defense-is.html.

[144] *Modernization of the Foreign Intelligence Surveillance Act: Hearing Before the S. Select Comm. on Intelligence*, 110th Cong. 19 (2007) (Statement of J. Michael McConnell, Dir. of Nat'l Intelligence).

[145] *FISA Hearing: Hearing Before the H. Permanent Select Comm. on Intelligence*, 110th Cong. 23 (2007) (Statement of J. Michael McConnell, Dir. of Nat'l Intelligence).

Such comments are not new or confined to those attempting to defend Executive Branch actions. In 1982, Senator Malcom Wallop expressed the view that the "net effect of FISA has been to confuse intelligence gathering with criminal law" and that it is "nonsense" to attempt a formula for comprehensive surveillance of those who constitute a security threat.[146] Scholar Gerald Reimers wrote that FISA's "extraordinary procedures and high standards of proof result in unnecessary delay if not a bar" to intelligence investigations.[147] Author Kim Taipale has written that when information comes from computers that do not know who placed the calls or their exact content, but legitimately focus the attention of government, it is almost impossible to establish probable cause in the FISA context.[148] Federal Judge Richard Posner stated that FISA's requirement of probable cause is no help "when the desperate need is to find out who is a terrorist."[149] Although strongly criticizing the expansion of FISA to include broad generic surveillance operations, noted professor William C. Banks recently acknowledged that in ongoing counterterrorism investigations where it might be impractical to seek a warrant "it is no longer realistic to argue that the Warrant Clause and its traditional law enforcement warrants and the criminal law version of probable cause should apply in the foreign intelligence context."[150] As one commentator stated in the *Wall Street Journal*, "One would think that agents charged with protecting us from a 'dirty nuke' would enjoy the same discretionary

---

[146] *Implementation of the Foreign Intelligence Surveillance Act of 1978*; *Report of the S. Select Comm. on Intelligence,* S. Rep. No. 97-691 at 10 (1982) (statement by Sen. Malcolm Wallop).

[147] Gerald F. Reimers II, *Foreign Intelligence Surveillance Act*, 4 J. NAT'L SECURITY L. 55, 101 (2000).

[148] Kim A. Taipale, *Whispering Wires and Warrantless Wiretaps: Data Mining and Foreign Intelligence Surveillance*, N.Y.U. REV. L. & SECURITY, No. VII SUPPL. BULL. ON L. & SEC. at n. 9 (Spring 2006), *available at* http://www.whisperingwires.info/.

[149] Richard A. Posner, Op-Ed., *A New Surveillance Act: A Better Way to Find the Needle in the Haystack,* WALL ST. J., Feb. 15, 2006, at A16.

[150] William C. Banks, *Programmatic Surveillance and FISA: Of Needles in Haystacks*, 88 TEX. L. REV. 1633, 1653 (2010). The general context of the article was an analysis of the FISA Court of Review Opinion *In re* Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008), pertaining to overseas surveillance of U.S. persons, but the wording is directly on point.

search authority as a patrolman who makes a traffic stop. In fact, they have less."[151]

The public claim that the FISA Court is somehow a rubber stamp because most applications are eventually approved, is completely ludicrous. This view does not reflect the real difficulty of obtaining a FISA order.[152] When the defense made a "rubber stamp" objection before the Ninth Circuit in *United States v. Cavanaugh*, the court noted that the lack of rejections was "consistent with a practice of careful compliance with statutory requirements on the part of the government."[153] Royce Lamberth, a former Chief Judge of the FISA Court, attributed the government's perfect record to the "superb internal review process created within DOJ,"[154] which requires personal approval of both the Attorney General and the head of the requesting agency for each FISA application. This often results in the submission of forty to fifty page affidavits at a minimum to FISA judges.[155] Judge Lamberth also stated that far from granting automatic approval of FISA requests, the Court often comes back to the government with questions and comments about their requests and often requires intelligence agencies to modify them to meet the Court's standards.[156] In 2013, Reggie Walton, current FISA Court presiding judge, said that "the court alters numerous government requests for data collection or even refuses some of them, even though that may not be reflected in the final statistics that the court sends to Congress."[157] In the opinion of Judge Richard Posner, the positive statistics are a reflection of the fact that the government is actually far too conservative in seeking surveillance orders. He

[151] Mark Riebling, *Uncuff the FBI*, WALL ST. J., June 4, 2002, at A20.
[152] Frederic J. Frommer, *Federal judge: FISA court not a rubber stamp,* AP NEWS, THE BIG STORY (July 11, 2013, 5:39 PM), http://bigstory.ap.org/article/federal-judge-fisa-court-not-rubber-stamp.
[153] United States v. Cavanaugh, 807 F.2d 787, 790 (9th Cir. 1987).
[154] BENJAMIN WITTES, THE FISA COURT SPEAKS, 226-27 (2008).
[155] Interview by The Third Branch with Judge Royce C. Lamberth, U.S. Dist. Court for the Dist. of Columbia (June 2002), http://www.uscourts.gov/ttb/june02ttb/interview.html.
[156] *Id.*; Frommer, *supra* note 152.
[157] Tom Risen, *FISA Judge Denies Surveillance Court Offers 'Rubber Stamp'*, U.S. NEWS & WORLD REPORT (Oct. 16, 2013, 1:10 PM), http://www.usnews.com/news/articles/2013/10/16/fisa-judge-denies-surveillance-court-offers-rubber-stamp.

believes that in our legalistic culture the FBI tries to avoid violating the law and does not want to sail anywhere close to the wind. "The analogy is to a person who has never missed a plane in his life because he contrives always to arrive at the airport eight hours before the scheduled departure time."[158]

## IV. CONSTITUTIONAL SEARCH WITHOUT PROBABLE CAUSE EVEN WHERE CRIME MAY BE DISCOVERED

In the words of Chief Justice Roberts, "As the text makes clear, 'the ultimate touchstone of the Fourth Amendment is reasonableness.'" [159] In other words, although the Fourth Amendment states that warrants should be supported by probable cause, the ultimate test of the constitutionality of a search is whether it is reasonable, not whether the government has established probable cause. Noted constitutional law scholar Akhil Amar has written that those who seek to impose a "global probable cause requirement have yet to identify even a single early case, treatise, or state constitution that explicitly proclaims 'probable cause' as the prerequisite for all 'searches and seizures.'"[160] In *National Treasury Employees Union v. Von Raab*, the Court stated that "neither a warrant nor probable cause, nor, indeed, any measure of individualized suspicion, is an indispensable component of reasonableness in every circumstance."[161] Rather, the reasonableness of a search is determined essentially by balancing the government's interest against the intrusion and expectation of privacy in the particular context of the case.[162]

An analysis of the Supreme Court's opinions demonstrates that there really is no inherent constitutional requirement that the government show probable cause before conducting a search for foreign intelligence purposes. In the past fifty years, the Court has

---

[158] Richard Posner, *Privacy, Surveillance and Law*, 75 U. CHI. L. REV. 245, 260 (2008).
[159] Riley v. California, 134 S. Ct. 2473, 2483 (2014) (citing Brigham City v. Stuart, 547 U.S. 398, 403 (2006)).
[160] Akhil Reed Amar, *Fourth Amendment First Principles,* 107 HARV. L. REV. 757, 782-83 (1994).
[161] Nat'l Treasury Employees Union v. Von Raab, 489 U.S. 656, 665 (1989).
[162] *Id.* at 665-67.

repeatedly sanctioned searches conducted without probable cause where significant safety and security concerns were present. The Court has not deviated from these holdings even where such searches may very well uncover criminal activity and eventually result in prosecution.

