A CONTAGION OF FEAR: POST-9/11 ALARM EXPANDS EXECUTIVE BRANCH AUTHORITY AND SANCTIONS PROSECUTORIAL EXPLOITATION OF AMERICA’S PRIVACY

Carol M. Bast*† and Cynthia A. Brown**

INTRODUCTION ........................................................................................................ 362
I. FOREIGN INTELLIGENCE SURVEILLANCE ACT ............................................. 366
   A. Congressional Review of Executive Branch Surveillance: The Church Committee ................................................................. 366
   B. Congress enacts FISA .................................................................................. 368
   C. Smith v. Maryland and third party doctrine .............................................. 372
   D. The USA PATRIOT Act and Recent Amendments to FISA ......... 374
II. THE JUDICIARY’S ACQUIESCENCE TO EXECUTIVE BRANCH AUTHORITY PRIOR TO 2013 ......................................................... 377
   A. The United States Supreme Court ............................................................. 377
   B. FISA Courts ................................................................................................. 378
   C. Other Federal Courts .................................................................................. 381
      i. Mayfield v. United States ........................................................................ 381
      ii. Al-Haramain ......................................................................................... 385
III. PRESENT STATE OF DOMESTIC SURVEILLANCE ...................................... 391
   A. The Terrorist Surveillance Program .......................................................... 393
   B. The Protect America Act ........................................................................... 396
   C. Snowden Disclosures of 2013 ................................................................. 397
   D. The Judicial Branch since the Snowden Disclosures ....................... 398
      i. FISA Courts ......................................................................................... 398
      ii. Other Federal Courts ......................................................................... 401
IV. THE FEDERAL PROSECUTOR ........................................................................ 406
   A. The Prosecutor: Power and Duty .............................................................. 406
   B. The Prosecutor and Legal Ethics ............................................................... 410
V. ANALYSIS ....................................................................................................... 414
   A. Overcriminalization .................................................................................. 417

* Associate Professor of Legal Studies, Department of Criminal Justice and Legal Studies, University of Central Florida, Orlando, Florida 32816.
† These authors contributed equally to this work.
** Cynthia A. Brown, J.D., Ph.D., is in an attorney in private practice with the law firm of Brown and Associates, PLLC.
INTRODUCTION

Following the attacks on September 11, 2001, the United States launched the War on Terror as the action has become known. According to the Bush Administration, the phrase encompassed the nation’s military, political, legal and ideological conflict with Islamic extremism and extremists’ use of terrorism to propel their agenda. Ironically, Al-Qaeda’s weapon, the use of fear as a means of coercion, in some respects now serves dually as a tool for our nation’s leaders. The influence of fear has arguably become a favorite tool of government leaders to coax an ever expanding swath of authority at the expense of individual liberties. In essence, the fear created by the terrorists is the genesis of a contagion of fear with the accompanying contagion-like effects. The influence of that fear, particularly of further terrorist attacks, makes many Americans quick to support and loath to criticize any government action that combats this threat and ensures national security.

America’s administrative response is not unlike that of the nation and presents a pattern characterized by a significant shift in the equilibrium of power among the three branches of government. This shift creates an imbalance that favors the executive and disadvantages the condition of the state. Acting, in part, to forestall future harm, the executive branch sought to broaden its authority and persuaded its sister branches to abbreviate, or forego altogether, required procedures at the expense of principles essential to liberal democracy. Legislative representatives who do not want to be seen as soft on terror acquiesce to the

1 President George W. Bush, Address to a Joint Session of Congress (Sept. 20, 2001), available at http://middleeast.about.com/od/usmideastpolicy/a/bush-war-on-terror-speech.htm. See also infra notes 434, 437 infra and accompanying text.


In effect, modern presidents have given themselves additional constitutional tools to reinforce themselves against political accountability and legal scrutiny. These tools are designed to protect U.S. interests by ensuring information security and secrecy, but they also greatly increase executive power and provide new avenues for presidents and executive branch officials to circumvent Congress and the courts.

Id.
executive’s requests. The third branch, the judiciary, finds it is restricted by both constitutional structure and cultural norms that hamper any far-reaching check on the executive. In turn, the executive branch too often capitalizes on the moral outrage and emotional fervor of a nation fearful of continued acts of terrorism. This allows the executive to accomplish what typically would be improbable in a country that historically favors the constitutional protections of individual rights from government power.

Fear serves the executive branch providing both the justification and the instrumentality needed to secure the objective of expanded authority. Terrorist incidents, then, supply a tool enabling the executive to pursue agendas that reach far beyond any immediate threat. After experiencing the increased power and authority of the newly enacted counterterrorist measures, few are eager to relinquish those powers. Such heightened powers might be used in other areas of government administration, with executive agencies finding it easy to rationalize the mission creep, for instance, in law enforcement efforts to reduce other crimes.

Professor Stuntz suggests that these increases in the executive’s legal authority, particularly in the area of searches and seizures, can be separated into two categories: special but limited powers exclusive to the fight against terrorism, and changes in enforcement authority applicable across the board. While the former is the product of congressional authorization through legislative enactments applicable to terrorism-related offenses, the latter is more likely to be the product of the federal bench and its resulting judicial decisions, application of which will not be restricted to a particular type of crime. Courts, however, will be called upon to assess the constitutionality of both the statutory provisions authorizing additional power and the exercise of those powers.

In the aftermath of September 11, this contagion of fear stimulated the public support needed by government officials to expand government surveillance under amendments to the Foreign Intelligence Surveillance Act (FISA). It seems that individuals are willing to cede communication privacy to the government in exchange for national se-

---

4 Id. at 2138-39.
5 Id. at 2139.
curity without realizing the ramifications of their actions. Federal prosecutors have joined the frenzy and are exploiting FISA surveillance to exponentially increase conviction rates in lieu of a search for truth. Cloaked beneath a virtually impenetrable shield of state secrets and national security, prosecutors may be able to avoid Fourth Amendment restrictions and procedural disclosure requirements by stretching FISA and its implementation.

Because of national security concerns, the extent of government wiretapping to investigate alleged terrorists is largely shrouded in secrecy; however, wiretaps were used in 2004 both to name Al-Haramain Islamic Foundation, Inc., an Oregon nonprofit corporation, as a specially designated global terrorist and to arrest an Oregon Muslim as a material witness in connection with the Madrid subway bombings. Wiretaps may have been used in May of 2010 to arrest the Muslim allegedly responsible for the May 1, 2010 bomb scare in Times Square.

On March 11, 2004, terrorists exploded bombs in commuter subway cars in Madrid, Spain, killing 191 and injuring nearly 1,600. On May 6, 2004, the FBI arrested Brandon Mayfield, a Muslim, in Oregon as a material witness because his fingerprints allegedly matched a fingerprint from a plastic bag containing detonation materials that the Spanish National Police had connected to the bombing. The arrest warrant was based at least in part on information obtained through a Foreign Intelligence Surveillance Act wiretap.

On May 3, 2010, Faisal Shahzad was arrested for allegedly planting a bomb in his parked car in a failed attempt to blow up the Times Square area in New York city. His arrest as he boarded an airplane at JFK airport came a mere fifty-three hours after discovery of the bomb and his identification as an alleged terrorist. The detailed information available on Shahzad's terrorist leanings in such close proximity to his arrest caused at least one newspaper to speculate that the information may have been gathered through a Foreign Intelligence Surveillance Act wiretap.

---

7 See also infra notes 14, 109, 149-204, 211-12, 407, infra and accompanying text.
8 See also infra notes 10-12, 17, 75-79, 108, 110-48, infra and accompanying text.
9 See also infra note 13, infra and accompanying text.
12 Mayfield v. United States, 588 F.3d 1252, 1255 (9th Cir. 2009).
13 Surveillance and Shahzad: Are wiretap limits making it harder to discover and pre-empt jihadists?
At this point, a reader only tangentially concerned with criminal law may assume no personal connection with FISA or terrorist activity. After all, why would the average reader be concerned with the vast discretion afforded the prosecutor to charge a suspected terrorist based on evidence obtained through a government wiretap? One’s perspective may change upon learning additional information on the 2004 wiretaps briefly referenced above. In March and April of 2004, the National Security Agency allegedly wiretapped conversations of Wendell Belew and Asim Ghafoor, two attorneys representing Al-Haramain, without obtaining a FISA court order. The two attorneys might never have known that consultations with their client were secretly wiretapped but for the government’s mistake of turning over the top secret log to another attorney representing Al-Haramain.Brandon Mayfield, also an attorney, was subjected to extensive surveillance and was held in jail for more than two weeks even though Spanish authorities disagreed with the FBI’s conclusion that Mayfield’s fingerprints matched the fingerprint related to the Madrid bombings.

This paper examines how the weapon of fear in the hands of America’s leaders delivers prosecutors a tempting license to convict at any cost — including the loss of individual freedoms that have until recently been the very foundation of this country. The manuscript considers how congressional authorization through legislative enactments, such as the USA PATRIOT Act and amendments to FISA, are part of the contagion of fear. The results facilitate expanded executive power and allow prosecutors to reap the political benefits of increased convictions through legislative mission creep — charging violations beyond the boundaries of terrorism-related atrocities and into the realm of ordinary, everyday crimes. Increased executive authority at the expense of individual rights and the contagion of fear provide tempting opportunities for prosecutors as the line between the search for truth and win at all costs disappears.

The contagion of fear, the expanded scope of FISA, and over-criminalization provide the prosecutor almost unlimited discretion. FISA wiretaps are a necessary tool in the prosecution’s arsenal, espe-


14 See also infra notes 109, 149-204, 211-12, 407, and accompanying text.

15 See also infra notes 17, 75-79, 108, 110-48, and accompanying text.
cially if, as suspected, they led to the detention of Shahzad. However, identifying Mayfield as a terrorist was an unfortunate “false positive,” with the inappropriateness of the government’s continued pursuit of Mayfield as a suspect indicated in part by the government settling Mayfield’s civil suit against the government for two million dollars.

The purpose of this paper is to examine how the prosecutor’s discretion should be channeled so as to separate a Shahzad from a Mayfield. Part II presents the FISA legislation. Part III inventories the judiciary’s response prior to 2013 to increased executive power and a nearly unrestricted stamp of approval by the judiciary branch, essentially eliminating the checks and balances so well-designed by our country’s founders. Part IV considers how 9/11 and its aftermath have systematically increased the executive’s law enforcement authority. Part V reviews the power of the federal prosecutor who has the means to avoid constitutional limitations, effectively waiving individual rights when any domestic activity is prosecuted in the War on Terror. Part VI provides an analysis of overcriminalization related to the War on Terror prosecutions.

I. FOREIGN INTELLIGENCE SURVEILLANCE ACT

A. Congressional Review of Executive Branch Surveillance: The Church Committee

The Nixon administration surveillance activities provided the impetus for Congress establishing the Church Committee in 1975. The committee was named after its chair, Senator Frank Church, and was charged with investigating the executive branch’s inappropriate use of electronic surveillance. In a multi-volume report, the committee documented the startling quantity of surreptitious wiretapping of Americans with no apparent connection to foreign intelligence information, with the surveillance performed without the benefit of prior judicial


17 See also infra notes 75-79, 108, 110-48, and accompanying text.

The stated reason for the surveillance by a number of government agencies, including the Federal Bureau of Investigation ("FBI") and the National Security Agency ("NSA"), was that the targets posed a danger to national security; however, the facts showed that the individuals were chosen as targets because of their membership in groups at odds with the executive branch rather than being chosen because of any actual danger to national security. To illustrate, individuals whose communication was intercepted included "political adherents of the right and the left, ranging from activist to casual supporters. The report found that investigations had been directed against proponents of racial causes and women's rights, outspoken apostles of nonviolence and racial harmony; establishment politicians; religious groups; and advocates of new lifestyles." Dr. Martin Luther King, Jr. and other civil rights advocates were under surveillance because they were voicing public concern but were unaligned with the executive branch. Without regard for constitutional or other legal limitations on executive branch power, the FBI opened sixty-five thousand domestic intelligence investigations in a single year.

Thus, the executive branch took it upon itself, with no prior judicial approval, the surveillance of countless individuals, many of whom showed no sign of any connection to any illegal act. The Church Committee reported "[g]overnment officials—including those whose principal duty is to enforce the law—have violated or ignored the law over long periods of time and have advocated and defended their right to break the law." The report included the following damning summary:

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

The Church Committee Report had a huge impact on public opinion, especially so closely following the revelation of executive branch surreptitious surveillance of domestic organizations.\(^{26}\) Congress decided that the time had come to curb executive branch surveillance practices in the domestic sphere and implement Church Committee Report recommendations by passing legislation designed to place checks and balances on executive branch domestic surveillance. "By enacting the Foreign Intelligence Act of 1978 [FISA], Congress provided the 'exclusive means' by which the President could authorize electronic surveillance within the United States,"\(^ {27}\) while recognizing the President's authority in matters of national security. The three purposes of the legislation were to:\(^ {28}\) (1) "impose[] accountability standards on domestic surveillance" by requiring "safeguards against [executive branch] abuse";\(^ {29}\) (2) "limit[] the authorized targets of surveillance to foreign powers and their agents" to narrow "surveillance of domestic groups" to "normal means applicable to domestic criminal investigations";\(^ {30}\) and (3) "require[] judicial review and approval of applications for FISA surveillance" and periodic reporting to Congress.\(^ {31}\)

While placing limits on executive branch surveillance, FISA standards allow

1. deliberate interception\(^ {32}\) of the contents of international radio or wire communications to or from a particular United States person in the United States in circumstances where that person has a reasonable expectation of privacy and a warrant would be required in the interception were undertaken for law enforcement purposes;
2. deliberate interception of the contents of a wholly domestic radio communication, and the installation or use of any monitoring device (such as a television camera or pen register) to ac-


\(^{28}\) Howell & Lesemann, supra note 26, at 149-50.

\(^{29}\) Id. at 149; FISA, 50 U.S.C. §§ 1802, 1822 (2000).


\(^ {32}\) Interception is defined as "the aural or other acquisition of the contents" of various kinds of communications by means of "electronic, mechanical or other device." 18 U.S.C.A. 2510(4) (West, Westlaw through Pub L. No. 113-74).
quire information about a person’s activities other than the contents of communications, when there is a reasonable expectation of privacy and a warrant would be required if the interception or monitoring were undertaken for law enforcement purposes; [and]

(3) interception in the United States of the contents of a wire communication to or from any person in the United States without the consent of a party to the communication.33

Congress cut the new FISA process for the government to conduct electronic surveillance out of whole cloth. FISA contains “a procedure under which the Attorney General can obtain a judicial warrant authorizing the use of electronic surveillance in the United States for foreign intelligence purposes.”34 FISA allows the executive branch to conduct surveillance of the communication of foreign powers;35 however, the executive branch must have a wiretapping court order rather than a warrant prior to domestic surveillance of Americans.36 To guard against FISA being used to investigate criminal activity rather than foreign intelligence, thus safeguarding the separation between foreign intelligence surveillance and law enforcement surveillance, the Attorney General must approve that “the purpose” of a proposed FISA surveillance was “to obtain foreign intelligence information.”37

FISA court orders must come from the Federal Intelligence Sur-

37 FISA, 50 U.S.C.A. §§ 1804(a)(6)(B) (formerly 1804(a)(7)(B)) (addressing electronic surveillance), 1823(a)(6)(B) (formerly 1823(a)(7)(B) (addressing physical evidence) (West, Westlaw through P.L. 113-74). The 2001 amendment to these sub-subsections reworded “the purpose” as “the significant purpose.”
veillance Court ("FISC"),\textsuperscript{38} a FISA-created court; the sole power of FISC is "to hear applications for and grant orders approving electronic surveillance anywhere within the United States."	extsuperscript{39} The Chief Justice of the United States Supreme Court appoints the eleven members of FISC, each of whom serves a non-renewable seven-year term.\textsuperscript{40} The denial of a FISA application would go to the Foreign Intelligence Surveillance Court of Review ("FISCR"), a court comprised of three federal judges designated by the Chief Justice of the United States Supreme Court.\textsuperscript{41} To date, FISCR has handled a single appeal.\textsuperscript{42} FISC hearings and FISCR appeals are conducted ex parte and proceedings are otherwise closed to the public.\textsuperscript{43}

A FISA application must contain a number of pieces of information. The application must contain "the identity, if known, or a description of the specific target of the electronic surveillance,"\textsuperscript{44} and "a statement of the facts and circumstances relied upon by the applicant" both that (1) "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and (2) "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power."\textsuperscript{45} The application must include "a statement of the proposed minimization procedures" "which shall be adopted by the Attorney General" "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information" other than foreign intelligence information.\textsuperscript{46} The applicant must certify (1) that "the information sought [is] foreign intelligence information"; (2) "that a significant purpose of the surveillance is to obtain foreign intelligence information"; and (3) "that such information cannot reasonably be obtained by nor-

\textsuperscript{38} Id. § 1803(a), (b). Wiretapping generally requires the applicant to first obtain a court order allowing the wiretapping. An exception to requiring a court order allows wiretapping in an emergency so long as the wiretapping application is filed within seven days. Id. § 1805(e).

\textsuperscript{39} Id. § 1803(a).

\textsuperscript{40} Id. § 1803(a), (d). Originally seven judges made up FISC, but the number was increased to eleven to handle the workload. FISC is considered an Article III court because each of its members is a United States district judge.

\textsuperscript{41} Id. § 1803(b).

\textsuperscript{42} In re Sealed Case, 310 F.3d 717 (FISA Ct. Rev. 2002).

\textsuperscript{43} 50 U.S.C.A. § 1803(c) (West, Westlaw through P.L. 113-74).

\textsuperscript{44} Id. § 1804(a)(2).

\textsuperscript{45} Id. § 1804(a)(3).

\textsuperscript{46} Id. §§ 1801(h)(1), 1804(a)(4).
mal investigative techniques."

Once presented with a FISA application, the two crucial inquiries the judge must make are that "there is probable cause to believe that" (1) "the target of the electronic surveillance is a foreign power or an agent of a foreign power"; and (2) "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." In reviewing the probable cause findings required to be made by the judge, one notes that the judge is not required to make a probable cause determination of wrongdoing as required under the Fourth Amendment, but a probable cause determination that the target may be a foreign power or the agent of a foreign power who uses or will use the target location. This disparity between the higher level of proof required by the Fourth Amendment probable cause standard and the lower level of proof required by the FISA foreign intelligence information probable cause standard is significant and, in fact, quite startling.

Unless the surveillance target is a United States person, the FISC judge is without authority to examine whether the information sought is foreign intelligence information. If the surveillance target is a United States person, the judge can determine whether the government’s certification is clearly erroneous.

A FISA court order may last up to ninety days if the target is an agent of a foreign power, or up to one hundred twenty days if the target is an agent of a foreign power but not a United States person, or up to

---

47 50 U.S.C.A. § 1804(a)(6) (West, Westlaw through P.L. 113-74). The 2001 amendment to this sub-subsection reworded "the purpose" as "the significant purpose."
48 Id. § 1805(a)(2).
49 Id. § 1801(c). Under FISA, "foreign intelligence information" is that which the government needs to deal with to protect the country against offensive actions by a foreign power or its agent such as "attack," "sabotage," or "clandestine intelligence activities." Id. Under FISA, a foreign power includes "a foreign government," "a faction of a foreign nation or nations, not substantially composed of United States persons," "an entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments," "a group engaged in international terrorism or activities in preparation therefor," "a foreign-based political organization, not substantially composed of United States persons," "an entity that is directed and controlled by a foreign government or governments," and "an entity not substantially composed of United States persons that is engaged in the international proliferation of weapons of mass destruction." Id. Under FISA, a United States person is either a United States citizen or a resident alien. See id. § 1801(f). FISA distinguishes between a United States person and one not falling within that category in many provisions, typically favoring one in the first rather than in the second category.
50 Id. § 1805(a)(4).
a year if the target is a foreign power. In contrast to the federal wire-tapping statutes, the FISA target may never learn that the target was subject to surveillance because FISA generally has no requirement that the target be notified of the surveillance. An exception requiring notification to the target is if the government intends to use any of the FISA-derived wiretap information as evidence in court or agency proceeding, in which case notification is required.

FISA requires the Attorney General to furnish reports to Congress and the judiciary, with the reports designed to provide information on the electronic surveillance accomplished by the executive branch under FISA. Each year in April the Attorney General reports to the Administrative Office of the United States Courts and to Congress the number of applications and extensions requested for FISA court orders and the "total number of such orders and extensions either granted, modified, or denied." FISA requires the Attorney General to report certain additional information to certain Congressional committees twice a year. This information includes (1) "the total number of applications made for orders and extensions of orders approving electronic surveillance under this subchapter where the nature and location of each facility or place at which the electronic surveillance will be directed is unknown"; (2) "each criminal case in which information acquired under this chapter has been authorized for use at trial during the period covered by such report"; and (3) "the total number of emergency employments of electronic surveillance . . . and the total number of subsequent orders approving or denying such electronic surveillance."

C. Smith v. Maryland and third party doctrine

The 1979 United States Supreme Court opinion, Smith v. Maryland, is one of the cases that established the third party doctrine, a

---

51 Id. § 1805(d)(1).
52 Id. § 1806(c).
53 Id. Congress expanded permissible FISA surveillance to physical searches in 1994. Id. §§ 1821-1829.
55 50 U.S.C.A. § 1808 (West, Westlaw through P.L. 113-74). Other reports are required to be provided to certain members of Congress. Id. §§ 1802(a)(1),(2), 1826, 1846, 1862, 1871, 1881f, 1885c.
56 442 U.S. 735 (1979). In this robbery case, the victim, Patricia McDonough, alleged that a man took her pocketbook; she provided the police with a description of both the robber and
doctrine instrumental in interpreting FISA. In Smith, the police asked the telephone company to install a pen register, which recorded the numbers dialed, on the home telephone of Smith, the alleged robber. The police obtained a warrant to search Smith’s home after the pen register showed that a call was made from Smith’s home to the victim’s home. After the search turned up incriminating evidence, Smith was arrested for robbery. Smith filed a motion to suppress the evidence derived from the pen register because the pen register had been installed without a warrant. The Maryland state trial court denied the motion to suppress and Smith was convicted. The highest court in Maryland, the Maryland Court of Appeals, affirmed.

A vigorous dissent to the Maryland Court of Appeals opinion reminded the reader of the temptation a powerful tool such as the pen register could pose in the hands of law enforcement:

The majority fails to give due weight to the impact of Watergate and its progeny, the recent revelations of illicit surveillance conducted by the F.B.I. upon activities of various civil rights, labor and political leaders, or indeed, the potential abuse to which the pen register may be put by police authorities. These factors and others have created an environment of distrust, fear and lack of confidence.

In the United States Supreme Court, the Court found that, even if Smith had an expectation of privacy because he dialed the telephone numbers in his own home, this expectation was not reasonable. The Court reminded the reader, “This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.” The Court reasoned, “When he used his phone, [Smith] voluntarily conveyed numerical information to the telephone company and ‘exposed’ that information to its equipment in the ordinary course of business. In so doing, [Smith] assumed the

---

57 Id. at 743-44.
58 Id. at 737.
59 Id. at 737-38.
61 442 U.S. at 743-44.
risk that the company would reveal to police the numbers he dialed.\footnote{Id. at 744.} The Court affirmed the Maryland Court of Appeals decision, stating that, because there was no search conducted by use of the pen register, the police did not need a warrant to make the request from the telephone company.\footnote{Id. at 745-46.}

There were two vigorous dissenting opinions to the United States Supreme Court decision. In his dissent in \textit{Smith}, Justice Stewart pointed out the intrusive nature of a study of pen register information and what it had the potential to reveal:

\begin{quote}
I doubt there are any who would be happy to have broadcast to the world a list of the local or long distance numbers they have called. This is not because such a list might in some sense be incriminating, but because it easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life.\footnote{Id. at 748 (Stewart, J., dissenting).}
\end{quote}

Justice Marshall's voiced the same concern but in a harsher tone of voice:

\begin{quote}
The prospect of unregulated governmental monitoring will undoubtedly prove disturbing even to those with nothing illicit to hide. Many individuals, including members of unpopular political organizations or journalists with confidential sources, may legitimately wish to avoid disclosure of their personal contacts. Permitting governmental access to telephone records on less than probable cause may thus impede certain forms of political affiliation and journalistic endeavor that are the hallmark of a truly free society. Particularly given the Government's previous reliance on warrantless telephonic surveillance to trace reporters' sources and monitor protected political activity, I am unwilling to insulate use of pen registers from independent judicial review.\footnote{Id. at 751 (Marshall, J., dissenting) (citations omitted) (footnote omitted).}
\end{quote}

D. \textit{The USA PATRIOT Act and Recent Amendments to FISA}

The circumstances of the crashes of the four airplanes in the horrible September 11, 2001 terrorist attacks are well known worldwide. In the United States, the fear generated by such terrorist incidents with-
in the continental United States motivated Congress to prevent future attacks by passing the "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism" Act (the USA PATRIOT Act, hereafter the "Patriot Act"). The purpose of the legislation, passed just forty-five days after the attacks, was to "provide . . . enhanced investigative tools and improve . . . information sharing for the law enforcement and intelligence communities to combat terrorism." The Patriot Act provides new tools to the executive branch, including roving wiretaps, internet communication and use tracking, "sneak-and-peak" searches, and business record searches. The forced separation formerly existing between law enforcement and intelligence agencies was done away with and the Patriot Act encouraged information transfer among those agencies.

The ten sections of the Patriot Act contain amendments to FISA and an Enhanced Surveillance Procedures section. For the most part, the Patriot Act consists of revisions to already-enacted statutes.

The revisions to FISA made by the Patriot Act are significant in two respects. The first significant amendment changed the previous requirement that gathering foreign intelligence be "the purpose" for executive branch surveillance to the requirement that gathering foreign intelligence be "a significant purpose" of the surveillance. Thus, this wording lowered the threshold for permissible surveillance, allowing surveillance by the executive branch when there was some other reason for the surveillance other than gathering foreign intelligence. The second significant amendment, the "coordination amendment," permits federal law enforcement and intelligence agencies performing surveil-

---

68 Id. § 206 (roving surveillance authority); see also § 217 (interception of computer trespasser communications); § 213 ("sneak-and-peak" warrants) and § 215 (business searches). Several Patriot Act provisions, including Section 215, were originally scheduled to sunset on Dec. 31, 2005. On Mar. 9, 2006, President Bush signed into law the Reauthorization Act, extending several provisions, of which Section 215 was one.
69 Id. § 504. See infra notes 74, 80, 91-105 and accompanying text.
70 Id. §§ 216-218 at 278-96.
73 USA PATRIOT Act § 218 (codified as amended at 50 U.S.C.A. §§ 1804(a)(7)(B), 1823(a)(7)(B) (West, Westlaw through P.L. 113-74)).
lance under FISA to coordinate their efforts to gather foreign intelligence information in the course of investigating certain criminal activity.\textsuperscript{74}

Attorney Brandon Mayfield's case against the United States alleging a Fourth Amendment violation based on government surveillance is an example of the intrusive use of FISA surveillance.\textsuperscript{75} Mayfield became a terrorist suspect after the 2004 explosions on commuter trains in Madrid, Spain.\textsuperscript{76} The executive branch obtained a FISA warrant to perform electronic surveillance of Mayfield's law practice and home activities as well as searches of his law office and his home even though there was evidence that the United States was targeting the wrong individual.\textsuperscript{77} Although the United States claimed that Mayfield's fingerprint matched a print on evidence recovered in connection with the bombing, the Spanish authorities disagreed with the purported match of Mayfield's fingerprint to the evidence and instead had identified persons from north Africa as suspects. Mayfield had last traveled out of the United States in the 1990s when serving in Germany as a United States Army lieutenant and his passport had since expired. There was

\textsuperscript{74} Id. § 504 (codified as amended at 50 U.S.C.A. § 1806 (West, Westlaw through P.L. 113-74)). This amendment did not replace any prior FISA language, but added "the coordination with law enforcement" section:

\begin{quote}
(k)(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate and protect against —

(A) actual or potential attack or other grave hostile acts of a foreign power or agent of a foreign power;

(B) sabotage or international terrorism by a foreign power or agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
\end{quote}

\textsuperscript{Id.}

\textsuperscript{75} Mayfield v. United States, 504 F. Supp. 2d 1023 (D. Or. 2007), vacated, 599 F.3d 964, 966 (9th Cir. 2010) (finding Mayfield "does not have standing to pursue his Fourth Amendment claim because his injuries already have been substantially redressed by the Settlement Agreement, and a declaratory judgment would not likely impact him or his family"). The trial court judge reached a much different decision than other courts to have considered the constitutionality of FISA. The judge found that sections 1804 and 1823 of FISA (as amended by the Patriot Act) are unconstitutional under the Fourth Amendment. See 504 F. Supp. 2d 1023 at 1042-43; see infra note 79 at 110-48 and accompanying text.

\textsuperscript{76} 504 F. Supp. 2d at 1026-27.

\textsuperscript{77} Id. at 1033-34.
no evidence of any connection between Spain and Mayfield, his law practice, or his family.\textsuperscript{78} The United States settled Mayfield's claims and made a hefty two million dollar payment, with the settlement exonerating him.\textsuperscript{79}

II. \textsc{The Judiciary's Acquiescence to Executive Branch Authority Prior to 2013}

Since 9/11, the judicial branch has had opportunities to consider the executive's expansion of power; however, prior to the Snowden disclosures of 2013, the judiciary had for the most part refrained from placing meaningful restrictions on the executive branch. Seemingly influenced by the perception of emergency created by the 9/11 attacks and the fact that terrorism has moved to the center of the national agenda, the judicial branch has resisted statutory interpretations that limit the administration's law enforcement capabilities. Decisions before the U.S. Supreme Court have not yet resulted in an interpretation of the constitutionality of the increased executive branch authority granted by FISA's amendments. An epic decision by the FISA appellate court, however, practically removes any check on the President's exercise of power under FISA.\textsuperscript{80}

A. \textsc{The United States Supreme Court}

Explicit responses from the United States Supreme Court on the War on Terror are found in six cases: \textit{Clapper v. Amnesty International USA},\textsuperscript{81} \textit{Holder v. Humanitarian Law Project},\textsuperscript{82} \textit{Hamdi v. Rumsfeld},\textsuperscript{83} \textit{Rasul v. Bush},\textsuperscript{84} \textit{Rumsfeld v. Padilla},\textsuperscript{85} and \textit{Hamdan v. Rumsfeld}.\textsuperscript{86} While none of these six decisions directly addresses FISA and surreptitious surveillance of Americans on the merits, the sum total of the Court's decisions cannot be counted as a victory for civil liberties over government power. The most recent decision challenged NSA telecommunications sur-

\textsuperscript{78} \textit{Id.} at 1033.
\textsuperscript{79} \textit{Mayfield v. United States}, 599 F.3d 964, 968 (9th Cir. 2010).
\textsuperscript{80} \textit{In re Sealed Case}, 310 F.3d 717 (FISA Ct. Rev. 2002).
\textsuperscript{81} 133 S. Ct. 1138 (2013).
\textsuperscript{82} 130 S. Ct. 2705 (2010).
\textsuperscript{83} 542 U.S. 507 (2004).
\textsuperscript{84} 542 U.S. 466 (2004).
\textsuperscript{85} 542 U.S. 426 (2004).
\textsuperscript{86} 548 U.S. 557 (2006).
veillance but the Court held that those allegedly being surveilled lacked Article III standing. The next to the most recent decision considered the constitutionality of a federal criminal statute prohibiting certain types of support to terrorist organizations as designated by the Secretary of State. The other four decisions address detainment and interrogation processes and provide considerable room for executive action and "relatively little space for the assertion of rights by citizens suspected of being enemy combatants."  

Clapper may or may not have been decided differently, had it reached the Court following the 2013 disclosures as the respondents' argument that their communications had been intercepted would have been more concrete with the Snowden revelations. Even though some Court watchers have speculated that the Court may reconsider the issue presented in Clapper, the Court thus far has refrained from doing so.

B. FISA Courts

The Patriot Act amended FISA to allow "a significant purpose" of surveillance to be to collect foreign intelligence rather than requiring collection of foreign intelligence to be "the purpose" of surveillance. In a March 6, 2002 memorandum, Attorney General Ashcroft approved Intelligence Sharing Procedures designed to implement his interpretation of the Patriot Act amendments. Attorney General Ashcroft interpreted this Patriot Act amendment to allow surveillance primarily to conduct criminal investigation so long as obtaining foreign intelligence was still a significant purpose of the surveillance. In addition, he interpreted the amendment to allow full consultation and cooperation between intelligence officers conducting FISA surveillance and law enforcement officers conducting criminal investigations. These interpretations served to demolish the "wall" between surveil-

---

87 133 S. Ct. 1138, 1142-3 (2013).
88 130 S. Ct. 2705, 2712 (2010).
92 Id.
93 Id.
lance to collect foreign intelligence and criminal investigation as originally contemplated by Congress under FISA.