In *Chimel v. California*,[163] the Supreme Court found that there was no constitutional violation when officers searched the area within a defendant's reach at the time of arrest, even though there was no reason for suspicion, or probable cause to believe evidence or weapons were at hand. This ruling was justified by the government's need to seize weapons that might be present and could be used to assault an officer, as well as the need to prevent the possible destruction of evidence.[164] Although prohibiting Indianapolis' use of internal roadblocks for no reason other than drug control, the Court in *Edmond* still recognized that historically it has authorized searches even for the purpose of discovering criminal acts where a strong government interest outweighed general privacy concerns. Thus, in *United States v. Martinez-Fuerte*, the Court permitted suspicionless searches in border regions because of the "formidable law enforcement problems posed by the northbound tide of illegal entrants into the US."[165] In *Michigan v. Sitz*, the Court sanctioned stops without individual cause at roadblocks to identify drunk drivers who certainly would have been prosecuted upon discovery.[166] The Court also approved warrantless inspections of operators in the vehicle-dismantling industry because of the need to identify those involved in motor vehicle theft.[167] Some of these searches have been quite intrusive, such as the strip searches authorized for prisoners in *Florence v. Board of Chosen Freeholders*.[168]

[163] Chimel v. California, 395 U.S. 752 (1969) (abrogation recognized by Davis v. United States, 131 S. Ct. 2419 (2011)).
[164] *Id.* at 764.
[165] Indianapolis v. Edmond, 531 U.S. 32, 38 (citing U.S. v. Martinez-Fuerte, 428 U.S. 543, 551-54 (1976)).
[166] Michigan Dep't of State Police v. Sitz, 496 U.S. 444 (1990).
[167] New York v. Burger, 482 U.S. 691, 702 (1987).
[168] Florence v. Bd. of Chosen Freeholders, 131 S. Ct. 1510, 1517 (2012).

At the same time, there is a long series of cases approving detailed searches without probable cause pursuant to government programs where public safety, not crime control, is the primary purpose. In each of these cases there existed the simultaneous possibility of detecting crime. Because the primary programmatic purpose of the searches in these special needs cases was safety and security, the Court's decisions are directly in line with the foundational arguments of this Article. Thus, in *Colonnade Catering Corp. v. United States*[169] the Court endorsed warrantless searches of the private property of those involved in the catering and liquor industry. Two years later in *United States v. Biswell*,[170] a case related to the firearms industry, the Court again sanctioned warrantless searches without suspicion.

Both of these actions arguably involved "closely regulated" businesses, but in *Camara v. Municipal Court*[171] and in *Marshall v. Barlows*[172] the Court authorized non-probable cause searches to insure compliance with general city housing, and occupational safety codes in simple electrical and plumbing businesses, respectively. These latter searches would have to be made in accordance with a warrant to insure that authorities did not unfairly target only particular corporations for political or other improper reasons. Yet, as the Court stated in *Barlows*, "Probable cause in the criminal sense is not required . . . [a warrant may issue] on a showing that reasonable legislative or administrative standards for conducting an inspection are satisfied."[173]

*Colonnade*, *Camara*, and *Barlows* permitted detailed and highly invasive searches for public safety purposes without any degree of suspicion. When reasonable suspicion is actually present and there is a compelling government interest, courts have approved what may be categorized as highly invasive searches. In *United States v. Flores-Montano*, the Supreme Court stated that because of the "longstanding right of the sovereign to protect itself" at the border,

[169] Colonnade Catering Corp. v. United States, 397 U.S. 72, 77 (1970).
[170] United States v. Biswell, 406 U.S. 311, 317 (1972).
[171] Camara v. Municipal Court, 387 U.S. 523, 540 (1967).
[172] Marshall v. Barlows, 436 U.S. 307, 339 (1978).
[173] *Id.* at 320.

"highly intrusive searches of the person," "searches of property that are destructive," and even searches carried out in a "particularly offensive manner" may be permitted with reasonable suspicion.[174] The Ninth Circuit followed this reasoning in *United States v. Cotterman*, holding that computer contents could actually be forensically examined and copied at the border based on reasonable suspicion.[175]

It should be noted that in 2008 the FISA Court of Review took a step in the direction of acknowledging the applicability of the above-cited special needs cases in the domestic FISA context with its decision in *In Re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*.[176] The case involved a service provider's appeal of a FISA Court finding that it was constitutional for the Attorney General to direct the interception of the communications of a U.S. person located outside the United States.[177] At the time, this had been authorized without a FISA Court order pursuant to the Protect America Act of 2007 ("PAA").[178] One year later, Congress passed the FISA Amendments Act ("FAA")[179] requiring a FISA Court order when surveillance was directed against U.S. persons even if they were located outside the United States. Analyzing the controlling PAA, the FISA Court of Review expressly found there is a "foreign intelligence exception" to the warrant requirement that parallels the "special needs" exception, a notion previously only hinted at in the *In Re Sealed Case* opinion.[180] In the FISA Appellate Court's opinion:

> The [Supreme Court] has recognized a comparable exception, outside the foreign intelligence context, in so-called 'special needs' cases. In those cases, the Court excused compliance with the Warrant Clause when the purpose behind the

[174] United States v. Flores-Montano, 541 U.S. 149, 152, 156 n.2 (2006).
[175] United States v. Cotterman, 709 F.3d 952, 970 (9th Cir. 2012).
[176] *In re* Directives, 551 F.3d 1004 (FISA Ct. 2011).
[177] *Id.*
[178] Protect America Act of 2007, Pub. L. No. 110-55, 121 Stat. 552 (codified at 50 U.S.C. §§ 1805(a)-(c)) (2010)).
[179] FISA Amendments Act of 2008, Pub. L. No. 110–261, §§ 701-03, 122 Stat. 2436 (codified at 50 U.S.C. §§ 1881 (2008)).
[180] *In re* Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

> governmental action went beyond routine law enforcement and insisting upon a warrant would materially interfere with the accomplishment of that purpose.[181]

The FISA Court of Review further found that "here the relevant government interest—the government's interest in national security—was of the highest order of magnitude."[182] Individual privacy rights, on the other hand, were protected by executive branch findings, certifications, and minimization requirements restricting the distribution of the information. The surveillance therefore met the key "reasonableness" test of the Fourth Amendment. It is true that the particular circumstances of this case involved surveillance of U.S. persons outside the United States pursuant to numerous, undisclosed, classified restrictions, but the language and theory applied by the Court is highly significant.