Attorney General Ashcroft notified FISC of the new Procedures in May 2002 and requested an order from the court vacating its prior orders in conflict with the Procedures, thus eliminating the wall between foreign intelligence collection and criminal investigation. In its order in response to Ashcroft’s request and its first-ever-published opinion, FISC rejected Ashcroft’s interpretations of the Patriot Act amendments to FISA. In the opinion, FISC referenced the government’s September 2000 confession of the inclusion of “misstatements and omissions of material facts” in approximately seventy-five FISA applications. The court voiced its concern with the government’s attempt to break down the wall between collection of foreign intelligence and criminal investigations in that:

> criminal prosecutors will tell the FBI when to use FISA (perhaps when they lack probable cause for a Title III electronic surveillance), what techniques to use, what information to look for, what information to keep as evidence, and when use of FISA can cease because there is enough evidence to arrest and prosecute. Such measures did not appear to be reasonably designed “to obtain, produce, or disseminate foreign intelligence information.”

The court saw Ashcroft’s proposed Procedures as a government attempt to substitute FISA for Title III electronic surveillances and Rule 41 searches.

It was not surprising that the government appealed its loss, especially because this was the first instance in which FISC had not acquiesced to a government request. In the first ever appeal to FISCR, FISCR reversed the FISC decision. The court found that FISA, as originally passed, did not outlaw the use of foreign intelligence collected

---

95 Id. at 626-27.
96 Id. at 620.
97 Id. at 624.
98 Id. at 623.
100 In re Sealed Case, 310 F.3d 717, 746 (Foreign Intel. Surv. Ct. Rev. 2002).
under FISA in criminal investigations. In addition, FISCR held that the wall between law enforcement and foreign intelligence investigations that FISC attempted to enforce was not required under FISA, as amended by the Patriot Act, or by the Fourth Amendment to the Constitution.

The FISCR decision endorsed the Patriot Act amendments to FISA even in light of the amendments lowering the standard to something below probable cause. The FISCR decision acknowledged as much, stating "the procedures and government showings required under FISA, if they do not meet the minimum Fourth Amendment warrant standards, certainly come close." The Fourth Amendment requires that a warrant be issued by a neutral, disinterested magistrate based on a probable cause finding of criminal activity and a description of the location to be searched and the items to be seized. The FISA foreign intelligence standard of probable cause differs from the Fourth Amendment probable cause standard in that the FISA standard requires only probable cause that the target is a foreign power or an agent of a foreign power; there is no requirement that the magistrate find probable cause of criminal wrongdoing. FISA facilitates the government in obtaining a court order allowing surveillance under the guise of national security even without meeting the Fourth Amendment warrant requirements.

After the FISCR decision, one might question whether the Fourth Amendment continues to mandate any framework for a court to approve law enforcement surveillance. The FISCR decision allows criminal surveillance to proceed after following the FISA procedures even though the FISA standard falls below that of the Fourth Amendment. Obtaining a FISA court order may become the preferred method of conducting surveillance in criminal investigations, as the law enforcement officer seeking judicial approval need not comply with the higher standard of the Fourth Amendment.

Employing FISA as the easier method for obtaining surveillance authority may result in an increase in surveillance applications under

101 Id. at 727.
102 Id. at 719-20, 746.
103 Id.
104 U.S. CONST. amend. IV.
FISA, which is what has happened. Prior to the Patriot Act (years 1979 through 2001) FISC granted 14,036 surveillance orders, without rejecting any surveillance applications; thus, the court granted an average of 610 annually.\(^\text{106}\) After the Patriot Act through 2012, FISC granted 19,906 surveillance orders and rejected eleven surveillance applications; thus, the court granted an average of 1,809 annually, amounting to a nearly 300 percent growth over the first twenty-three years.\(^\text{107}\)

C. Other Federal Courts

Similarly, other federal courts have not presented a meaningful challenge to the executive branch’s increased power. Particularly, in cases addressing the issue of FISA, the courts have almost unanimously found in favor of the government’s law enforcement efforts. Although hundreds of cases have been addressed by the federal judiciary since 9/11, the exceptions are limited to two: *Mayfield v. United States*\(^\text{108}\) and *Al-Haramain v. Bush*.\(^\text{109}\)

i. Mayfield v. United States\(^\text{110}\)

On March 11, 2004, terrorists exploded bombs in commuter subway cars in Madrid, Spain.\(^\text{111}\) The explosions killed 191 people and injured nearly 1,600, including Americans.\(^\text{112}\) During the investigation following the bombings, the Spanish National Police (SNP) located a


\(^{107}\) Id.

\(^{108}\) *Mayfield*, 504 F. Supp. 2d 1023, 1026-27 (D. Or. 2007), vacated, 599 F.3d 964 (9th Cir. 2010).


\(^{110}\) Steven T. Wax, the Public Defender, represented Brandon Mayfield in the criminal proceeding. For Wax’s account, see STEVEN T. WAX, KAFKA COMES TO AMERICA: FIGHTING FOR JUSTICE IN THE WAR ON TERROR (2008). The Kafka reference is to Kafka’s *The Trial*, in which the suspect, Joseph K., is arrested without ever being informed of the criminal charges against him nor the evidence forming the basis of the charges. *Id.* at 176-77.

\(^{111}\) *Mayfield*, 504 F. Supp. 2d at 1026-27.

\(^{112}\) *Id.* at 1027.
van used by the terrorists. Inside was a plastic bag that contained detonation materials believed to have been used by the bombers. On the bag containing the detonators, SNP investigators discovered a latent fingerprint. Seeking the help of the FBI, the SNP transmitted the print to FBI fingerprint experts in Quantico, Virginia.

Initially, the FBI failed to identify a match with the Madrid print. The decision was made to select the twenty individuals whose prints shared the most characteristics with the Madrid print. On March 17, 2004, an FBI fingerprint specialist matched the Madrid print with Brandon Mayfield. An independent examiner and an FBI manager, both of whom knew of Quantico’s initial match determination and of Mayfield’s Muslim faith, later reviewed the prints and agreed with the FBI’s initial determination. It is not uncommon for fingerprint analysts to interpret fingerprint data consistently with information known prior to examining the fingerprint data. It seems that the intense desire to locate a bombing suspect and the circumstance of Mayfield being Muslim reinforced the confirmation bias of FBI personnel that Mayfield was connected to the Madrid bombing. On March 20, the FBI issued its formal statement reporting that Mayfield’s fingerprint matched Madrid’s latent fingerprint #17. Mayfield, a United States citizen, was a former U.S. Army officer from Kansas. An attorney practicing near Portland, Oregon, Mayfield is Muslim.

The following day FBI agents commenced surveillance of Mayfield and his family. The FBI wiretapped the telephones in Mayfield’s Oregon home and law office, bugged both his residence and his office and conducted sneak-and-peak surveillance of the home and the office. The authorization for the surreptitious surveillance came not from a

113 Id.
114 Id.
115 Id.
116 Id.
117 Id.
118 Id.
119 Mayfield v. United States, 599 F.3d 964, 966-67 (9th Cir. 2010).
120 504 F. Supp. 2d at 1027-28.
121 599 F.3d at 967.
122 Id. at 966.
123 Id.
124 504 F. Supp. 2d at 1028.
125 Id.
Fourth Amendment warrant but from a FISA order. On multiple occasions after surveillance began, family members returned to the Mayfield’s home and noticed small indications that someone had been in their home. Consistent with the FISA surveillance, the Mayfields were not entitled to any notice that the surveillance, including the sneak-and-peek searches, was ongoing.

The FBI sent Mayfield’s fingerprints to the SNP on April 2 even though by this time the Spanish authorities had identified Moroccans as the bombing suspects and had taken them into custody. The Spanish authorities found “too many unexplained dissimilarities” to match Mayfield’s fingerprint with the Madrid print. FBI officials flew to Madrid for meetings in an effort to convince the SNP that the FBI match was reliable. Notwithstanding the FBI’s insistence during the meetings in Spain, the Spanish authorities continued to disagree with the FBI’s determination that Mayfield was a match and refused to validate the FBI’s identification. Spanish authorities issued an April 13, 2004 report to the FBI stating that the SNP disagreed with the FBI match of Mayfield’s fingerprint and the Madrid print.

On May 4, 2004, the federal government requested an order from the federal district court naming Mayfield as a material witness. The affidavit filed in support of the request stated that there was a “100% positive identification” between Mayfield and the Madrid print and that Mayfield was Muslim with ties to the Muslim community. The affidavit failed to mention that the Spanish authorities had refuted the FBI conclusion that Mayfield’s fingerprint matched the Madrid print. The FBI’s affidavit supporting the request for an arrest warrant indicated that Mayfield’s Muslim faith played a significant role in his identification, selection and subsequent arrest. The affidavit contained several references to Mayfield’s faith, to his attendance at a Muslim mosque,
and to his advertisements of his law practice in a Muslim publication. The FBI arrested Mayfield on May 6 and held him without bail on a material witness warrant. Mayfield was released on May 21, one day after Spanish authorities announced that they had matched the Madrid print with Ouhane Daoud, an Algerian citizen.

Mayfield filed civil suit against the federal government on October 4, 2004, which resulted in a two million dollar settlement in November of 2006. The settlement allowed Mayfield to request declaratory relief that two sections of the Foreign Intelligence Surveillance Act (50 U.S.C. §§ 1804, 1823) are unconstitutional. The United States district court judge granted declaratory relief requested by Mayfield, holding that the statutes violated the Fourth Amendment. The judge found that FISA does not require probable cause that the suspect was involved with criminal activity; FISA requires only that a “significant purpose” of the warrant, rather than the “primary purpose,” is to collect foreign intelligence; so long as the government provides the information necessary for the application, FISA requires the judge to issue the court order unless the government certification is clearly erroneous; unless surveillance information is used in a criminal prosecution, a FISA target is not informed of the surveillance; FISA does not require that the information expected to be surveilled be described with any particularity; and the duration of a FISA court of 120 days is overly long.

On appeal, the United States Court of Appeals vacated the district court opinion; it held that Mayfield lacked standing, “because his inju-

---

136 Id. In a June 8, Senate Judiciary Committee hearing, Senator Russell Feingold was disturbed by the apparent religious profiling of Mayfield. “Mr. Mayfield appears to have been singled out for heightened scrutiny based on a number of legitimate test, but also because of his religious beliefs.” WAX, supra note 110 at 248-49.
137 599 F.3d at 967; 504 F. Supp. 2d at 1029.
138 599 F.3d at 967, 968.
139 Id. at 968. 50 U.S.C.A. § 1804 (West, Westlaw through P.L. 113-74) sets forth the requirements for obtaining a court order to conduct electronic surveillance and section 1823 sets forth the requirements for obtaining a court order to conduct physical searches.
140 504 F. Supp. 2d at 1042-43.
141 Id. at 1036.
142 Id.
143 Id. at 1039.
144 Id.
145 Id. at 1040.
146 Id.
ries already have been substantially redressed by the settlement agreement" and he no longer has the ability to request an injunction that would force the federal government to return or destroy the confiscated FISA information.

ii. Al-Haramain

Wendell Belew and Asim Ghafoor are attorneys who represented the Al-Haramain Islamic Foundation, Inc., an Oregon nonprofit corporation. Belew and Ghafoor sued the United States alleging that the NSA secretly wiretapped their conversations with a director or directors of Al-Haramain in March and April 2004 without first obtaining a FISA court order. The fact that Belew and Ghafoor learned of NSA’s surreptitious surveillance was a matter of happenstance, and the surveillance might never have been revealed had a confidential log of their conversations not been provided in error to another attorney representing Al-Haramain.

In August 2004, the Office of Foreign Assets Control (OFAC) inadvertently provided a copy of the NSA conversation log, classified top secret, to Lynne Bernabei among various discovery documents related to an ongoing matter with OFAC. At the time, Bernabei was an attorney representing Al-Haramain in OFAC’s investigation to determine whether Al-Haramain should be named a specially designated global terrorist. She in turn provided copies of the log to Al-Haramain’s directors. Several months later, the FBI realized the error, informed Bernabei that she had inadvertently received the top secret log, and requested its return. Bernabei returned it to the FBI, but the FBI failed to request the log’s return from Al-Haramain’s directors.

In September 2004, the OFAC named Al-Haramain as a specially designated global terrorist based on the NSA log of the Belew and

147 Mayfield v. United States, 599 F.3d 964, 966 (9th Cir. 2010).
148 Id. at 973.
150 Id. at 1218.
151 Id. at 1218-19.
152 Id. at 1219.
153 Id. at 1218.
154 Id. at 1219.
155 Id.
156 Id.
Al-Haramain, Belew, and Ghafoor chose FISA as their weapon, bringing suit under FISA’s civil penalty provisions. They asked that the wiretapping be declared illegal, that the wiretapped information be disclosed, that the information be destroyed, and that the court enjoin further wiretapping of their conversations without court order. For the administrative wrong, they requested statutory damages, punitive damages, costs, and attorney fees.

The government argued that state secrets privilege protected the log, which was submitted to the court as a sealed document, as well as other information concerning plaintiffs’ claims, and that the case should be dismissed. The court found that a government confirmation or denial that plaintiffs’ conversations were secretly wiretapped, as disclosed in the sealed document, would not present a danger to national security. Accordingly, the court denied the government’s motion to dismiss, and on the government’s request certified the ruling for interlocutory appeal. During the appeal, the judicial panel on Multi-district Litigation reassigned this case to Chief Judge Vaughn Walker of the Northern District of California.

On appeal, the United States Court of Appeals for the Ninth Circuit in 2007 agreed with the district court. Although the state secrets privilege protects the sealed document from public disclosure, the state secrets privilege does not preclude the continuation of Al-Haramain’s lawsuit. The appellate court did, however, reverse the trial court’s decision to allow the participants of the conversations to reconstruct the sealed document. Whether FISA preempts the state secrets privilege was a question left unanswered by the circuit court. The circuit court remanded the matter to the district court to allow consideration of this question.

157 Id. at 1218.
158 Id.
159 Id.
160 Id.
161 Id. at 1219.
162 Id. at 1224.
163 Id. at 1233.
164 Al-Haramain Islamic Found., Inc. v. Bush, 507 F.3d 1190, 1196 (9th Cir. 2007).
165 Id. at 1198.
166 Id.
167 Id. at 1193.
168 Id.
169 Id.
On remand, the district court determined affirmatively that FISA preempts the state secrets privilege where a litigant seeks information from government wiretapping. Where the government claims that disclosure of information obtained by wiretap would endanger national security, 50 U.S.C. § 1806(f) directs the court to review the information in camera, ex parte. "Section 1806(f)...is in effect a codification of the state secrets privilege for purposes of relevant cases under FISA, as modified to reflect Congress's precise directive to the federal courts for the handling of materials and information with purported national security implications." The court dismissed the complaint without prejudice, specifically allowing the plaintiffs to re-file their action and present sufficient facts to demonstrate that they qualified as "aggrieved persons" under FISA.

The plaintiffs filed an amended complaint including a more detailed factual basis for their claims, relying in part on public statements by the government and a description of the government's investigations of Al-Haramain. The facts describe a series of telephone conversations between Belew, in Washington, D.C., and Soliman al-Buthi, an alleged director of Al-Haramain located in Riyadh, Saudia Arabia, and between Ghafoor, located in Washington, D.C., and al-Buthi, located in Riyadh, Saudia Arabia. The conversations concerning the attorneys' representation of Al-Haramain occurred in the spring of 2004. During the conversations, the parties mentioned various individuals who were linked to Osama bin-Laden.

The government argued that the plaintiffs lacked standing to bring their lawsuit, contending that, without the government admitting that the plaintiffs' conversations were subject to wiretapping in the absence of a court order, the plaintiffs would be unable to furnish evidence that they were subjects of warrantless wiretapping. The district court disagreed and on January 5, 2009, it issued its decision finding that the

---

171 Id. at 1119.
172 Id. at 1137.
174 Id. at 1080.
175 Id.
176 Id. at 1080-81.
177 Id. at 1085, 1086.
plaintiffs had presented sufficient evidence to plead that they are “aggrieved persons” under FISA. 178 Further, the court held that “to find plaintiffs’ showing inadequate would effectively render [the relevant] provisions of FISA without effect.” 179 The court denied the government’s motion to dismiss and took several other actions designed to protect classified information while allowing the plaintiffs to proceed with the lawsuit. 180 The court ordered the government to make the sealed document available for in camera, ex parte review, to facilitate security clearance for several attorneys representing the plaintiffs, and to review and declassify any documents subject to declassification. 181

The court denied the government’s motion to dismiss and took several other actions designed to protect classified information while allowing the plaintiffs to proceed with the lawsuit. 180 The court ordered the government to make the sealed document available for in camera, ex parte review, to facilitate security clearance for several attorneys representing the plaintiffs, and to review and declassify any documents subject to declassification. 181

The court denied the government’s motion to dismiss and took several other actions designed to protect classified information while allowing the plaintiffs to proceed with the lawsuit. 180 The court ordered the government to make the sealed document available for in camera, ex parte review, to facilitate security clearance for several attorneys representing the plaintiffs, and to review and declassify any documents subject to declassification. 181

The government failed to comply with the court’s 2009 directives and the plaintiffs requested summary judgment. 182 In a momentous decision approximately one year later, the United States District Court for the Northern District of California granted plaintiffs’ motion for summary judgment on their claim that the government intercepted their conversations without court order in violation of FISA; the court denied the government’s motion to dismiss and motion in opposition to plaintiffs’ motion for summary judgment. 183 “[D]efendants have failed to meet their burden to come forward, in response to plaintiffs’ prima facie case of electronic surveillance, with evidence that a FISA warrant was obtained, that plaintiffs were not surveilled or that the surveillance was otherwise lawful.” 184 The court commented: “[u]nder defendants’ theory, executive branch officials may treat FISA as optional and freely employ the [state secrets privilege] to evade FISA, a statute enacted specifically to rein in and create a judicial check for executive-branch abuses of surveillance authority.” 185

The court remarked on “defendants’ intransigence following the court’s January 5, 2009 order and the limited progress made to date along the normal arc of civil litigation.” 186 Woven through the decision

---

178 Id. at 1086.
179 Id.
180 Id. at 1089.
181 Id. at 1089-90.
183 Id. at 1183.
184 Id.
185 Id. at 1195-96.
186 Id. at 1195.
are numerous examples of the government’s failure to cooperate with the court. For example, in a May 22, 2009 order, the court noted that the government had not cooperated with several court orders and ordered the government to show cause why the court should not impose various sanctions. In the March 31, 2010 decision, the court characterized the period between January 5, 2009 and May 22, 2009 as “several months of which the defining feature was defendants’ refusal to cooperate with the court’s orders punctuated by their unsuccessful attempts to obtain untimely appellate review.” Even after two of plaintiffs’ attorneys received security clearance, the government “refused to cooperate with the court’s orders, asserting that plaintiffs’ attorneys did not ‘need to know’ the information that the court had determined plaintiffs attorneys would need in order to participate in the litigation.” In addition, the “defendants refused to agree to any terms of the protective order proposed by plaintiffs and refused to propose one of their own.”

The court’s grant of plaintiffs’ motion for summary judgment was largely dictated by the government’s failure to submit information for in camera review pursuant to § 1806(f). The government “in an impressive display of argumentative acrobatics” argued that FISA was not applicable. The court opined that the government’s reliance on the decision of the court of appeals during the interlocutory appeal was misplaced. “The court of appeals did not contemplate that the judicial process should be intentionally stymied by defendants’ tactical avoidance of FISA . . . .”

The court concluded that “[p]laintiffs have made out a prima facie case and defendants have foregone multiple opportunities to show that a warrant existed, including specifically rejecting the method created by Congress for this very purpose.” The court found that “defendants must be deemed estopped from arguing that a warrant might have ex-

---

188 700 F. Supp. 2d at 1191.
189 Id.
190 Id.
191 Id. at 1196.
192 Id.
193 Id.
194 Id. at 1196-97.
195 Id. at 1197.
isted or, conversely, must be deemed to have admitted that no warrant existed. Having found the government liable under FISA, the court gave the plaintiffs a choice—pursue their remaining claims or dismiss the remaining claims and allow the court to enter judgment. The plaintiffs filed a motion to dismiss their second through sixth claims and a proposed judgment on April 16, 2010.

The district court held that FISA preempts the state secrets privilege and the government implicitly waived sovereign immunity under the 50 U.S.C. § 1810 civil liability provision. Based on this holding, the district court awarded $20,400 in liquidated damages to each of two individual plaintiffs, $2,515,387.09 in attorney's fees, and $22,012.36 in costs.

The issue on appeal for the second time before the Court of Appeals for the Ninth Circuit was whether the district court's holding that the government had waived sovereign immunity under § 1810 was correct. The appellate court found that any waiver of sovereign immunity must be explicit and, thus, there had been no waiver of sovereign immunity under § 1810. Therefore, the court reversed the awards of liquidated damages, attorney's fees, and costs. Although the holding of the appellate court was not favorable to the plaintiffs, the appellate court took the opportunity to dispute the government's "unfortunate argument that the plaintiffs have somehow engaged in 'game-playing.'" The appellate court applauded the way in which the plaintiffs had engaged in the litigation:

In light of the complex, ever-evolving nature of this litigation, and considering the significant infringement on individual liberties that would occur if the Executive Branch were to disregard congressionally-mandated procedures for obtaining judicial authorization of international wiretaps, the charge of "game-playing" lobbed by the government is as careless as it is inaccurate. Throughout, the plaintiffs have proposed ways of advancing their lawsuit without jeopard-

---

196 Id.
197 Id. at 1203.
198 Pls' Request Dismiss Cl. 2-6, ECF No. 116; Pls.' Proposed J., Apr. 16, 2010, ECF No. 117.
199 Al-Haramain Islamic Found., Inc. v. Obama, 705 F.3d 845, 848 (9th Cir. 2012).
200 Id. at 850.
201 Id. at 848.
202 Id. at 855.
203 Id. at 848.
izing national security, ultimately going so far as to disclaim any reliance whatsoever on the Sealed Document. That their suit has ultimately failed does not in any way call into question the integrity with which they pursued it.\textsuperscript{204}

The USA Patriot Act, subsequent amendments, and cases like \textit{Mayfield} and \textit{Al-Haramin} must be examined against a background of terrorism that is broader than the 9/11 events. In reviewing terrorism incidents over the centuries, the result of the incidents is the physical and emotional harm inflicted on the victims and the fear that the incidents engender in others who might become similarly victimized. The others who were indirectly affected by the fear that the 9/11 events caused in them are many times greater than those directly affected. Thus this "fear multiplication"\textsuperscript{205} effect has a widespread impact on society.

In an age in which information is almost instantly communicated to all parts of the globe, terrorism incidents are reported in detail and the reports fill the news for days. The government typically reacts quickly, and usually overreacts, in an effort to safeguard its citizens. Even though it is impossible to prevent all future terrorist attacks, the majority of the population demands that the government take forceful action in the interest of preserving national security, often with a resulting loss of individual privacy. "The public demands effective security measures as if total protection would be provided. This is an impossibility because the results would be an undemocratic transformation of the political order, replaced with a repressive 'surveillance society.'"\textsuperscript{206}

III. PRESENT STATE OF DOMESTIC SURVEILLANCE

The present state of domestic surveillance under President Bush and President Obama must be seen against the backdrop of the state secrets privilege; the breadth of that privilege should be kept in mind when reading the descriptions of the surveillance activities during the two presidencies as described below.

A 1953 case, \textit{United States v. Reynolds},\textsuperscript{207} gave birth to the state se-

\textsuperscript{204} \textit{Id.} at 848-49.

\textsuperscript{205} \textsc{Stephen Sloan}, TERRORISM: THE PRESENT THREAT IN CONTEXT 1-2 (2006).

\textsuperscript{206} \textit{Id.} at 23 (endnote omitted).

\textsuperscript{207} United States v. Reynolds, 345 U.S. 1 (1953). In Reynolds, three widows of civilian observers killed in a crash of a B-29 in 1948 while testing secret electronic equipment. The plaintiffs sought disclosure of the Air Force official accident investigation report and statements of the surviving crew members. \textit{Id.} at 2-3. The Court held that:
crets privilege. As applied in Reynolds, the state secrets privilege could be thrown up by the government like a brick wall against discovery without the government showing any necessity for the state secrets privilege nor the contested material having to pass an in camera review.

It is ironic that Reynolds left the country with the judicial branch’s complete acquiescence to an executive branch’s claim of state secret privilege, when, in reality, there was no state secret to protect in Reynolds. In 2000, a daughter of one of the civilian engineers killed in the Reynolds crash reviewed the contested documents, then declassified, and found no evidence that they contained any type of government secret.208 The documents showed “that the B-29 that crashed in 1948 was not fit for flying; that the crew had not previously flown together; and that the civilian engineers who died in the crash had not been instructed about emergency exit procedures.”209 One of the prime government motivations was “shielding the Air Force from substantial public embarrassment.”210

The federal government considers much of the information gathered in a FISA wiretap to be classified information or subject to the state secrets privilege, unavailable to all but those with a top security privilege, because the information concerns foreign intelligence. Thus, the FISA target may be blissfully unaware that he or she is subject to the most intrusive government surveillance and, even if the target somehow has knowledge of the wiretap, the target may not effectively challenge the legality of the wiretap where the target cannot gain access to that which the government claims to be classified information or subject to the state secrets privilege.

In one case, the targets of electronic surveillance received confirmation of the surveillance in a classified document that was inadvertently turned over to the targets’ attorney among unclassified documents when the formal claim of privilege was filed by the Secretary of the Air Force, under circumstances indicating a reasonable possibility that military secrets were involved, there was certainly a sufficient showing of privilege to cut off further demand for the document on the showing of necessity for its compulsion that had then been made.

Id. at 10-11.


209 Id. at 1393 (footnotes omitted). See id. at 1294-1312.

210 Id. at 1290.
provided to the attorney by the government during discovery. The judge in the case ordered the classified document be returned to the government under seal.\textsuperscript{211} Thus, the targets were in the anomalous position of having learned of the government surveillance through a classified document but being unable to use that same document to establish their status as aggrieved persons.\textsuperscript{212}

Both the George W. Bush administration and the Obama administration have invoked the state secrets privilege to build a firewall effectively preventing investigation into NSA surveillance.\textsuperscript{213} The same danger exists that existed with Reynolds in that deference to the executive branch may very well shroud information other than state secrets in secrecy and some information on surveillance is only available by virtue of it being accessible through the Snowden revelations. "[D]ocuments revealed by Edward Snowden have made all too clear that abuses have resulted from the secrecy surrounding the government’s interpretation of the law and of the national security surveillance programs, and the lack of effective oversight of these programs."\textsuperscript{214} These revelations may give cause for a court to closer scrutinize a future executive branch’s claim of state secrets privilege and may make one who makes international calls suspicious of government surveillance.

A. The Terrorist Surveillance Program\textsuperscript{215}

Nearly five years into the George W. Bush presidency, two New York Times reporters revealed information on what became to be

\textsuperscript{211} In re National Security Agency Telecommunications Records Litigation, 595 F. Supp. 2d 1077, 1082 (N.D. Cal. 2009); In re National Security Agency Telecommunications Records Litigation, 564 F. Supp. 2d 1109, 1111-12, 1130 (N.D. Cal. 2008). See supra notes 149-204, and accompanying text.

\textsuperscript{212} "If reports are to be believed, plaintiffs herein would have had little difficulty establishing their ‘aggrieved person’ status if they were able to support their request with the Sealed Document." 564 F. Supp. 2d at 1134.


known as the Terrorist Surveillance Program (TSP). The TSP was hauntingly reminiscent of President Roosevelt’s executive order some seventy years earlier in which he authorized surreptitious surveillance in the name of national security. Under the TSP, President Bush had authorized wiretapping to gather evidence of terrorist action of at least 500 individuals in this country and an estimated 5,000 to 7,000 individuals outside the country. Unlike FISA wiretapping, which is authorized by a super warrant in accordance with statutory provisions, the Bush wiretapping was authorized by executive order and was conducted by the NSA without the aid of any warrant, any court oversight, or any prior congressional knowledge or approval. In fact, the surreptitious surveillance was authorized by President Bush in 2002 and did not come to light until some three years later.

President Bush’s decision to authorize warrantless surveillance was severely criticized because the TSP procedure was not in conformity with FISA; to this, the Bush Administration’s response was that, because of the need for national security, the country is in the midst of “a different war.” The TSP procedure differed from the FISA requirements in a number of respects. Apparently, TSP substituted an NSA employee for a federal judge in making the initial decision to conduct surveillance, with the NSA employee using a standard of “reasonable suspicion” in determining whether to further target from information gleaned in data mining. The TSP activities were not reported to Congress or to the judiciary, as required under FISA. In fact, the Bush Administration vigorously denied being engaged in any secret intelligence gathering until the TSP details were revealed in the New York Times in 2005.

TSP included the computerized data mining of vast data bases of telecommunications; this search was done by the federal government with the cooperation of major telecommunications companies. Prior

\[\text{\cite{216}}\]
\[\text{\cite{217}}\]
\[\text{\cite{218}}\]
\[\text{\cite{219}}\]
\[\text{\cite{220}}\]
\[\text{\cite{221}}\]
\[\text{\cite{222}}\]
\[\text{\cite{223}}\]
\[\text{\cite{224}}\]
\[\text{\cite{225}}\]

\[\text{\cite{221}}\]
\[\text{\cite{222}}\]
\[\text{\cite{223}}\]
\[\text{\cite{224}}\]
\[\text{\cite{225}}\]

Jon D. Michaels, *All the President’s Spies: Private-Public Intelligence Partnerships in the War on
to the disclosure of the TSP activities, it was widely assumed that both the federal government and the telecommunications companies were complying with FISA.\footnote{Id. at 910, 911.} After the disclosure of the TSP activities, a number of persons who were allegedly targets of TSP surveillance sued the telecommunications companies for their participation in the warrantless surreptitious surveillance.\footnote{See, e.g., Hepting v. AT & T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006), remanded, 539 F.3d 1157 (9th Cir. 2008) (remanding in light of the FISA Amendments Act of 2008).} FISA was amended in 2008 to provide specific statutory protection after the fact to the telecommunications companies who had facilitated the secret surveillance.\footnote{50 U.S.C.A. § 1885a (West, Westlaw through P.L. 113-74).}

Approximately a half a dozen undersea cables carry international communications from other continents to each coast of the United States; when the cables surface on the Atlantic and Pacific coasts, telecommunications switches spread the communications to various parts of the United States.\footnote{JAMES BAMFORD, THE SHADOW FACTORY: THE ULTRA-SECRET NSA FROM 9/11 TO THE EAVESDROPPING ON AMERICA 176-77 (2008).} AT&T and NSA cooperated in having a splitter installed in the AT&T switching station in San Francisco; the splitter created an exact copy of the communications flowing through the switching station and transmitted this copy to NSA.\footnote{Id. at 194-95.} NSA apparently used similar equipment to review communications flowing through other AT&T switching stations in the United States.\footnote{Id. at 188-90, 193.}

Under “peering” agreements among AT&T and other telecommunications companies, the companies make joint use of telecommunications cables, allowing the companies to avoid the cost of entirely separate communications systems. The fact that telecommunication cables are shared permitted the federal government to access communication traffic of telecommunication companies other than AT&T. The existence of the splitter in the San Francisco switching station provided the executive branch with access to the domestic as well as the international telecommunications handled by the San Francisco switch.\footnote{ERIC LICHTBLAU, BUSH’S LAW: THE REMAKING OF AMERICAN JUSTICE 139 (Anchor Books 2009) (2008).}

In a 2008 FISA amendment, Congress attempted to foreclose war-
rantless surveillance, such as TSP, from again being conducted by the executive branch. The 2008 FISA amendment named FISA, and other federal statutes as the "exclusive means" of the federal government performing surveillance.233

B. *The Protect America Act*234

Following the negative public reaction to TSP, Congress passed the Protect America Act of 2007 (PPA).235 The effect of the PPA was to authorize NSA surveillance and to authorize surveillance without FISA restrictions when "directed at a person reasonably believed to be located outside of the United States."236 It was up to the Attorney General to define, by "reasonable procedures," the phrase "directed at."237 The PAA required no connection between the surveillance target and the agent of a foreign power or terrorist except that gathering foreign intelligence information be the "significant purpose of the acquisition."238

Congress passed the PAA conditioned on a six-month sunset,239 which went into effect when Congress failed to pass legislation by the sunset-imposed deadline. The House and Senate had difficulty in passing legislation because the two houses disagreed on whether the telecommunications companies should be granted retroactive immunity for their participation in TSP surveillance.240 At the end of the six-month period, the PAA provisions were replaced with the prior FISA provisions until July 2008, when the FISA Amendments Act of 2008 took effect.241

---

235 Id.
236 Id. at § 2 (emphasis added).
237 Id.
238 Id. at § 2.
239 Id. at § 6.
240 Jon D. Michaels, *All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror*, 96 CAL. L. REV. 901, 922 n.86 (2008).