There are certainly strong government interests in enforcing city housing and occupational safety codes, as well as stopping illegal immigration. But these cannot compare with the need of the government to protect the nation against a potentially devastating attack perpetrated by a rogue or ambitious nation or, more likely, by a terrorist organization with nothing to lose because it has no home territory to protect. This is an interest "of the highest order of magnitude."[183] As Judge Wilkinson wrote, that the current war is unconventional does not make its consequences any less grave.[184] This is especially true as non-state actors continually seek to obtain WMDs. Such weapons in the hands of committed terrorists pose a potentially existential threat to the nation and, in this context, our need for accurate, timely intelligence cannot be overstated.

On the other side of the balancing test suggested by the Court's cases, intelligence targets have a strong privacy interest in the confidentiality of their communications, but businesses, multi-unit home owners, and drivers have a significant privacy interest in

---

[181] *In re* Directives, 551 F.3d at 1010.
[182] *Id.* at 1012.
[183] *Id.*
[184] Hamdi v. Rumsfeld, 316 F.3d 450, 464 (4th Cir. 2003) (quoting Hamdi v. Rumsfeld, 296 F.3d 278 (4th Cir. 2002)).

protecting against government intrusions on their property. These private entities did not prevail even where there was no reasonable suspicion and the government's need was much less than exists in the national security context.

There are other elements of the "reasonableness" equation that are mentioned in *Flores-Montano*, *Camara*, and *Barlows* that should be considered when evaluating what the Court might approve in national security surveillance cases. Specifically, *Flores-Montano* and *Cotterman* both held that when reasonable suspicion is present, government border searches of the person or their property could be "highly intrusive." *Camara* and *Barlows*, while acknowledging that probable cause was not needed, still inserted the need for some type of judicially approved warrant to insure that government's search decisions would be made on an objective, acceptable, non-political basis. As the Court said in *Barlows*, a warrant would show that the subject of the search was chosen after reviewing "neutral sources" and thus clearly protect an employer's Fourth Amendment rights.[185]

In 1969, former Nuremberg prosecutor, Justice Jackson protégé, and law professor Telford Taylor argued that the courts should not be involved in the surveillance process at all. Wiretaps were non-adversary steps in the investigative process and there was no case or controversy that would warrant judicial intervention. Such surveillance should be solely an executive decision.[186] This position appears rather naïve today in light of the complete interjection of the judiciary into the surveillance process under Title III in 1968 and FISA in 1978. In the author's opinion, it is also highly unlikely that the Supreme Court would find government intrusion without some type of judicial review to be constitutional.

The analysis above, however, strongly suggests that a statute authorizing intelligence surveillance warrants based on reasonable suspicion alone would and should pass constitutional muster. Time and again the Supreme Court has recognized that detailed searches can be conducted without establishing probable cause, even when the

[185] Marshall v. Barlows, 436 U.S. 307, 339 (1978).

[186] TELFORD TAYLOR, TWO STUDIES IN CONSTITUTIONAL INTERPRETATION: SEARCH, SEIZURE, AND SURVEILLANCE AND FAIR TRIAL AND FREE PRESS 83-90 (1969).

results of those searches could, as with intelligence surveillance, potentially result in criminal prosecution. Such a statute would insure that the government's overwhelming interest in safeguarding our population would be met far better than it is now with the obstacles created by the burdensome FISA standard of probable cause. Privacy would be protected by a warrant process guaranteeing judicial control and guidance so that surveillance could not be initiated for political, partisan, or personal reasons, and by the need to demonstrate there was reasonable suspicion, or specific articulable facts to suspect a specific target. Congress overreacted when it imposed the highest criminal law search standard on foreign intelligence surveillance and the result of their decision has proven hazardous to the American people. Meanwhile, our European allies have demonstrated a civilized respect for individual privacy but, as will be discussed in the next section, many recognize that imposing such hurdles is far too dangerous when it comes to protecting a nation's security.

## V. NATIONAL SECURITY SURVEILLANCE IN EUROPE

Numerous legal commentators have written quite favorably about the European approach to privacy protection as opposed to what they consider more intrusive U.S. laws.[187] In their opinion, "The U.S. Constitutional amendment protections (as applied) and U.S. federal and state laws fall short" of international standards.[188] The European convention and the enforcement mechanisms

[187] Francesca Bignami, *European versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609 (2007); Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L. J. 751 (2003); Jeffery A. Brauch, *Human Rights Protections in the Post 9/11 World*, 31 QUINNIPIAC L. REV. 339 (2013); European Digital Rights Initiative (EDRi) & Fundamental Rights Experts Grp. (FREE), *Submission to the United States Cong., the European Parliament and Comm'n & the Council of the European Union, & the Secretary-General & the Parliamentary Assemb. of the Council of Eur. on the surveillance activities of the United States and certain European States' national security and "intelligence" agencies* (Aug. 2013), http://www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/submission_us-europe_edri_final/submission_us-europe_edri_finalen.pdf.

[188] *EDRi* & *FREE*, *supra* note 187, at 15.

embodied by the European Court of Human Rights are considered to form the "most comprehensive and effective system for the protection of human rights in the world."[189] As might be expected, in Europe there was loud and public (if hypocritical) fury over what some believed to be Edward Snowden's "monstrous allegations of total monitoring of various telecommunications and internet services."[190]

Yet, according to a study by the Max Planck Institute, as observed by Stewart Baker, "[Y]ou're 100 times more likely to be surveilled by your own government if you live in the Netherlands or if you live in Italy . . . 30 to 50 times more likely to be surveilled if you're a French or German national than in the United States."[191] In national security matters, most of the major European powers, unlike the United States, do not require either judicial approval or probable cause before the executive branch with general legislative oversight can conduct electronic surveillance.[192] A more nuanced analysis of

[189] Brauch, *supra* note 187; MARK W. JANIS ET AL., EUROPEAN HUMAN RIGHTS LAW: TEXT AND MATERIALS 3 (2nd ed. 2000).

[190] David Wright & Reinhard Kreissl, *European Responses to the Snowden Revelations: A Discussion Paper* 8 (Dec. 2013), *available at* http://irissproject.eu/wp-content/uploads/2013/12/IRISS_European-responses-to-the-Snowden-revelations_18-Dec-2013_Final.pdf.; *see also id.* at 13 (for a discussion of the hypocrisy of European politicians criticizing the United States when their own agencies have been carrying out mass surveillance programs).