At the end of 2012, Congress extended for an additional five years certain provisions of the 2008 amendments that otherwise would have been subject to sunset provisions on December 31, 2012. FISA Amendments Act Reauthorization Act of 2012, Pub. L. No. 112-238, 126 Stat.
C. Snowden Disclosures of 2013

The sweep of the surveillance under the Obama presidency was revealed to the public beginning in June 2013 with Edward Snowden's leak of NSA information during the summer of 2013.\(^{242}\) The leaked information was the subject of numerous newspaper articles,\(^{243}\) the first on June 5, 2013 in The Guardian. The article concerned a FISC order dated April 25, 2013 that required Verizon to turn over telephone metadata on international and domestic telephone calls to the NSA under the business records provision of section 215 of the Patriot Act. Rather than containing the substance of the calls, metadata contains the conversants' telephone numbers, the time and duration of the call, and the geographic location of the conversants.\(^{244}\) Subsequent newspaper articles revealed similar FISC section 215 business records orders allowing the NSA access to telephone metadata from other telecommunications companies.\(^{245}\) The NSA is not limited on telephone calls to gathering metadata, as it uses its Upstream program to collect information directly from fiber-optic cables comprising the backbone of the Internet. The four telecommunications companies facilitating this collection have as yet not been identified.\(^{246}\)

On June 6, 2013, The Washington Post and The Guardian broke revelations on a program named Prism that permits the NSA access to the systems of nine prominent Internet companies. In contrast to the metadata collected from Verizon, the information available to the NSA included email, audio chat, video chat, and file transfer contents together with the Internet customer's search history. The names of the Inter-

---


\(^{244}\) Glenn Greenwald, NSA collecting phone records of millions of Verizon customers daily; Exclusive: Top secret court order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama, GUARDIAN, June 5, 2013, http://www.theguardian.com/world/2013/jun/06/verizon-court-order.


\(^{246}\) Id.
net companies and the beginning date of NSA access were Microsoft from 2007, Yahoo from 2008, Google, Facebook, and PalTalk from 2009, YouTube from 2010, Skype and AOL from 2011, and Apple from 2012.\(^{247}\)

NSA uses a number of methods to circumvent the encryption protecting a good portion of the information being transmitted via the Internet. Certain methods involve software engineering, such as gaining access through software security weaknesses, through "back doors" into software that software companies have been enticed to provide, or through incorporating security weaknesses into encryption standards. Other methods include gaining pre-encryption access to target computers, using its library of encryption keys to access encrypted information, or breaking encryption.\(^{248}\)

D. The Judicial Branch since the Snowden Disclosures

Since June of 2013, it is as if a curtain had been drawn back on scenes that were previously hidden from public view. The Snowden revelations unleashed a sea change with regard to all things FISA, including challenges to the newly-revealed NSA programs.

i. FISA Courts

Two changes concerning the FISC were the release by the FISC of certain FISC documents considered "public filings"\(^{249}\) and the release of a number of FISC pre-June 2013 opinions, including an October 3, 2011 opinion authored by FISC Judge John D. Bates.\(^{250}\)

The two FISC opinions discussed below were largely supportive of NSA activities; however, each of the opinions notes problems with NSA activities. The first opinion dated August 29, 2013 and authored


by FISC Judge Claire V. Eagan\(^{251}\) permitted NSA access to telephone metadata; the second opinion, the Bates opinion referenced in the preceding paragraph,\(^{252}\) dealt with NSA collection of telephone and Internet communications.

As far as problems with NSA activities are concerned, Judge Eagan noted in the first opinion, “The Court is aware that in prior years there have been incidents of non-compliance with respect to NSA’s handling of produced information. Through oversight by this Court over a period of months, those issues were resolved.”\(^{253}\)

In the first opinion, Judge Eagan granted the FBI’s application to collect telephone metadata business records from certain telephone service providers under section 215 of the Patriot Act.\(^{254}\) Prior to granting the application, the judge first determined that the business records production did not violate the Fourth Amendment in that the production fell squarely within the third party doctrine announced in *Smith v. Maryland*.\(^{255}\) The judge found that the facts in *Smith* were extremely similar to the case before the court with “telephone companies maintain[ing] call detail records in the normal course of business for a variety of purposes.”\(^{256}\) The judge explained, “The telephone user, having conveyed this information to a telephone company that retains the information in the ordinary course of business, assumes the risk that the company will provide that information to the government.”\(^{257}\) The judge added, “Thus, the Supreme Court concluded that a person does not have a legitimate expectation of privacy in telephone numbers dialed and, therefore, when the government obtained that dialing infor-

\(^{251}\) *In Re Application of the Fed. Bureau of Investigation for an Order Requiring the Prod. of Tangible Things from [Redacted], No. BR 13-109, 2013 WL 5741573, at *1 (F.I.S.C. Aug. 29, 2013) (declassified and redacted) [hereinafter Eagan opinion].*

\(^{252}\) Bates opinion at *1.

\(^{253}\) Eagan opinion at *1 n.8.

\(^{254}\) *Id.* “Those telephone company business records consist of a very large volume of each company’s call detail records or telephony metadata, but expressly exclude the contents of any communication; the name, address, or financial information of any subscriber or customer; or any cell site location information . . . .” *Id.* Although the application produces a substantial volume of business records, “trained personnel [initiate] a query process that requires a reasonable, articulable suspicion (RAS), as determined by a limited set of personnel, that the selection term (e.g., a telephone number) that will be used to search the data is associated with one of the identified international terrorist organizations.” *Id.*

\(^{255}\) *Id.* at *2. For information on *Smith v. Maryland*, see notes 56-65, *supra* and accompany text.

\(^{256}\) Eagan opinion at *2.

\(^{257}\) *Id.*
mation, it "was not a 'search,' and no warrant was required" under the Fourth Amendment."\(^{258}\)

Next, Judge Eagan reviewed the application to determine whether the proposed business records production complied with section 215. The judge recognized that under the Patriot Act, "Congress provided the government with more latitude at the production stage under Section 215 by not requiring specific and articulable facts or meeting a materiality standard."\(^ {259}\) The judge explained that "[w]here there is no requirement for specific and articulable facts or materiality, the government may meet the standard under Section 215 if it can demonstrate reasonable grounds to believe that the information sought to be produced has some bearing on its investigations of the identified international terrorist organizations."\(^ {260}\) The judge further recognized that Congress "imposed post-production checks in the form of mandated minimization procedures and a structured adversarial process."\(^ {261}\) Judge Eagan noted that Congress ratified this statutory framework by reenacting section 215 without change and after members of Congress had been provided with information concerning the collection of telephone metadata in bulk.\(^ {262}\)

In the second opinion, Judge Bates seemed much more concerned about government omissions regarding its collection efforts. "The Court is troubled that the government's revelations regarding NSA's acquisition of Internet transactions mark the third instance in less than three years in which the government has disclosed a substantial misrepresentation regarding the scope of a major collection program."\(^ {263}\) The judge continued, "The government's submissions make clear not only that NSA has been acquiring Internet transactions since before the Court's approval of the first Section 702 certification in 2008, but also that NSA seeks to continue the collection of Internet transactions."\(^ {264}\)

In the 2011 opinion, Judge Bates considered the government's request to collect telephone and Internet communications under section 702 of the Patriot Act.\(^ {265}\) The judge did not seem to have a problem

\(^{258}\) Id.
\(^{259}\) Id. at *5.
\(^{260}\) Id. at *6.
\(^{261}\) Id. at *5.
\(^{262}\) Id. at *8-9.
\(^{263}\) Id. at *5 n.14.
\(^{264}\) Id. at *6 (footnote omitted).
\(^{265}\) Id. at *1.
approving the government application to the extent it was similar to prior applications concerning collection of communications from Internet service providers; however, the government’s "upstream collection" of Internet communications, which "refers to NSA’s interception of Internet communications as they transit [redacted], . . . rather than to acquisitions directly from Internet service providers" presented more of a problem to the judge. Although the upstream collection was only some nine percent of the Internet communications collected, the technological limits on the collection method foreclosed the government’s ability to locate "wholly domestic communications acquired through this collection, nor can it know the number of non-target communications acquired or the extent to which those communications are to or from United States persons or persons in the United States."

Judge Bates reviewed the types of Internet communications collected by the government, distinguishing a "single discrete communication" transaction from a transaction containing "multiple discrete communications" (MCTs). The MCTs were more problematic because "NSA is likely acquiring tens of thousands of discrete communications of non-target United States persons and persons in the United States, by virtue of the fact that their communications are included in MCTs selected for acquisition by NSA’s upstream collection devices."

Judge Bates held that NSA’s minimization of retained MCTs did not comply with statutory requirements and that the NSA’s targeting and minimization methods concerning MCTs were not consistent with the Fourth Amendment.

ii. Other Federal Courts

The Snowden disclosures enabled plaintiffs in two cases to challenge the NSA’s collection of telephone metadata and to request pre-

---

266 Id. at *9.
267 Id. at *2.
268 Id. at *2 n.3.
269 Id. at *9.
270 Id. at *10.
271 Id. at *9.
272 Id. at *11.
273 Id. at *21.
274 Id. at *28.

Although the *American Civil Liberties Union* opinion was patriotic in tone and acquiesced to the NSA collection, Judge Pauley emphasized the potential for abuse with such collection:

>This blunt tool only works because it collects everything. Such a program, if unchecked, imperils the civil liberties of every citizen. Each time someone in the United States makes or receives a telephone call, the telecommunications provider makes a record of when, and to what telephone number the call was placed, and how long it lasted. The NSA collects that telephony metadata. If plumbed, such data can reveal a rich profile of every individual as well as a comprehensive record of people’s associations with one another.277

Although recognizing the potential for abuse by the executive branch, the judge deferred to the other two branches of federal government to determine whether to continue the bulk telephone metadata collection program.278

Judge Pauley noted that, although the FISC operates in secrecy, the NSA metadata collection program “is subject to extensive oversight by all three branches of government.”279 Congress ratified section 215 by reenacting it a number of times and use of the metadata is subject to minimization requirements.280

The judge found that the plaintiffs did have standing, but that the only party able to challenge a FISC order under the statutory scheme was the party subject to the order to produce. In holding that the metadata collection program did not violate the Fourth Amendment, the judge invoked the “bedrock holding” of *Smith v. Mary-

---

275 959 F. Supp. 2d 724, 757 (S.D.N.Y. 2013). The judge commented that the lawsuit was a product of the Snowden revelations. *Id.* at 730.
276 957 F. Supp. 2d 1, 43 (D.D.C. 2013). This lawsuit was also the product of the Snowden revelations. *Id.* at 10.
277 959 F. Supp. 2d at 757.
278 *Id.*
279 *Id.* at 731-32.
280 *Id.* at 733-34.
281 *Id.* at 738.
282 *Id.* at 741.
that relied on the third party doctrine. The opinion discussed Smith but refused to distinguish Smith from the case under consideration. The judge relied on Amnesty International in dismissing the plaintiffs' First Amendment claims as a "speculative fear" that the NSA collection had a "chilling effect" on plaintiffs' telephone communication. The judge found the metadata collection program to be lawful and denied the plaintiffs' motion for a preliminary injunction.

Judge Leon in Klayman seems much less trusting of government representations than Judge Pauley in American Civil Liberties Union. For example, Judge Leon stated:

While more recent FISC opinions expressly state that cell-site location information is not covered by Section 1861 production orders, the Government has not affirmatively represented to this Court that the NSA has not, at any point in the history of the Bulk Telephony Metadata Program, collected location information... about cell phones.  

Another example is the government's representation that the number of metadata records located within three hops of a target is "substantially larger than 300, but is still a very small percentage of the total volume of metadata records." Judge Leon responded, "The first part of this assertion is a glaring understatement, while the second part is virtually meaningless when placed in context." The judge pointed out, "it is possible to arrive at a query result in the millions within three hops while using even conservative numbers."

Judge Leon in Klayman clearly warned of the potential for government abuse of the collection program. "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this systematic and high-tech collection and retention of personal data on virtually every single citizen for purposes of querying and analyzing it without prior judicial approv-

---

283 Id. at 749-52. For information on Smith v. Maryland, see notes 56-65, supra and accompany text.
284 959 F. Supp. 2d at 749-52.
285 Id. at 753-54.
286 Id. at 757.
287 957 F. Supp. 2d at 15 n.17.
288 Id. at 16 n.21.
289 Id.
290 Id.
The judge added, "Surely, such a program infringes on 'that degree of privacy' that the Founders enshrined in the Fourth Amendment."  

Judge Leon first considered whether the NSA metadata collection program exceeds the statutory scheme, thus violating the Administrative Procedure Act. The judge found that, although the recipient of a production order can challenge NSA activity, the statutory scheme precludes a subscriber from doing so.

Then the judge proceeded to consider whether a non-FISC court could consider whether the application of a FISC order violated the United States Constitution. The judge decided that, because Congress had not expressly ruled out such a challenge, the court could review the plaintiffs' claims. The court reasoned, "Where, as here, core individual constitutional rights are implicated by Government action, Congress should not be able to cut off a citizen's right to judicial review of that Government action simply because it intended for the conduct to remain secret by operation of the design of its statutory scheme."

The judge next concluded that the plaintiffs had standing to challenge the bulk collection of telephone metadata and the analysis of the data as they "can point to strong evidence that, as Verizon customers, their telephony metadata has been collected for the last seven years (and stored for the last five) and will continue to be collected barring judicial or legislative intervention."

in 2012 in which the Court distinguished Jones from Knotts. Judge Leon inquired, “When do present-day circumstances—the evolutions in the Government’s surveillance capabilities, citizens’ phone habits, and the relationship between the NSA and telecom companies—become so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like Smith simply does not apply?” The court decided that Klayman should be distinguished from Smith.

The first distinction was the length of time, with the pen register in Smith operational for a few days, whereas the metadata collection program in Klayman operational since May of 2006, retaining five years of records, and continuing operational into the foreseeable future. In Smith, there was a “one-time, targeted request for data regarding an individual suspect,” while in Klayman, there was “what is effectively a joint intelligence-gathering operation” between NSA and the telecommunications companies, with NSA receiving a “daily, all-encompassing, indiscriminate dump of phone metadata.” Today’s technology is far more sophisticated and less costly than that available in 1976. In 1976, there were many fewer landline phones per person than there are with today’s “ubiquitous” cell phone. Today we live in a “cell phone-centric culture” with much more information available through metadata than in the past.

Because of the differences between Klayman and Smith, Judge Leon found that there was a search in Klayman and proceeded to determine whether the search was reasonable. In examining whether the situation was urgent, thus excusing the usual warrant requirement, “the Government does not cite a single instance in which analysis of the NSA’s bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was
time-sensitive in nature." The judge found that the search was unreasonable and granted a preliminary injunction as to two individual plaintiffs.

IV. THE FEDERAL PROSECUTOR

A. The Prosecutor: Power and Duty

The prosecutor is the individual responsible for prosecuting those suspected of committing crimes, simultaneously serving as the government’s advocate, officer of the court, and administrator. As administrator, the prosecutor’s duty is “to seek justice, not merely to convict.” The overarching, aspirational goal is to serve society. As the United States Supreme Court announced in 1935:

The United States Attorney is the representative not of an ordinary party to a controversy, but of a sovereignty whose obligation to govern impartially is as compelling as its obligation to govern at all; and whose interest, therefore, in a criminal prosecution is not that it shall win a case, but that justice shall be done.

The ideal prosecutor would be unbiased, without any conflict of interest such as personal gain, securing a conviction based on evidence of guilt beyond a reasonable doubt while keeping in mind principles of justice and fairness. Public confidence in the criminal justice system is largely based on the trustworthiness of the prosecutor.