[191] Tom Gjelten, *Weekend Edition: Which Citizens Are Under More Surveillance, U.S. or European?* (NPR radio broadcast July 28, 2013), http://www.npr.org/2013/07/28/206231873/who-spies-more-the-united-states-or-europe (quoting statement by former NSA General Counsel Stewart Baker). Baker appears to be referring to HANS-JÖRG ALBRECHT ET AL., RECHTSWIRKLICHKEIT UND EFFIZIENZ DER ÜBERWACHUNG DER TELEKOMMUNIKATION NACH DEN §§ 100A, 100B STPO UND ANDERER VERDECKTER ERMITTLUNGSMAßNAHMEN [LEGAL REALITY AND EFFICIENCY OF THE SURVEILLANCE OF TELECOMMUNICATIONS UNDER §§ 100A, 100B OF THE CRIMINAL PROCEDURE CODE AND OTHER CONCEALED MEASURES FOR INVESTIGATIONS] (2003). *See* Stewart Baker, *Europe, the Cloud, and the New York Times*, VOLOKH CONSPIRACY (Oct. 16, 2013, 6:10 AM), http://www.volokh.com/2013/10/16/europe-cloud-new-york-times/. Paul M. Schwartz challenges the study on various grounds including the fact that the United States does not count consensual monitoring and the Max Plank Institute did. Paul M. Schwartz, *Evaluating Telecommunications Surveillance in Germany: The Lessons of The Max Planck Institute's Study*, 72 GEO. WASH. L. REV. 1244, 1251-52 (2004).

[192] A key survey was conducted by Christopher Wolf who summarized his findings with the following 2013 quote for NPR: "We can have a debate over whether or not

European culture and law suggests that citizens focus more on "personal dignity" and "interpersonal relations" than on fear of government action taken to protect the nation.[193] Although there is some dispute among scholars, there seems to be recognition that European citizens do not want the media or their neighbors to have access to their personal life, nor do they want a totalitarian government to marshal and manipulate files on private citizens, but, at the same time, they want to protect their country against invasion and terrorist threats.[194] Francesca Bignami traces this thinking to the Nazi invasions that first destroyed the sovereignty of European nations, then subjugated the citizenry, in part through access to personal files.[195]

It is interesting that the European Data Protection Directives and proposed regulations reflect these distinct purposes.[196] These documents, drafted in 1995, 2002, and 2012, which encourage harmonizing legislation among states and could eventually result in enforceable law, require that businesses should process "personal data" only with consent and only when absolutely necessary, and then only for a short time, so there is a "right to be forgotten."[197] At the same time, the European Union's Data Retention Directive of 2002 attempts to insure that internet and telephone companies maintain data as to the identity, source, time, duration, and

---

the judicial and legislative approval process is working here in America, but the fact is, it exists, and in many places in Europe you don't have that kind of due process . . . You don't have legislative oversight. In fact, the national security investigations are done completely in the dark or mostly in the dark." Gjelten, *supra* note 191.

[193] *See* James Q. Whitman, *Two Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1155-62 (2004); Bignami, *supra* note 187, at 609-11; *see also* Saperstein, *supra* note 32, at 1965-67.

[194] *See* Bignami, *supra* note 187, at 621.

[195] *See id.* at 609-10; Saperstein, *supra* note 32, at 1965-66.

[196] *See* Council Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 31-38; *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Data and on the Free Movement of Such Data*, at 1-2, 6-7, COM (2012) 11 final (Jan. 25, 2012).

[197] *See* Paul M. Schwartz, *The EU-U.S. Privacy Collision: A Turn To Institutions and Procedures*, 126 HARV. L. REV. 1966, 1994-95 (2013).

destination of all communications for six to twenty-four months, to aid in "the fight against serious crime and terrorism."[198]

European law is complex, but in essence each State is responsible for maintaining law and order and safeguarding its national security[199] while complying with the privacy mandates of Article 8 of the European Convention on the Protection of Human Rights.[200] Article 8, "Right to respect for private and family life," provides that

> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic wellbeing of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[201]

"Accordance with law" means that the law must be accessible to the public and precise enough that citizens understand the

---

[198] *See* Benjamin Wittes, *Mark Klamberg on EU Metadata Collection*, LAWFARE (Sept. 29, 2013 1:03 PM), http://www.lawfareblog.com/2013/09/mark-klamberg-on-eu-metadata-collection/. The Court of Justice of the European Union rejected the Retention Directive in 2014 in a case brought by the Netherlands and Ireland. Joined Cases C-293/12 & C-594/12, Digital Rights Ireland Ltd. v. Minister for Comm'ns, Marine and Natural Res., 2014 EUR-Lex CELEX LEXIS ¶ 41 (Apr. 8, 2014). The ramifications of the decision are unclear as many nations passed legislation conforming to the guidance of the Directive and the ECHR has not found these statutes to be illegal. *Id.*

[199] *See* Kaarlo Tuori, *A European Security Constitution*, *in* LAW AND SECURITY IN EUROPE: RECONSIDERING THE SECURITY CONSTITUTION 59 (Massimo Fichera & Jen Kreme eds., 2013).

[200] *See* Wittes, *supra* note 198, at 2.

[201] Council of Europe, *European Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols Nos. 11 and 14*, art. 8, Nov. 4, 1950, ETS 5, *available at* http://www.echr.coe.int/Documents/Convention_ENG.pdf.

requirements and consequences of violation.[202] "Necessary in a democratic society" means that the law must be proportionate to the legitimate aims pursued.[203] National courts, and ultimately the European Court on Human Rights ("ECHR"), will determine if a state statute is in accordance with law and necessary in a democratic society.[204] "A margin of appreciation is left to the competent national authorities" in assessing what is necessary, especially in matters of national security,[205] although it is not uncommon for each nation's law to be challenged before and ruled upon by the ECHR.[206]

The following summary of key national security surveillance law provisions and practices in the major European powers draws from studies conducted by Winston Maxwell and Christopher Wolf,[207] Privacy International,[208] law review articles, and instructive court decisions, along with numerous other cited sources.