The broad discretion afforded to prosecutors to file charges and prosecute individuals has not diminished since 9/11. In fact, both the increase in executive authority and the new means available for charging and trying the accused effectively amplify the discretion prosecutors have enjoyed historically. Seventy years ago, Justice Jackson, former United States Attorney General, recognized the breadth of prosecutori-

---

313 Id. at 40.
314 Id. at 41.
315 Id. at 43.
317 AM. BAR ASS’N, ABA STANDARDS FOR CRIMINAL JUSTICE: PROSECUTION FUNCTION AND DEFENSE FUNCTION 3-1.2(c) (3d ed. 1993).
318 NAT’L DIST. ATTORNEYS ASSN’, NATIONAL PROSECUTION STANDARDS 1-1.2 (3d ed. 2009).
320 Id.
al power. Noting that "[t]he prosecutor has more control over life, liberty, and reputation than any other person in America," Justice Jackson added further comment:

His discretion is tremendous. He can have citizens investigated and, if he is that kind of person, he can have this done to the tune of public statements and veiled or unveiled intimations. Or the prosecutor may choose a more subtle course and simply have a citizen's friends interviewed. The prosecutor can order arrests, present cases to the grand jury in secret session, and on the basis of his one-sided presentation of the facts, can cause the citizen to be indicted and held for trial. He may dismiss the case before trial, in which case the defense never has a chance to be heard. Or he may go on with a public trial. If he obtains a conviction, the prosecutor can still make recommendations as to sentence, as to whether the prisoner should get probation or a suspended sentence, and after he is put away, as to whether he is a fit subject for parole. While the prosecutor at his best is one of the most beneficent forces in our society, when he acts from malice or other base motives, he is one of the worst.

At the end of the day, it is the enforcers of the law, not the law, deciding who shall be punished for what conduct. The prosecutors' routine, everyday decisions control the direction and outcome of criminal cases and have greater impact and more serious consequences than those of any other criminal justice official. Often recognized as the most pervasive and dominant force in criminal justice, the federal prosecutor's power has grown exponentially since 9/11.

A unique feature of the prosecutor's powerful role is the fact that important, sometimes life-and-death decisions are totally discretionary and virtually unreviewable. Decisions are most often made behind

---

322 Id.
closed doors and without oversight, save other prosecutors.\textsuperscript{327} Two of the more important responsibilities resting with the prosecution – charging and plea bargaining – are outside the public view.\textsuperscript{328} Prosecutors are not alone in the discretion with which they operate, at least in the criminal justice system. Police officers and judges, as well, enjoy considerable discretion. Without some degree of discretionary power, the system would likely fail. The disturbing difference between prosecutors and other criminal justice officials is the power of the prosecutor has gone essentially unchecked.\textsuperscript{329} Unlike law enforcement and the judiciary, prosecutors have rarely been criticized, held accountable or stripped of power and discretion.\textsuperscript{330} In fact, since 9/11 federal prosecutors are heralded for their heroic attempts to thwart evil and convict the terrorists who pose continued threats to our nation and her citizens. In the sake of national security, their reward is the grant of even more authority and discretion that is not without corresponding cost to Americans’ civil liberties.

The prosecutor has broad, almost unlimited, discretion to file criminal charges and prosecute criminal cases and may be zealous in his pursuit of convictions of those who violate the law. Except for protection afforded the suspect under the Fourth and Fifth Amendments to the Constitution and the ethics rules described below, the investigatory and charging stages are generally devoid of rules governing the activities of the prosecutor. There is not a great deal of oversight to ensure that the prosecutor observes guarantees provided the suspect under the Constitution, with the United States Supreme Court opining that it is generally inappropriate for the courts to review prosecutorial decisions.\textsuperscript{331} Where a dispute arises, the dispute is decided by a contest, with the one who has more power, typically the prosecutor, being the winner.

One might wonder whether it is advisable not to place more specific limitations on the prosecutor’s authority, given the temptation of an individual to abuse authority and use the position for personal gain, to say nothing of the potential that the prosecutorial system might be caught up in a contagion of fear, such that prosecutions become politi-

\textsuperscript{327} Id. at 5-6.
\textsuperscript{328} Id.
\textsuperscript{329} Id. at 7-8.
\textsuperscript{330} Id.
Criminal defendants have attempted to limit the prosecutor’s power by attacking prosecutorial immunity, bringing allegations of prosecutorial vindictiveness, and subjecting the prosecutor to discipline for violating ethics rules, all with scant success. Prosecutorial immunity has been shown to provide the prosecutor wide latitude and shields the prosecutor from adverse action.\textsuperscript{332} Prosecutorial vindictiveness has not provided much protection for a criminal defendant.\textsuperscript{333} Other responses to prosecutorial misconduct include dismissal or retrial of a case,\textsuperscript{334} bar discipline, although rarely resulting in much more than a reprimand,\textsuperscript{335} and sanction by a presiding judge.\textsuperscript{336}

In perhaps the most famous description of the prosecutor’s difficult role, Justice Jackson stated, “The qualities of a good prosecutor are as elusive and as impossible to define as those which mark a gentle-


\textsuperscript{333} Blackledge v. Perry, 417 U.S. 21, 27 (1974) (finding that “the Due Process Clause is not offended by all possibilities of increased punishment upon retrial after appeal, but only by those that pose a realistic likelihood of ‘vindictiveness’”). The Court seriously limited the success of claims of prosecutorial vindictiveness pretrial in cases from 1978 and 1982. Bordenkircher v. Hayes, 434 U.S. 357, 365 (1978) (finding no necessity to limit the prosecutor’s threat of bringing more serious charges when Hayes decided not to plead guilty); United States v. Goodwin, 457 U.S. 368, 384 (1982)(“[t]he possibility that a prosecutor would respond to defendant’s pretrial demand for a jury trial by bringing charges not in the public interest that could be explained only as a penalty imposed on the defendant is so unlikely that a presumption of vindictiveness certainly is not warranted”).


man.” Justice Jackson recognized that the prosecutor must serve society while avoiding decisions based on self-interest. “A sensitiveness to fair play and sportsmanship is perhaps the best protection against the abuse of power, and the citizen’s safety lies in the prosecutor who tempers zeal with human kindness, who seeks truth and not victims, who serves the law and not factional purposes, and who approaches his task with humility.”

B. The Prosecutor and Legal Ethics

The American Bar Association Model Rules of Professional Conduct recognize the various roles assumed by the attorney, as “a representative of clients, an officer of the legal system and a public citizen having special responsibility for the quality of justice” and allude to the attorney’s self-interest in “earning a satisfactory living” even while “remaining an ethical person.” An attorney is guided by the rules, “substantive and procedural law,” and “personal conscience and the approbation of professional peers.” The attorney is to be “a zealous advocate on behalf of a client” but that requirement is tempered by the condition that the “opposing party is well represented.”

The rules view the various roles of the attorney as “usually harmonious” but recognize that certain conflict may arise. “In the nature of law practice, however, conflicting responsibilities are encountered. Where the conflict cannot be resolved by specific provisions in the rules,

[s]uch issues must be resolved through the exercise of sensitive professional and moral judgment guided by the basic principles underlying the Rules. These principles include the lawyer’s obligation zealously to protect and pursue a client’s legitimate interests, within the bounds of the law, while maintaining a professional, courteous and civil attitude toward all persons involved in the legal system.

The aspirational goal of the rules is that the legal professional be

[338] Id.
[339] MODEL RULES OF PROF’L CONDUCT, supra note 316 at Preamble.
[340] Id.
[341] Id.
[342] Id.
[343] Id.
self-regulating. “The legal profession’s relative autonomy carries with it special responsibilities of self-governance. The profession has a responsibility to assure that its regulations are conceived in the public interest and not in furtherance of parochial or self-interested concerns of the bar.”344 Failing that, the legal profession might lose its independence. “Neglect of these responsibilities compromises the independence of the profession and the public interest which it serves.”345

The ethics rules subject the attorney to discipline for conduct involving “dishonesty, fraud, deceit or misrepresentation” whether the conduct occurs inside or outside the practice of law.346 Although the rules are broad in encompassing attorney conduct even outside the practice of law, the drafters apparently thought this provision necessary to safeguard the integrity of the legal system.

Although the prosecutor’s discretion is vast, it is not without some limits; the prosecutor is bound by ethics rules, which paint in broad-brush strokes the ideals of promoting justice for society and fairness to the criminal defendant. The United States Supreme Court recognized the tension between a prosecutor’s inclination to convict and the rights to be accorded the defendant. “While [the prosecutor] may strike hard blows, he is not a liberty to strike foul ones.”347 Because the prosecutor is ethically bound to bring charges only if supported by probable cause and dismiss charges not so supported, a foul blow might include a decision to charge a particular defendant based on a mere suspicion of the defendant’s guilt. The prosecutor’s responsibility as a “minister of justice . . . carries with it specific obligations to see that the defendant is accorded procedural justice and that guilt is decided upon the basis of sufficient evidence.”348 The prosecutor is not obligated to pursue all charges supported by probable cause when it is determined that it is not in society’s interest to do so.

The ethics rules include a few specific limitations on prosecutorial discretion. The prosecutor is prohibited from making decisions to investigate or file charges based on “invidious discrimination”349 using factors such as the suspect’s “race, religion, sex, national origin, or po-

344 Id.
345 Id.
346 Id.
348 MODEL RULES OF PROF’L CONDUCT R., supra note 316 at 3.8 cmt. 1.
349 NAT’L DIST. ATTORNEYS ASS’N, supra note 318 at 4-1.4.
itical association, activities or beliefs." The prosecutor must be aware of potential conflicts of interest and must guard against making decisions that would give him a personal or political advantage.

The ABA ethics rules are concerned with the wellbeing of the attorney, the client, the public, and the legal profession; however, the overriding concern is for the wellbeing of the legal profession, with the hope that the legal profession can continue to be self-regulating rather than be regulated by the government. The rules recognize the inherent conflict of interest among the attorney, the client, the public, and the legal profession; although the interests of some of these players may align at times, there is a necessary tension among them. Under the rules, the interest of the client in winning and the interest of the attorney in maximizing profit must yield to the interest of the bar organization in maintaining itself as a viable, independent organization.

A terrorism case such as Mayfield or Shahzad presents a situation where conflicting responsibilities are encountered not easily resolved under the ethics rules. Each of the players in a terrorism case—the public, the government, the prosecutor, the judge, the alleged terrorist, and the criminal defense attorney—seeks to maximize its own happiness with varying degrees of empathy for the other players. The prosecutor is the agent of both the public and the government while the criminal defense attorney is the agent of the alleged terrorist. The agent's duty is to zealously represent the interest of the principle; however, this duty necessarily conflicts in some respect with the agent achieving maximum happiness. At times an agent with less than altruistic motivations may act in ways that undercut the interests of the principle.

What are the interests of the players in a terrorism case? The public wants to be protected against terrorist acts and is generally in favor of the government's use of anticipatory measures to stop terrorist activity; the government's interest ranges from protecting the public against terrorist acts, to furthering its agenda, to deterring others; the prosecutor is interested in winning, protecting the public, convicting a terrorist, furthering his career, garnering prestige; the judge's interests range from earning a livelihood, to seeing that justice is done, to advancing his career, to garnering prestige; the alleged terrorist is interested in freedom.

and possibly further his own personal agenda; and the criminal defense attorney’s interests range from earning a livelihood, to zealously representing the client, to winning, to advancing his career, to garnering prestige. In addition, one theory behind criminal prosecutions is that prosecuting one suspect may deter others from committing a similar offense.

Two typical conflicts occur in the legal system. The first occurs where the attorney’s self-interest has a negative effect on the opponent and the second occurs where the attorney’s self-interest has a negative effect on another, which negative effect has the potential of harming the legal profession, such as through underhanded behavior involving dishonesty, fraud, deceit or misrepresentation. The second type of conflict may include an attorney’s action that has a negative effect on the client. In our adversarial system, it is expected that one party wins and the other party loses, with this scenario repeated numerous times during an attorney’s career. Because the attorney has various degrees of career success, sometimes winning and sometimes losing, the first type of conflict involves what may be called “reciprocal costs,” with reciprocal costs “socially wasteful” where the costs are greater than the benefits. The second type of conduct involves “backlash concerns,” where there is a public outcry against attorney action that brings dispute to the legal profession. A number of ethics rules are in place to alleviate attorney action that might cause public outcry, such as dishonesty, fraud, deceit or misrepresentation or harassment of another. In addition, the attorney may violate the attorney’s duty to zealously represent the client where the attorney’s desire to maximize the attorney’s self-interest results in less than selfless attention to the needs of the client.

Most attorneys try to abide by the ethics rules and avoid self-interest; however, there are those who act on self-interest, unconsciously or consciously. After all, ethics rules are the fossils of prior inappropriate attorney conduct. In addition, each attorney has been shaped by numerous factors over a lifetime, many of which the attorney is unaware, which may cause the attorney to operate according to a bias of the way in which the attorney perceives a case. “[C]ognitive research

353 Id. at 353.
354 Id. at 350-51.
demonstrates that people systematically hold a set of cognitive biases, rendering them neither perfectly rational information processors, nor wholly random or irrational decision makers.\textsuperscript{355} One cognitive bias is “belief theory,” which appears to have been demonstrated powerfully in \textit{Mayfield}. In \textit{Mayfield}, the fingerprint analysts linked Mayfield with the latent fingerprint from the Madrid bombings and were adamant in maintaining the linkage theory of 100 percent identification between Mayfield’s fingerprint and the latent fingerprint even in the face of the Spanish National Police’s identification of the Moroccan perpetrators. Perhaps belief theory is at work when, once a prosecutor institutes a criminal charge, the prosecutor seems bound to pursue the criminal charge to conviction at all costs, even in the face of evidence of the suspect’s innocence.

Within the immense discretion accorded the prosecutor, there is a parameter of appropriate prosecutorial discretion surrounded by an area still within the prosecutor’s discretion but which is inappropriate. The prosecutor steps from the parameter of appropriate discretion into inappropriate discretion whenever the prosecutor loses sight of principles of justice and fairness. One of the reasons terrorist prosecutions can be so troubling is that the contagion of fear has such a powerful effect that a prosecutor can easily be moved from within the parameter of appropriate prosecutorial discretion to a place where the desire to convict at all costs takes over.

\textbf{V. Analysis}

There is increasing evidence that prosecutors have fallen victim to what Balkin and Levinson refer to as the National Surveillance State.\textsuperscript{356} This is a theory of constitutional development based on the nation’s response to the needs of “warfare, foreign policy and domestic law enforcement” following 9/11.\textsuperscript{357} Balkin and Levinson suggest that the September 11 attacks and the Bush Administration’s War on Terror accelerated America’s transition to a National Surveillance State by creating a parallel law enforcement structure that navigates around the traditional criminal justice system constrained by traditional civil liberties.


\textsuperscript{357} \textit{Id.}
By instituting rules for surveillance, apprehension, interrogations, detention, prosecution and punishment based on the executive’s power to conduct war, national security enforcement encroaches on and displaces the criminal justice system usually hallmarked by civil liberties protections, checks and balances, and oversight by independent actors, such as judges.\(^{359}\)

Warrantless domestic surveillance and actions outside statutory privacy protections, such as FISA, as contemplated by Congress in 1978, and telecommunications privacy laws, are actions by the executive branch contradictory to constitutionally guaranteed civil liberties. Consequently, these activities are also contrary to procedural protections afforded by criminal process. Historically, evidence derived from these practices, as well as evidence derived from coercive interrogations, cannot be introduced in ordinary criminal proceedings.

Arguing that the criminal justice system is outmoded and not sufficiently flexible to address the new national security issues that have arisen since 9/11, the executive branch created what amounts to a parallel structure that allows prosecutors “to treat dangers within the United States as matters of war and national security rather than matters of criminal justice.”\(^{360}\) Evidence not admissible in traditional criminal justice courts may be used in the parallel structure that is created.\(^{361}\) Returning to the traditional criminal justice system presents prosecutors with a significant disadvantage when they are no longer allowed to use evidence acquired at the expense of civil liberties.\(^{362}\) The prosecutors will be increasingly tempted to avail themselves of a system with less resistance, and perhaps more significantly, less accountability, that falls “under the aegis of national security rather than criminal procedure.”\(^{363}\) A result in part of the epidemic of fear and in part of the prosecutors’ zeal to win, the criminal justice system with its associated protections, processes and checks may morph into a system that is devoid of the same accountability.

Preventive, anticipatory prosecution is just one characteristic of the National Surveillance State.\(^{364}\) Public and private modes of surveil-
lance are integral components, as well. Electronic surveillance, loca-
tional tracking, data mining, surreptitious searches and information
analysis are all tools that the government has employed to exert social
control. Whether Balkin’s theory of a National Surveillance State is
accepted, the arrival of the conditions he describes is irrefutable and
rest in the hands of federal prosecutors as powerful tools at their dis-
posal.