*Germany*

1. In national security cases, German authorities may conduct individually targeted or strategic collection of communications without Court Order. The responsible Federal Minister of Federal State Authority may order these measures.[209]

2. Because the law is designed to be preventative in nature, a lower standard of "actual indications" rather than probable cause

[202] *E.g.,* Wittes, *supra* note 198, at 2. These formulations actually are mentioned in numerous ECHR decisions, some of which will be referenced in the following section on cases reviewing European state law.
[203] *Id.*
[204] *Id.*
[205] *Id.*
[206] *See, e.g.*, Press Release, Court of Justice of the European Union, The Court of Justice Declares the Date Retention Directive to be Invalid (April 8, 2014), http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf.
[207] *See* MAXWELL & WOLF, GLOBAL REALITY, *supra* note 32, at 8-12; MAXWELL& WOLF, A SOBER LOOK, *supra* note 32, at 5-9.
[208] *See* PRIVACY INT'L, *supra* note 32.
[209] MAXWELL & WOLF, A SOBER LOOK, *supra* note 32, at 8.

or reasonable belief was found to be a more appropriate standard for this non-judicial process.[210]

3. Oversight is provided by a parliamentary Control Panel that appoints a non-judicial, supervisory body called the G-10 Committee.[211]

4. In the landmark 1978 case of *Klass v. Germany*, the European Court of Human Rights found this system of oversight was not violative of Article 8 of the Convention and that "the exclusion of judicial control does not exceed the limits of what may be deemed necessary in a democratic society."[212]

*United Kingdom*

1. Under the Regulatory and Investigatory Powers Act of 2000 ("RIPA"), authorities may order public and private telecommunications entities to provide data.[213] The Secretary of State (Home Secretary) may also issue orders for actual interception of communications in national security and other serious cases without judicial supervision. [214]

2. The standard for the above orders is that the Secretary must find them "necessary" for the interests of national security and "proportionate to what is sought to be achieved by the conduct."[215]

3. Oversight is provided by Interception of Communications and Intelligence Service Commissioners and an Investigatory Powers Tribunal which can hear complaints. Although members are appointed from the ranks of senior judges, this is not before-the-fact judicial review as "the operations of MI-5 and MI-6 are largely beyond the discretion of the courts, insulat(ing) serious

[210] Saperstein, *supra* note 32, at 1976 (citing IAIN CAMERON, NATIONAL SECURITY AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS 110 (2000)).
[211] MAXWELL & WOLF, A SOBER LOOK, *supra* note 32, at 8.
[212] Saperstein, *supra* note 32, at 1977 (citing Klass v. Fed. Republic of Ger., 28 Eur. Ct. H.R. (ser. A) 1, at 20-21, 23 (1978)).
[213] RIPA, 2000, c. 23, § 22. See MAXWELL & WOLF, *supra* note 32, at 8 for a discussion of RIPA.
[214] RIPA, 2000, c. 23, § 5(3).
[215] *Id.* at §§ 5(2)(a), (3)(b).

crimes against the State such as terrorism and espionage from the scrutiny deserving of more ordinary criminal investigations."[216]

4. The specifics of the RIPA legislation are important, as the ECHR had previously found in *Malone v. U.K.*[217] and *Liberty v. U.K.*[218] that prior UK law was not precise and clear enough to meet the "in accordance with law" component of Article 8. The ECHR found in 2010 that RIPA, however, fully complied with Article 8 in *Kennedy v. United Kingdom*.[219]

*France*

1. The Government may conduct general untargeted monitoring of the airwaves and internet traffic without review.[220]

2. When "broad surveillance reveals a potential threat," under the Internal Security Code, a targeted interception can be implemented without judicial review after authorization from the Prime Minister's Office.[221]

3. A new Anti-Terror Act was enacted on January 23, 2006. It grants increased powers to the police and intelligence services, allowing them to get telecommunications data directly from Internet Service Providers, apparently with no need for permission from the Prime Minister's Office.[222] A recent French law will also permit the government to request connection data from telecommunications operators and Internet companies in real time, not only for national security reasons, but also "to

[216] Saperstein, *supra* note 32, at 1979-80.
[217] Malone v. U.K. 82 Eur. Ct. H.R. (ser. A) 1 *passim* (1984).
[218] Liberty v. U.K., Eur. Ct. H.R. (Jan. 10, 2008), http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-87207#{itemid":["001-87207"]}.
[219] Kennedy v. U.K., Eur. Ct. H.R. (May 18, 2010) http://hudoc.echr.coe.int/sites/eng/pages/search.aspx?i=001-98473#{"itemid":["001-98473"]}.
[220] MAXWELL & WOLF, A SOBER LOOK, *supra* note 32, at 7 n.53.
[221] *Id.*
[222] PRIVACY INT'L, *supra* note 32 (citing Contrôle de l'application de la loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers (Oct. 21, 2014), http://senat.fr./application-des-lois/pj105-109.html).

protect the scientific and economic potential of France" and "fight criminality."[223]

4. Oversight is provided by a special security commission made up of one person appointed by President, one member of the National Assembly, and one member of the Senate.[224]

5. Prior to 1991 there were no specific laws regulating surveillance. The laws mentioned above were passed after the ECHR, in *Kruslin v. France*, found that, pursuant to Article 8, France must have a specific code.[225]

*Spain*

1. Generally the government must obtain a court issued warrant to intercept communications, but in limited instances the government may obtain the information without a warrant and cloud service companies may provide the information voluntarily.[226] The National Police and Guardia Civil apparently have developed a program with SINTEL, a telephone installation company, that enables them to obtain telephonic communications without court authorization.[227]

2. Courts grant warrants using a standard of "sufficient evidence that the intercepted communication would be material to a criminal investigation."[228]

3. Spain has declared to the EU Data Protection Working Party that its law "provides for parliamentary oversight and/or control over the activities of intelligence services alongside the

[223] Emily Picy & Leila Aboud, *Opponents of French Surveillance Law Race to Get Support for Review*, REUTERS (Dec. 12. 2013), http://www.reuters.com/article/2013/12/12/us-france-surveillance-idUSBRE9BB15M20131212.
[224] MAXWELL & WOLFE, A GLOBAL LOOK, *supra* note 32, at 7.
[225] Kruslin v. France, Eur. Ct. H.R. (Apr. 24, 1990), http://hudoc.echr.coe.int/sites/eng/pages/search/aspx?i=001-5726#["itemid":["001-5727"]}.
[226] MAXWELL & WOLFE, GLOBAL REALITY, *supra* note 32, at 10-11.
[227] PRIVACY INT'L, *supra* note 32.
[228] MAXWELL & WOLF, GLOBAL REALITY, *supra* note 32, at 11.

competences of the data protection authorities for the data processing."[229]

4. Spain has been prompted by its national courts to set up a system of clear regulation.[230]

*Italy*

1. Italy conducts numerous wiretaps, with the number of phones targeted "widely seen as among the highest in Europe."[231] Under law 155/200, the Prime Minister decides whether or not to intercept, then submits an application to a three judge panel.[232] Traditionally judges have been investigative magistrates similar to US prosecutors.[233] "Preemptive wiretapping," where there is no public prosecutor investigation, is allowed in national security cases.[234]

2. The standard applied when determining wiretap approvals appears to be whether it is "indispensable" to the government's need in the investigation. Grave evidence of a crime is necessary for ordinary criminal wiretaps, but these restrictions do not apply to mafia and national security investigations.[235]