The considerable expansion of prosecutorial power and discretion,
the increasing difficulty of challenging the prosecution’s use of surrepti-
tious surveillance evidence, the lack of oversight or accountability, and
the continuing national fear of terrorist threats present unparalleled op-
portunity for administrative misconduct. Unfortunately, there is evi-
dence that prosecutors are not immune from the temptation to act
without regard for both legal and ethical concerns. How much great-
er is the temptation given the current political climate, and what will be
the ultimate cost in terms of American citizenry and the citizen state?

The trustworthiness of the prosecutorial system “must rely ulti-
mately on the character, integrity, sensitivity, and competence of” the
prosecutors. Prosecutorial guidelines have the dual purposes of “ens-
uring the fair and effective exercise of prosecutorial responsibility by
attorneys for the government, and promoting confidence on the part of
the public and individual defendants that important prosecutorial deci-
sions will be made rationally and objectively on the merits of each
case.”

As more fully explained in the following section, the prosecutor
increasingly has gained more power over the years with the passage of
additional criminal statutes. Criminalizing more actions results in a
broader arena for the prosecutor, with new crimes available as the basis
for establishing probable cause for a search warrant or inducing coop-
eration from a suspect.
A. Overcriminalization

In many respects, the interests of the legislator and the prosecutor align. With the public’s call for tough law enforcement, the legislature garners positive press by passing additional criminal statutes and those statutes give the prosecution more flexibility in charging decisions. Any legislator not voting in favor of an anti-terrorist statute could be branded anti-democratic and could be held responsible for any future terrorist attack. The public’s conclusion is that the legislature is protecting society by addressing crime incidents lately in the news even if those incidents were previously adequately covered by criminal statutes already on the books. Voters may be more likely to re-elect a legislator who has been tough on crime. As far as the prosecution is concerned, additional convictions reflect well on the prosecution.

The growth of criminal law has been increasingly rapid over the last forty years. The prosecutor has gained increasingly more power over the years with the passage of additional criminal statutes. Criminalizing more actions results in a broader arena for the prosecutor, with new crimes available as the basis for establishing probable cause for a search warrant or inducing cooperation from a suspect. In the sixteen years between 1970 and 1996, Congress passed more than four tenths of the federal crimes passed since the Civil War, with more activity in even number years, which are election years. State legislatures and Congress continue to add to criminal statutes while rarely repealing criminal statutes, with this phenomenon so frequently noted that it has become known as a “one-way ratchet.” As of the close of 2007, there were approximately 4,450 federal crimes on the books, an increase of 452 crimes since 2000. Since 1980, the average rate of passage of federal criminal statutes has been level, with Congress creating at least fifty new federal crimes annually; that means that each ten years has resulted in an additional 500 acts made crimes.

Because terrorism is a central component of the national agenda,
the executive branch has successfully justified innumerable expansions of authority. The nation, our congressional leaders, and the judiciary have acquiesced to the President's requests, in part as a reaction to the fear wrought from terrorist attacks on American soil and the exploitation of fear by the country's administration. The belief may stem from the idea that 9/11 could have been prevented if the government had had more information, and this justifies the government's expanded information gathering capabilities, including access to what would otherwise be considered within the privacy realm. The idea that terrorism is preventable further serves the executive's push for additional allowable activities. It is in the government's best interest to promote this idea because it also guarantees the continued increased funding for the law enforcement and intelligence communities. "[A]gencies have both promoted the idea that they can prevent threats from crystallizing into anything more concrete, and at times exaggerated the reality of threats in order to secure their own continued existence."

Whether due to the realities of prevention or the exaggeration of reality, one outcome of the efforts of the executive branch is the increased powers among traditional law enforcement entities, including the Department of Justice (DOJ). These agencies have received new powers that have long been on their wish list, both for antiterrorism efforts and for ordinary law enforcement purposes. In this respect, law enforcement actions become another component of the collective reaction to the fear of terrorism, but these agencies also promulgate the sentiment, benefiting from its continued generation. Perhaps, the greatest evidence of the increase in federal law enforcement's power is the almost unfettered discretion of federal prosecutors. Because of the events of 9/11 and our responses to those events, a new criminal process is emerging, and although it is designed to assist in the War on Terror, its application is not restricted to antiterrorism efforts.

According to a Center on Law and Security report, in the ten years following 9/11, the DOJ's terrorism prosecution efforts are characterized by "a heavy reliance on preventive law enforcement, an increasingly aggressive use of material support statutes, and a high conviction rate" of eighty-seven percent. For example, the crime of material

---

378 See Parry, supra note 89, at 782.
support to terror groups can bring with it a fifteen-year prison term.\textsuperscript{380} During the Obama presidency, the number of indictments almost doubled from the Bush presidency average of twenty-seven annually and there was a higher proportion of cases with serious charges.\textsuperscript{381}

Terrorism cases over the years have involved a substantial use of informants. "Since 9-11, 41\% of terrorism cases have involved an informant."\textsuperscript{382} The new presidency has also been marked by an increased use of informants, amounting to almost fifty percent of terrorism cases, with sting operations comprising at least fifteen percent of the informant cases.\textsuperscript{383} "Since 2009, the federal government has expanded its use of aggressive and often controversial investigations, whereby a confidential informant or undercover officer makes contact with a potential terror suspect and assists him in the planning of an attempted terror crime."\textsuperscript{384}

Although criminal charges are based on more than 150 federal statutes,\textsuperscript{385} the most common charge over the ten years has been general criminal conspiracy under 18 U.S.C. § 371. In the last three years covered in the report, material support charges under 18 U.S.C. §§ 2339A, 2339B have been increasingly frequently used in prosecutions,\textsuperscript{386} with crimes under those two statutes becoming the second and third most commonly charged.\textsuperscript{387} "Since 2007, material support has gone from being charged in 11.6\% of cases to 69.4\% in 2010. In 2011 so far, 87.5\% of cases involve a material support charge."\textsuperscript{388}

The United States Supreme Court upheld the constitutionality of § 2339B in Holder v. Humanitarian Law Project,\textsuperscript{389} refusing to separate the culpability of support for non-violent activities from support for violent activities.\textsuperscript{390} "Section 2339A requires that the defendant knows or intends the material support provided will be used to prepare or carry out


\textsuperscript{380} Id. at 4.
\textsuperscript{381} Id. at 2.
\textsuperscript{382} Id. at 26.
\textsuperscript{383} Id. at 4.
\textsuperscript{384} Id. at 26.
\textsuperscript{385} Id. at 27-31.
\textsuperscript{386} Id. at 13-14.
\textsuperscript{387} Id. at 13 Figure 12.
\textsuperscript{388} Id. at 19 (emphasis in original).
\textsuperscript{389} Holder v. Humanitarian Law Project, 130 S. Ct. 2705, 2731 (2010). See supra notes 82, 88 and accompanying text.
\textsuperscript{390} 130 S. Ct. at 2727.
a violation of certain sections of the criminal code." Section 2339B marries a "broad scope of activities that constitute material support with the lack of specific intent", thus, under this statute "any knowing material support for a foreign terrorist organization, whether intended to support illegal activity or not, can result in prosecution for very serious terrorism charges and in lengthy prison sentences." The new trends in terrorism prosecution with the Obama presidency may be a cause for concern with "the weakened presumption of innocence when it comes to terrorism suspects, the excessive reliance on overly broad material support statutes, and the narrow line between legitimate FBI preventive tactics and entrapment." The National Security Division of the DOJ issues statistics on unsealed terrorism related convictions. The division tracks convictions related to terrorist acts planned or committed outside the territorial jurisdiction of the United States as well as within the United States. Criminal cases arising from the division’s investigations are divided into two categories, distinguished by the level of coordination and monitoring required by the Counterterrorism Section of the National Security Division or its predecessor in the Criminal Division. Category I cases include violations of federal statutes that are directly related to terrorism and are utilized regularly in terrorism matters. Category II cases include defendants charged with violating a variety of other statutes where the violation involves a link to terrorism but may fail to qualify as a terrorist act. Category II offenses include unlawful activity such as fraud, immigration violations, false statements, perjury, obstruction of justice, drug charges and general conspiracy charges. The DOJ reports "using Category II offenses and others is often an effective method – and sometimes the only available method – of deterring and

---

391 CTR. ON LAW & SEC., supra note 379, at 21.
392 Id.
393 Id.
394 Id. at 5.
396 Id. at 1.
397 Id.
398 Id.
399 Id.
400 Id.
disrupting potential terrorist planning and support activities." The statistics reported reveal that the number of defendants charged with Category II offenses is just over one and one fifth times the number of defendants charged with Category I offenses.

Identifying alternative charges for criminal behavior is not a prosecutorial practice born of the attacks on September 11. It is hardly a novel mechanism for achieving convictions. In determining what charges to file, the prosecutor in effect assumes legislative and adjudicative functions. Power in criminal law has migrated from the courts to the prosecutor both because of the wide range of criminal statutes and the high percentage of criminal charges that result in guilty pleas.

Although one would suppose that this is a recent phenomenon, Justice Robert H. Jackson was cognizant of it at least seventy years ago.

With the law books filled with a great assortment of crimes, a prosecutor stands a fair chance of finding at least a technical violation of some act on the part of almost anyone. In such a case, it is not a question of discovering the commission of a crime and then looking for the man who has committed it, it is a question of picking the man and then searching the law books, or putting investigators to work, to pin some offense on him.

Both the Center on Law and Security and DOJ's National Security Division reported on terrorism-related convictions and include data indicating a considerably larger number of individuals prosecuted for crimes other than violations of our nation’s terrorism statutes. These prosecutions are for offenses that may be considered “general” or “ordinary” crimes. At every possible opportunity, the administration emphasizes its efforts to identify terror plots, arrest domestic and international terrorists, and convict those indicted. No occasion is spared to inform the public of the threats against it or the government’s success at thwarting harm, further justifying the grant of increased power to the executive.

The prospect that the government has adopted a policy of prosecut-

---

401 Id.
402 Id. at 2.
404 Id. at 673.
405 See supra note 321, at 19.
ing suspected terrorists at the earliest available opportunity has generated criticism from both the civil liberties and national security perspectives, with the former contending that we risk prosecuting dissenting thought uncoupled from culpable action and the latter contending that such a policy would sacrifice the benefits of additional intelligence and evidence gathering.406

There is hardly any debate over the harm prevented from lawful intelligence gathering that leads law enforcement officials to the accurate identification of those individuals who intend to cause serious injury and destruction to others. The prosecutions that stem from the evidence gathering and identification are, likewise, laudable. Researchers, practitioners, observers, and others are voicing concern, however, about the harm that may be caused from the administration’s preventive efforts and the shift in the balance of power that significantly favors the executive. This shift in power to the executive is coupled with an epidemic of fear that the administration simultaneously “fights against” and spreads creating an environment where prosecutors may be seeing “ghosts,” so to speak, of terrorists. In other words, whether it is fear of harm, an overzealous desire to win at all costs, a need to justify expanded authority (and perhaps the further expansion of authority), the opportunity to get more criminals off the street, or some combination of these motivations, prosecutors’ policy of anticipatory prosecution is leading to a high percentage of convictions at the expense of constitutionally guaranteed rights and liberties, not the least of which is privacy.

It is the premise of this paper that a dangerous cycle is developing. It begins with actual terrorists and their attempts to coerce behavior through tactics that generate pervasive fear. Then, through slight of hand, almost like a carnival trick, the administration pretends to quell the fear, all the while concurrently acting to maintain fear’s presence in the minds of the nation and, in particular, its two sister branches of government. As long as the sense of fear is palpable, continued expansive authority is not only justified but welcomed. Now, armed with new authorities the President is equipped to better battle threats of terror. Commanding military-type, intelligence gathering tactics on domestic soil of American citizens enables the administration to keep a watchful

eye on the nation. It is a foregone conclusion that this watchful eye will locate conduct that may be interpreted as unlawful, given the number of statutes which criminalize behavior. Whether the behavior actually qualifies as criminal, there is likely to be a statute under which the conduct could be deemed criminal. The executive now has the authority to institute ongoing secret surveillance of individuals to determine whether their conduct may become criminal, anticipate the future criminal behavior, arrest the individuals and prosecute them pursuant to statutes in an effort to stop harm before it occurs. In so doing and by continually keeping the public apprised of its detection, the administration simultaneously alleviates fear and lets the public know that it has much of which it should be afraid. And, the cycle continues.

Many aspects of this cycle or contagion of fear are topics that have been contemplated, discussed and warrant further consideration. This paper, however, limits its examination to the role privacy, or the dissipation of privacy, plays in the administration’s antiterrorism agenda. The authors suggest the expansive intelligence gathering practices granted to the President serve as a primary enabling factor in the continuation of the cycle described above. As a point in fact, the post-9/11 amendments to FISA empower the executive branch to conduct counterintelligence surveillance, including wiretapping, data mining and sneak-and-peek searches, of Americans without Fourth Amendment probable cause and without ever informing the targets of the surveillance efforts. Furthermore, with one exception, the government has successfully hidden behind its state secret privilege and secured protection from revealing the particulars related to its surreptitious surveillance, allowing the administration to continue the secrecy. Both the legislative branch and the judicial branch have sanctioned these activities, notwithstanding their obvious conflict with the Constitution and the resulting deprivation of individual liberties.

B. Criminal Law on the Books and as Prosecuted

Overcriminalization, together with the power of the prosecutor

under FISA and the contagion of fear of terrorism is a lethal combination leading to an almost necessary loss of protection for civil liberties. "[T]he Department must shift its primary focus from investigating and prosecuting past crimes to identifying threats of future terrorist acts, preventing them from happening, and punishing would-be perpetrators for their plans of terror."  

With the number of criminal statutes and their broad reach, many of which statutes cover behavior not commonly thought to be illegal, it is fairly easy for one to commit a felony without realizing it. The logical consequence of the preceding sentence would be for one to live in peril of being sanctioned at any moment for some type of violation. However, there is a gap between the law as reflected in statutes and court decisions, on one hand, and the law as enforced. In many instances, "formal law is neither behaved nor enforced. . . . Those charged with enforcing the law frequently exercise their discretion in a manner that enforces norms instead, just as those charged with complying with it frequently exercise their discretion in a manner that complies with norms instead." The typical individual thinks of himself as law-abiding and acts in conformance with what the individual believes to be legal even though the individual may be in technical violation of a criminal statute. In fact, there may be a public outcry where a police officer strictly enforces the law for a minor violation.

An easy-to-understand example of the distinction between the law on the books and the law as enforced is speed limits. On the highway, the posted speed limit may be sixty-five, yet traffic is traveling at seventy-five or even eighty. One reason for the variance between the posted speed limit and speed at which the traffic is moving is that the motorist knows that a police officer usually gives motorists a ten miles or so over the speed limit leeway free from being subject to ticketing. In turn, a police officer who clocks the speed of a vehicle at seventy-five or below will probably not pull over the vehicle but a police officer is likely to pull over a vehicle clocked at eighty or more. Although the posted speed limit is sixty-five, the norm has increased the speed limit

---


by ten miles, with both the motorist and the officer acting as if the posted speed limit were seventy-five.

The posted speed limit remains sixty-five and, because a vehicle traveling at sixty-seven violates the speed limit, a police officer is entitled to stop and ticket a motorist traveling two miles per hour over the speed limit. If this happens, this means that the officer is sanctioning the motorist for driving at a speed that both of them typically consider to be "legal"—that is within their norms. There are several reasons an officer may choose to stop a motorist exceeding the speed limit by a mere two miles. One reason is to forestall the parameter of acceptable deviance from continuing to enlarge. Over time and without some attempt to reign in vehicle speed, the variance between the posted speed and traffic flow may increase from ten miles to eleven to fifteen miles and beyond. Another reason to stop the vehicle traveling two miles over the speed limit is that the officer has targeted the driver of a particular vehicle and the traffic violation gives the officer an excuse to stop the vehicle and question the driver. A minority motorist is likely to complain of racial profiling—that the officer's alleged reason for stopping the vehicle was a pretext for stopping the vehicle for some other reason, perhaps an unfounded suspicion that the officer might uncover evidence of some illegal activity. However, in 1996 the United States Supreme Court decided that the Constitution does not prohibit a police officer pulling over a vehicle for a traffic violation even if the alleged traffic violation is a pretext for an impermissible factor such as race.411

Professor Edwards coined the term "parameter of acceptable deviance" to mean behavior that is technically in violation of a legal norm but that is not customarily treated by law enforcement as a violation.412 In the above example, the parameter of acceptable deviance is between sixty-five and seventy-six miles per hour. The public may adopt the parameter of acceptable deviance as the outer limit of what is legal and assume that behavior within the parameter of acceptable deviance will not be sanctioned. This means that behavior falling within the pa-

411 Whren v. United States, 517 U.S. 806, 813, 819 (1996). The Court stated: "We of course agree with petitioners that the Constitution prohibits selective enforcement of the law based on considerations such as race. But the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause, not the Fourth Amendment." Id. at 819.