---

[229] *Report of the Data Protection Working Party* (Apr. 10, 2014), http://www.cnpd.public.lu/fr/publications/groupe-art29/wp215 en.pdf.
[230] *See* PRIVACY INT'L, *supra* note 32; *El Supremo Cree Inaplazable Regular El Control de Teléfonos* (Dec. 13, 2004), http://elpais.com/diario/2004/12/13/espana/1102892412_850215.html.
[231] Rachel Donadio, *An Untapped Phone in Italy? It's Possible*, N.Y. TIMES (May 10, 2010), http://www.nytimes.com/2010/05/31/world/europe/31italy.html?pagewanted=all&_r=0 (reporting 112,000 phones targeted in 2009); Alesandro Rizzo & Colleen Barry, *Wiretap Bill Spurs Debate and Protests in Italy*, SALON (July 8, 2010), http://www.salon.com/2010/07/08/eu_italy_stop_listening/.
[232] Donadio, *supra* note 231.
[233] Eric Weiner, *Wiretapping European Style*, SLATE (Feb. 14, 2006), http://www.slate.com/articles/news_and_politics/how_they_do_it/2006/02/wiretapping_europeanstyle.html.
[234] PRIVACY INT'L, *supra* note 32.
[235] Stacy Meichtry & Margherita Stankaty, *Italy's Senate Approves Wiretap Bill*, WALL ST. J. (June 14, 2010), http://online.wsj.com/news/articles/SB10001424052748703627704575298771076540944.

3. The Italian Parliament and the Italian Data Protection Authority, known as the Garante, provide oversight of potential privacy violations.[236]

4. Italy's 2010 wiretap law has drawn protests from media who can be fined for publishing leaks, as well as from prosecutors who had even fewer restrictions in the past.[237]

A review of these laws reveals that four out of these five countries do not require judicial review before surveillance in national security cases and none demand that the government show probable cause. Phrases like "necessary and proportionate," "actual indications," "potential threat," "material," and "indispensable to the government" all suggest that the government cannot conduct surveillance without good reason. But none of these imply that the government must wait to obtain sufficient evidence to demonstrate to a court that, at the time surveillance is initiated, the target, more likely than not, is guilty of a crime or is an agent of a foreign power. European law is "designed to be preventative in nature," discovering plots in the planning stages before it may be too late to thwart an attack.[238] Yet each of these laws complies with "the most comprehensive and effective system for the protection of human rights in the world" as enforced by the European Court of Human Rights.[239]

As noted above, the fact that these European nations and courts have not burdened the government with excessive standards in national security cases can, in part, be attributed to cultures that focus on dignity and security after the "searing legacy of World War II."[240] But the repeated tragedies of terrorist attacks in France in the 1960's related to Algerian independence,[241] the horrific Munich

[236] *Italian Legislation Data Protection Code*, http://www.garanteprivacy.it/home_en/italian-legislation (last visited Oct. 28, 2014).
[237] Donadio, *supra* note 231; Rizzo & Barry, *supra* note 231.
[238] *See* Saperstein, *supra* note 32, at 1975-76 (quoting IAIN CAMERON, NATIONAL SECURITY AND THE EUROPEAN CONVENTION ON HUMAN RIGHTS 110 (discussing the incompatibility between rigorous legal standards and national security objectives)).
[239] Brauch, *supra* note 187.
[240] Saperstein, *supra* note 32, at 1966.
[241] *Id.* at 1970.

massacre, the outrages of the Bader-Meinhof gang in Germany,[242] the thirty year battle with the IRA in the UK,[243] and the shocking assaults of the Red Brigades in Italy, resulting in the assassination of popular Prime Minister Also Moro,[244] certainly had an impact on European populations, and created a political will to avoid imposing needless burdens on their security services. In the words of the ECHR, "Democratic societies nowadays find themselves threatened by highly sophisticated forms of espionage and by terrorism, with the result that the State must be able, in order effectively to counter such threats, to undertake the secret surveillance of subversive elements operating within its jurisdiction."[245]

The events of September 11th of course shocked the United States. Yet it is only through skill and luck that we have managed to avoid repeated attacks of the kind endured by Europe in the twentieth century. Our intelligence agencies continue to labor under the legally unjustifiable probable cause standard established by the ill-conceived Foreign Intelligence Surveillance Act of 1978. As shown above, probable cause and judicial review are not mandated by the rigorous standards of European Human Rights law or by U.S. Supreme Court decisions highlighting the requirement of reasonableness in Fourth Amendment searches. We must now ensure that we do not repeat past mistakes by overreacting to the Edward Snowden revelations of 2013.

## VI. POTENTIAL LEGAL DANGER ASSOCIATED WITH THE METADATA REVELATIONS

As noted previously, there have been strong public reactions to the revelations of Edward Snowden which identified NSA surveillance in Europe, NSA access to European conversations

[242] *See Who Were the Baader-Meinhof Gang?*, BBC News (Feb. 12, 2007 6:18 GMT), http://news.bbc.co.uk/2/hi/europe/6314559.stm.
[243] *See* Ann Marie Imbornoni et al., *The Northern Irish Conflict: A Chronology*, INFOPLEASE, http://www.infoplease.com/spot/northireland1.html (last visited Oct. 28, 2014) for a discussion on the IRA conflict and resulting terrorism.
[244] *See 1978 Aldo Moro Snatched at Gunpoint*, BBC NEWS, http://news.bbc.co.uk/onthisday/hi/dates/stories/march/16/newsid_4232000/4232691.stm (last visited Oct. 28, 2014).
[245] Klass v. Fed. Republic of Ger., 28 Eur. Ct. H.R. (ser. A) 1, 48 (1978).

passing through the United States, NSA access to some content of the international conversations of U.S. persons, and the collection of metadata on all calls in the United States for a period of five years.[246] The primary concern for purposes of this Article is the metadata program and the litigation surrounding it.

Metadata refers to the accumulation by NSA of data on numbers dialed, and time and duration of calls made by telephone subscribers both overseas and in the United States. Metadata does not include content.[247] It is the same information routinely collected by the government with a pen register/trap and trace order based on simple "relevance" to a federal investigation.[248] The legal controversy surrounding the collection of this data has been highlighted in two excellent, but opposing, opinions by U.S. District Judges in *Klayman v. Obama*[249] and in *ACLU v. Clapper*.[250]

One of the focal points of both District Court decisions was the third party doctrine, developed by the Supreme Court with respect to bank records in *United States v. Miller* in 1976,[251] and with respect to telephone records in *Smith v. Maryland* in 1979.[252] Under this doctrine, since the Fourth Amendment applies only to government searches where one has a reasonable expectation of privacy, and since a person has no such expectation in what he shares with a third party, the government need not obtain a search warrant or show probable cause to obtain data shared with a third party.[253]

---

[246] *See* Jacobsen & Barber, *supra* note 33; Jim Newell, *Thousands Gather in Washington in Anti-NSA 'Stop Watching US' Rally*, THE GUARDIAN (Oct. 26, 2013), http://www.theguardian.com/world/2013/oct/26/nsa-rally-stop-watching-washington-snowden.

[247] *See* Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) and ACLU v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) for descriptions of the metadata program.

[248] 18 U.S.C. §§ 3121-3127 (2014); Sievert, *supra* note 19, at 335-37.

[249] Klayman, 957 F. Supp. 2d. 1.

[250] Clapper, 959 F. Supp. 2d 724.

[251] United States v. Miller, 425 U.S. 435 (1976).

[252] Smith v. Maryland, 442 U.S. 735 (1979).

[253] *Id.* at 743-44.

Judge Leon in *Klayman* tried to distinguish *Smith* in part on the grounds that *Smith* involved a short-lived pen register, whereas the metadata program collected the records of hundreds of millions of citizens over five years.[254] He also believed that the ubiquity of cell phones today had dramatically altered the quantity of information that is available and what the information can tell about people's lives.[255] Therefore, in Judge Leon's opinion, the collection and search of these records compromised a strong privacy interest. Moreover, the government's claim that the program was needed "to identify unknown terrorist operatives and prevent terrorist attacks" was undermined by the fact that the government had not shown that identification through metadata collection had "actually stopped an imminent attack."[256] This latter point is curious, as stopping a criminal or terrorist attack in the planning stages is equally, if not more effective, than stopping it immediately before the act is committed. If authorities wait, there is never any guarantee they will be able to prevent conspirators from succeeding at a later date when the attack is "imminent."

Judge Pauley, in *Clapper*, countered the *Klayman* decision by noting that *Smith*'s bedrock holding is that individuals have no expectation of privacy in what they knowingly give to third parties, and that the information conveyed (basic call data) was no different than that obtained in *Smith*.[257] While people may have an entirely different relationship with telephones now than they did thirty-four years ago, "this Court observes that their relationship with their telecommunications providers has not changed and is just as frustrating."[258] The fact that there are more calls placed today does not undermine *Smith*'s holding that there is no expectation of privacy in metadata. In addition, the judge wrote, "the effectiveness of bulk telephony metadata collection cannot be seriously disputed." He then cited three instances in which plots to bomb major sites in

[254] Klayman, 957 F. Supp. 2d at 31.
[255] *Id.* at 34.
[256] *Id.* at 39-40.
[257] ACLU v. Clapper, 959 F. Supp. 2d 724, 750-51 (S.D.N.Y. 2013).
[258] *Id.* at 752.

New York and Denmark were uncovered in their planning stages because of metadata.[259]

President Obama may have solved the immediate crisis posed by metadata collection by directing that separate phone companies maintain the data instead of the NSA and that they provide access only upon receiving a subpoena or court order.[260] This of course will impede the government, as it will take time to contact the numerous distinct phone companies and Internet Service Providers. But the real long-term concern created by the metadata dispute and associated litigation, as well as by public opinion, is the challenge to the third party doctrine.

In *Klayman*, Judge Leon essentially rejected the third party doctrine, making repeated references to the concurring opinion of Justice Sotomayor and four other justices in *United States v. Jones*, finding that, even though the target was observed by third parties, the length of the surveillance was problematic.[261] *Jones* involved lengthy surveillance of a vehicle on public roads in the District of Columbia and Maryland utilizing a government-installed GPS tracking device.[262] The government naturally responded that the vehicle was in the plain view of third parties on the highway and, in accordance with *United States v. Knotts*, there was no expectation of privacy.[263] The *Jones* Court found the tracking illegal, with four judges objecting to the violation of property rights while installing the GPS device,[264] and four others finding the length of the surveillance to be problematic.[265] Perhaps even more troubling for the government, however, was the concurring opinion of Justice Sotomayor in which she stated:

---

[259] *Id.* at 755.
[260] *See* David Jackson, *Obama unveils plan to change NSA data collection*, USA TODAY (Mar. 27, 2014), http://www.usatoday.com/story/news/nation/2014/03/27/obama-national-security-agency-edward-snowden-metadata-plam/6950657/.
[261] Klayman, 957 F. Supp. 2d at 31.
[262] United States v. Jones, 132 S. Ct. 945, 946 (2012).
[263] *Id.* at 951-52 (discussing in relevant part United States v. Knotts, 460 U.S. 276 (1983)).
[264] *Id.* at 946 (majority opinion).
[265] *Id.* at 964 (Alito, J., concurring).

> More fundamentally, it may be necessary to reconsider the premise that an individual has no expectation of privacy in information voluntarily disclosed to third parties [e.g., *Smith* and *Miller*]. This approach is ill suited to the digital age in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.[266]

As discussed in this Article, at present the government must demonstrate probable cause that a target is an agent of a foreign power before conducting FISA surveillance. The government also needs probable cause for physical searches, arrests, and indictments. Probable cause does not exist at the moment an informant advises an agent an individual is a dangerous terrorist, or when an agent observes a suspect clandestinely meet a terrorist or spy. It is generally established only after the receipt of corroborating evidence such as that contained in phone, bank, and travel records. These records are currently obtained with a Grand Jury subpoena or court order based merely on relevance to the federal investigation.[267] This lower standard exists because in the past the Supreme Court has held, in cases such as *Smith* and *Miller*, that there was no expectation of privacy in these records because of the third party doctrine. Probable cause is not needed and often is not present at this stage of an investigation.

Judge Leon's essential rejection of the third party doctrine finds support in the questions raised by Justice Sotomayor. It is also supported by the public outcry of those whose response to the Snowden revelations has been to demand probable cause before the government obtains records.[268] If this rejection of the third party doctrine were to lead to statutory or judicial requirements that the government meet a standard higher than legitimate relevance before obtaining phone, bank, travel, and other records shared with a third party, the government would often be stymied in the earliest stages of

---

[266] *Id.* at 957 (Sotomayor, J., concurring).

[267] *See* Sievert, *supra* note 19, at 336.

[268] *See* Mark K. Matthews, *Grayson wants to halt government collection of citizens' phone, Internet records*, ORLANDO SENTINEL (June 11, 2013), http://articles.orlandosentinel.com/2013-06-11/news/os-grayson-stop-snooping-20130611_1_ phone-records-grayson-nsa.

an investigation. Probable cause, as defined, seldom if ever exists in these early stages. The ability to obtain the corroborating evidence that would support a FISA order, Title III warrant, or indictment, would be foreclosed.

As has been repeatedly stated in this Article, the mandate to demonstrate probable cause before conducting electronic surveillance in intelligence cases was an unjustified overreaction to the Watergate era. A further requirement that the government show probable cause to obtain basic records from a third party would be another overreaction, which would likely eviscerate the government's ability to protect the American people.

## VII. CONCLUSION

There are countless ways FISA can be modified to enable the government to effectively monitor foreign intelligence in the United States without violating American civil liberties. Judge Posner has proposed that Congress appoint a special steering committee composed of executive branch officials and a retired federal judge to monitor surveillance.[269] Daniel Saperstein suggests greater congressional oversight through a secret commission and the creation of an Interception of Communications Commission.[270] Telford Taylor thought that the Congress and the Judiciary should not be involved at all.[271]

It is more important at this point to outline the key concepts that should form the basis of any future legislation, rather than to set forth another step-by-step proposal. First, to accommodate the demands of the executive and the civil liberties community in a realistic fashion, it will be necessary to establish a system that relies upon Congress, the Executive, and the Judiciary. Second, to insure a new law will pass constitutional muster, it must draw upon the major Supreme Court cases examined in this Article, which means it must require a judicial interception warrant of some type to guard against politically or personally motivated investigations. It must also

[269] Posner, *supra* note 149.
[270] *See* Saperstein, *supra* note 32, at 1983.
[271] *See* Taylor, *supra* note 186, at 86-87.

incorporate a standard of evidence such as reasonable or articulable suspicion that would permit a detailed search. As has been made clear, probable cause is simply not necessary in intelligence cases involving both the foreign affairs power and public safety interests, and attempting to comply with that standard has been and will continue to be detrimental to the safety of the people of the United States.

Although the author believes this reasonable suspicion standard should apply to all FISA interceptions, the most urgent need, and the one that may be most favorably considered by Congress, relates to the monitoring of Al Qaeda, ISIS (the Islamic State of Iraq and Syria, also known as "ISIL") and those who are attempting an attack with a WMD. Therefore, FISA should be changed to allow interception where there is reasonable suspicion to believe the target is a person subject to an AUMF or engaged in an effort to employ a WMD in the United States or against U.S. facilities. Harvard Law professor Jack Goldsmith argued when he was head of the Office of Legal Counsel in 2003 that both the AUMF as well as the concept of special needs should permit the President to monitor Al Qaeda without going through the traditional requirements of the FISA statute.[272] His argument was later supported by the wording of *Hamdi v. Rumsfeld*, stating that the AUMF allowed the President to utilize all necessary elements of military force against Al Qaeda and the Taliban.[273] Surely, monitoring the enemy is one such element of military force. Goldsmith's position is strongly opposed by those who state that FISA requires the President to follow the procedures established by Congress and not act without FISA court approval.[274] But as*suming*

[272] The memo, which is heavily redacted, was released on Sept. 7, 2014. Memorandum for the Attorney Gen. Re: STELLAR WIND – Implications of Hamdi v. Rumsfeld by Jack Goldsmith (July 16, 2004); see Matt Danzer, *The Legal Justifications for Domestic Surveillance: A Summary*, LAWFARE (Sept. 11, 2014, 7:00 PM), http://www.lawfareblog.com/2014/09/the-legal-justifications-for-domestic-surveillance-a-summary/ for a summary of the original memo.

[273] Hamdi v. Rumsfeld, 542 U.S. 507, 518 (2004).

[274] *See, e.g.*, Geoffrey Stone, *Bush's Spy Program and FISA*, THE UNIV. OF CHICAGO LAW SCH. FACULTY BLOG (Jan. 4, 2006), http://uchicagolaw.typepad.com/faculty/2006/01/bushs_spy_progr_1.html; see Jeremy Neff, *Does (FISA + NSA)* AUMF = Illegal Domestic Spying?*, 75 U. CIN. L. REV. 887, 889-90 (2006).

*Congress can intrude on the President's authority in this area, there is nothing preventing Congress* from amending the FISA statute to provide for more efficient interception when the target is the subject of an AUMF or planning a WMD attack.

Abandoning probable cause would certainly raise legal concerns similar to those expressed in *United States v. Truong*[275] and by the petitioners in *In Re Sealed Case*,[276] if the intent and direct result was ordinary criminal prosecution as opposed to intelligence collection. At the same time, an interception intended to obtain intelligence is likely to pick up evidence of national security crimes (sabotage, terrorism, espionage). The government should be able to use this evidence under the doctrine that the government can use anything it finds while it is legally present.[277] The solution in part would be to draw upon the 2001 FISA Court's practice and prohibit criminal division direction and control of intelligence wiretaps. In addition, as Judge Posner has suggested, "the use of intercepted information for any other purpose other than investigating (or prosecuting) threats to national security would be forbidden. Information could not be used as evidence or leads in the prosecution of ordinary crime."[278] Finally, if the government thought it was likely to uncover criminal acts other than national security crimes, it would be wise in those few cases to go the extra step and seek to demonstrate probable cause instead of reasonable suspicion before obtaining a judicial warrant.

Any public fears regarding the creation of a new FISA could be assuaged by establishing an independent body to look after the concerns of the civilian community. We have seen such entities in

---

[275] United States v. Truong, 629 F.2d 908, 913-14 (4th Cir. 1980).
[276] *In re* Sealed Case, 310 F.3d 717, 721-22 (FISA Ct. Rev. 2002).
[277] This type of action falls under a doctrine known as the "plain view doctrine." *See* Washington v. Chrisman, 455 U.S. 1, 2 (1982); Harris v. United States, 390 U.S. 234, 236 (1968); *see also* United States v. Kahn, 415 U.S. 143, 157 (1974); United Stated v. Schwartz, 535 F.2d 160, 163 (2d Cir. 1976).
[278] Posner, *supra* note 158, at 258; *see* William Pollak, *Shu'ubiyya or Security? Preserving Civil Liberties by Limiting FISA Evidence to National Security Prosecutions*, 42 U. MICH. J. L. REFORM 221 (2008) (arguing for a test whereby ordinary crime could only be prosecuted when uncovered by a FISA if it is "inextricably intertwined" with a national security offense).

Germany's G-10 committee, the U.K.'s Interception of Communications Commission, and Italy's Data Protection Authority. These organizations perform a variety of roles, from reviewing all surveillance after the fact to issuing reports to the legislature, or, in some cases, examining individual allegations of excessive surveillance. An American version of this independent body would exist alongside the judiciary, which would grant the initial interception warrant based on a finding of reasonable suspicion.

Any objective individual who steps back and reviews the series of attempted attacks on the United States in the last fifteen years understands our population is in great danger, and this is especially so if our adversaries obtain some type of WMD. It is folly to hamstring our intelligence services by imposing a criminal law search standard that is neither constitutionally required nor mandated by the recognized human rights principles of the international community. It is imperative, therefore, that we correct the mistakes of the past and enact a new, more effective Foreign Intelligence Surveillance Act.