412 See supra note 410, at 56.
ter of acceptable deviance would not be treated by law enforcement as a violation and ordinarily would not be recognized by the public as a violation subject to formal sanction, while behavior falling outside of the parameter of acceptable deviance would be subject to law enforcement sanction and the public would recognize such sanction as appropriate.

A police officer whose norms coincide with the parameter of acceptable deviance may refuse to stop a vehicle traveling between sixty-five and seventy-six because the officer does not view a vehicle traveling at that speed as violating the traffic ordinance; in other words, where the motorist’s perceived parameter of acceptable deviance coincides with the officer’s perceived parameter of acceptable deviance, one might speak of a “strong social fidelity”\(^\text{413}\) between the motorist and the officer. The public’s identification with the parameter of acceptable deviance may be strong enough that the public may protest an attempt to sanction behavior within the parameter of acceptable deviance. In that circumstance, the public is attempting to make the law as enforced conform to the public’s parameter of acceptable deviance. In effect, the parameter of acceptable deviance is put forward as a defense to strict enforcement of the traffic ordinance. An officer who enforces the law against a person of privilege where the person’s behavior was within the parameter of acceptable deviance may be subject to a claim that the enforcement was politically motivated. “Tellingly, it has become standard practice for political and business elites accused of crimes to complain that they are the victims of politically motivated prosecutors who have ‘criminalized’ normatively acceptable political and business practices.”\(^\text{414}\) Depending on the strength of the social fidelity between the public and the elite, the public may or may not support the political or business elite who claims unfair selection for prosecution based on the political or personal prejudice of the prosecutor towards the elite. The public probably would not support the elite where the public views the elite as receiving special treatment not available to the public.

Even so, the public may excuse enforcement of the speed limit within the parameter of acceptable deviance as long as there is some other justification that makes the officer’s action appear reasonable to

\(^{413}\) Id. at 74.

\(^{414}\) Id. at 76.
the public, such as apprehending a motorist suspected of perpetrating a serious crime. The public may be more willing to make an exception to its norms where the majority of the public has some reason to differentiate itself from the suspect, such as viewing the suspect as distinct from the majority because of race or ethnicity. What if in that situation the motorist is innocent of the crime but is of the same minority race or ethnicity as the suspect the police are targeting? In all likelihood, there would be no outcry from the public in general but there very well may be an outcry from the affected minority; this would be evidence of a weak social fidelity between the minority and the officer.

One parallel between the violation of a traffic ordinance and a more serious offense is that a parameter of acceptable deviance exists for a crime as it does for a traffic violation, with a gap between the crime on the books and the crime as prosecuted. A second parallel is the suspect’s claim of being selectively prosecuted based on race, ethnicity, politics, or negative personal bias. One distinction between violation of a traffic ordinance and commission of a crime is the moral stigma that attaches to a criminal defendant but that does not normally attach to a violator of a traffic ordinance. In contrast to a traffic violation, a crime carries a flavor of moral culpability for an action falling within the perimeter defined by the criminal statute but outside the parameter of acceptable deviance. However, the crime is more easily excused and does not carry the same moral culpability where the action falls within the parameter of acceptable deviance. The parameter of acceptable deviance can expand and contract over time, dependent on public norms.

The breadth of criminal statutes juxtaposed against budgetary limits on their enforcement necessarily means that it is impossible to prosecute all those who are guilty of violating criminal statutes and the prosecutor must exercise discretion in deciding which suspects to prosecute. As stated earlier, the prosecutor has immense discretion in deciding who to prosecute and what criminal charges to level. One would think that the public would want tax dollars spent to take the most dangerous individuals off the streets or to deter others from committing the same crime so as to make the best use of limited resources.

A criminal defendant would understandably be upset to learn that someone who was similarly situated was not selected by the prosecution while the defendant was, but selecting one suspecting from a number of suspects and prosecuting that individual is not unconstitution-
A selective prosecution claim, even if based on impermissible factors such as race, ethnicity, or religion is an extremely difficult one to prove because the suspect must pursue an Equal Protection claim; to be successful on such a claim, the suspect must “show both that the passive enforcement system had a discriminatory effect and that it was motivated by a discriminatory purpose.” Even if a prosecutor seems to be overzealous with respect to a particular suspect, the suspect will make little headway with a claim of prosecutorial vindictiveness, and the prosecutor is protected by prosecutorial immunity when acting as an advocate.

The public’s priorities may cause the prosecutor to focus on a particular category of offense, such as those offenses the prosecutor can claim are related to terrorism. Late in 2013, the public viewed protecting the country from terrorism as the nation’s top priority (83%), followed closely by the priority of protecting Americans’ jobs (81%). As far as President Obama’s approach to foreign policy and national security issues, 51% rate the president as not sufficiently tough, 37% rate the president as demonstrating a sufficient degree of toughness, and 5% rate him as overly tough. When questioned concerning the terrorists capability to spear a major attack, a substantial majority viewed that threat as similar (36%) or greater (34%) than the September 2001 attack.

The accused may claim that the prosecution is pretextual, that is there is an underlying reason for the prosecutor bringing the charge other than the acts constituting the charged offense, such that the prosecutor’s motivation is based on one or more characteristics of the suspect rather than the alleged offense committed by the suspect. Thus, there is a “pre-text, a story that precedes the actual criminal charge and explains the decision to exercise federal jurisdiction.” However, in

---

417 See supra note 333, and accompanying text.
418 See supra note 332, and accompanying text.
420 Id. at 13.
421 Id. at 31.
each case there is an explanation of the prosecutor’s decision to bring a particular federal charge against a particular individual. The premise here is that the prosecutor’s decision is less than appropriate in certain cases, with the difficulty lying in distinguishing those cases in which prosecutorial discretion is exercised appropriately from those in which the exercise is inappropriate.

One can easily identify *Mayfield* as falling within the category of inappropriate use of prosecutorial discretion because Mayfield was innocent of the charged offense, Mayfield was targeted because he is Muslim, tying the fingerprint evidence from the Madrid bombing meant that Mayfield was suspect, and the prosecutor continued to pursue Mayfield as a suspect even after it was clear that the latent fingerprint did not belong to Mayfield. Mayfield is also an example of pretextual prosecution because in the government’s agenda of fighting the War on Terror, it seems that the latent fingerprint from the Madrid bombing was matched to Mayfield because Mayfield is Muslim and the prosecutor was all too eager to apprehend a dangerous terrorist.

In contrast to Mayfield, federal prosecution is usually based on sufficient reliable evidence to convict; however, the charge giving rise to an allegation of pretextual prosecution may fall either within or without the parameter of acceptable deviance. Edwards views enforcement of a law within the parameter of acceptable deviance based on an impermissible factor, such as racial profiling, a “system breakdown” and suggests that law enforcement in this type of instance be reviewed under a standard of “heightened scrutiny.” It stands to reason that the system may also be broken where the prosecutor targets someone as a suspect based on an impermissible factor even if the suspect’s acts technically fall within the statutory definition of a crime where the acts fall outside the parameter of acceptable deviance.

The smooth functioning of the American criminal justice system assumes public confidence in the government and in the system. Criminal law, like other areas of the law, has substantive and procedural aspects, with its substance largely based on criminal statutes and case law interpretation and procedure entailing the process by which crimes are investigated and suspects are moved through the system. Public confidence is based both on the public being provided with the knowledge of the acts constituting crimes and a perception that the procedure used

423 See supra note 410, at 84, 88.
to enforce criminal law is fair. "[T]he moral stigma of the criminal sanction will attach in the long term only if the public is persuaded both of the moral culpability of the proscribed conduct and of the reliability of the adjudication of the defendant's guilt."424

The public's trust in the government is at one of the lowest levels in the past fifty years, with nineteen per cent saying that they can "just about always" trust the federal government or have trust in the government "most of the time."425 A half century ago (1958) seventy-three per cent of the public said they could trust the federal government "just about always or most of the time."426 A majority of the public (55%) is frustrated with the federal government, while a little under one-third (30%) says it is angry with the government and another a little over one-tenth (12%) says it is "basically content" with the government.427

The public's general distrust with the federal government contrasts with the public's trust in the federal government to protect the public against terrorism. When asked whether the government threatens the individual's rights or freedoms, fifty per cent said no (slightly lower than the fifty-four per cent of October 2003), thirty per cent characterized the government as a "major threat" (a significant increase from the eighteen per cent of October 1997 and higher than June 2000's previous high of twenty-three per cent), and seventeen per cent see the government a "minor threat." Within two months of 9/11, sixty-seven per cent said no, fourteen per cent said the government presented a major threat, and fourteen per cent said the government presented a minor threat.428

CONCLUSION

The federal government was designed with separation of powers among the three branches so that if one branch usurped power, it could

427 See supra note 425.
428 The Pew Research Ctr. For the People & the Press, supra note 426, at 63.
be checked by the other two branches. The fear of terrorism stresses separation of powers and throws the three branches out of balance. In 1952 during the Korean War, President Truman seized steel mills under guise of national security. The United States Supreme Court found that the President lacked such power.\textsuperscript{429} Allowing such power in the hands of the President would have had a deleterious effect on separation of powers. "[E]mergency powers are consistent with free government only when their control is lodged elsewhere than in the Executive who exercises them."\textsuperscript{430}

The year prior to President Truman’s steel mills seizure, Associate Justice Robert H. Jackson warned that the country must not be tempted by a wartime mentality of fear to break with the rule of law. "The essence of liberty is the rule of law. . . . Because liberty cannot exist apart from the impartial rule of law, it is vulnerable to wartime stresses, for then the rule of law breaks down. The same passions and anxieties may result from a long period of tension which may be almost as demoralizing as actual war."\textsuperscript{431} He foresaw that, in a rush of patriotism during wartime, the country might easily forego some of its most cherished civil liberties in the interest of national security. "Wartime psychology plays no favorites among rights but tends to break down any right which obstructs its path."\textsuperscript{432} He added: "It is easy, by giving way to the passion, intolerance and suspicions of wartime, to reduce our liberties to a shadow, often in answer to exaggerated claims of security."\textsuperscript{433}

This same wartime psychology that Justice Jackson had warned about arose shortly following September 11, 2001, when President Bush announced a War on Terror. "Our war on terror begins with Al Qaida, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped, and defeated. . . . We will take defensive measures against terrorism to protect Americans."\textsuperscript{434} Although it was not a declaration of war in the traditional sense, President Bush correctly gauged that the sentiment stirred up in the country would allow the executive branch to spearhead actions, perhaps at the

\textsuperscript{429} Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 588-89 (1952).
\textsuperscript{430} Id. at 652 (Jackson, J., concurring).
\textsuperscript{432} Id. at 112.
\textsuperscript{433} Id. at 116.
\textsuperscript{434} Bush, supra note 1.
expense of civil liberties, difficult in peacetime. President Bush’s analogy to the country being at war was not in any way new in that it was one used in the prior sixty years when tackling a variety of targeted social problems. However, the 9/11 attach was a defining moment that allowed a shift in power to the executive branch and away from the judicial branch and Congress.

The war analogy has its roots in St. Augustine’s Just War Theory from the fifth century in which conflict became righteous, buoyed by religious authority. The communist red scare of the 1950s is similar to the terrorist scare of the 2000s in that each created a fear in the public of a persistent but ill-defined force that endangers the stability of society. President Bush stated, “Freedom and fear, justice and cruelty have always been at war, and we know that God is not neutral between them. Fellow citizens, we’ll meet violence with patient justice, assured of the rightness of our cause and confident of the victories to come.”

With the War on Terror, power swung to the executive branch and away from the other two branches of government; the new emphasis on national security permitted the executive branch more leeway under the guise of state secrets in engaging in secret programs such as the TSP.

After 9/11, Congress rushed to pass legislation directed at terrorist activities, which contained fewer built-in safeguards because of the presumed immediacy of the threat. The executive branch took the lead in implementing the new legislation, often largely in secret, under the guise of national security. The courts were loath to second guess the executive branch and the power of the courts was weaker under the anti-terrorist legislation. Although the 9/11 emergency situation led the judicial and legislative branches to cede power to the executive branch, this imbalance may be dangerous over time. “The accretion of dangerous power does not come in a day. It does come, however slowly, from

435 Since World War II, “[w]ar infected language, not only as a metaphor for efforts to ameliorate major social problems but also in the everyday idioms of social life, from sport to business. The United States declared war on cancer, crime, drugs, and poverty; military terms became part of the common vocabulary . . . .” Richard H. Kohn, The Danger of Militarization in an Endless “War” on Terrorism, 73 MILITARY HIST. 177, 191 (2009).


437 Bush, supra note 1.

438 See supra notes 207-14, and accompanying text.
A CONTAGION OF FEAR

the generative force of unchecked disregard of the restrictions that
cense in even the most disinterested assertion of authority.” Histori-
cally, the press has been a check on government abuse of power and,
with FISA, may be the only check on the executive branch.

FISA has been on the books for over thirty years but was rarely in
the news until 2001. The Patriot Act and subsequent amendments
shifted additional authority from the judicial to the executive branch,
with few limits on the prosecutor who was seen as instrumental in se-
curing national security. Power may have dangerously shifted to the
executive branch, with the other two branches acquiescing. The public
may generally assume that the protections under FISA are similar to
those under usual criminal investigation where evidence is obtained af-
fter obtaining a warrant based on probable cause and the defendant has
a right to be notified of any evidence the prosecution has. For exam-
ple, FISA requires the court to take facts as presented and without in-
dependent investigation. FISA allows prosecutors to camouflage fish-
ing expeditions under protection of national security and state secrets.
The executive branch is throwing out a wide net. The combination of
far-ranging criminal statutes and FISA allows the prosecutor to secure a
conviction. The prosecution abuses FISA and our privacy rights to
calm our fear of terrorism. The prosecution extorts guilt at the expense
of the truth. The combination of FISA and prosecutorial abuse seem-
ingly results in a feeling that it is better an innocent person be convicted
than a terrorist go free.

Invocation of the Just War Theory in support of executive branch-
led government surveillance did not end with President Bush, with
President Obama relying on the Just War Theory as well in the coun-
try’s continued War on Terror. Perhaps because President Obama was
trained as an attorney, the President was careful to note a legal basis for
executive branch action in a major speech just two weeks before the
first Snowden disclosure. “Moreover, America’s actions are legal. . .
Within a week, Congress overwhelmingly authorized the use of force. . .
So this is a just war—a war waged proportionally, in last resort, and in
self-defense.” In the speech, the President emphasized the national

439 Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 594 (1952) (Frankfurter, J., con-
curring).

440 President Barack H. Obama, Address at the National Defense University, WASH. POST
23/read-president-obamas-speech-on-the-future-of-the-war-on-terror.
security value of government surveillance at the risk of some loss of privacy. “[S]ome [measures taken], like expanded surveillance, raised difficult questions about the balance we strike between our interests in security and our values of privacy. . . . Much of our best counter-terrorism cooperation results in the gathering and sharing of intelligence . . . .” Government surveillance technology continues to evolve, as does the ways in which one communicates. “[W]e will have to keep working hard to strike the appropriate balance between our need for security and preserving those freedoms that make us who we are.” He added, “That means reviewing the authorities of law enforcement, so we can intercept new types of communication, and build in privacy protections to prevent abuse.”  

The patriotic atmosphere invoked with the Just War Theory can be dangerous in that it emerges at the confluence of almost unchecked prosecutorial power, sophisticated NSA surveillance capability, national security-motivated state secrecy, and little oversight by the judiciary or Congress. With the sophisticated surveillance capability comes an inherent potential for abuse and the government is naturally reluctant to give up any capability once acquired. Given human nature, there is a temptation to use technological capability to penetrate whatever privacy the average individual assumed he possessed, at least prior to the Snowden disclosures, to gather foreign intelligence information to prevent terrorist acts or perhaps to gain political or economic advantage.  

Government control and power are enhanced through knowledge gained through electronic surveillance, with the extent of information gathered known only in the executive branch; the tendency is to continue to gather as much information as possible without alerting the people from whom the information is gathered. National security is a powerful watchword that can be used to justify surveillance to prevent terrorist incidents, with a loosening of the protection normally afforded under the United States Constitution. Secrecy goes hand in hand with national security and the government will claim state secrets privilege to keep the nature of the surveillance, the information gathered, and the manipulation of the data from public view. None of this operation is transparent. With the cloak of state secrets, the government can claim that it is engaging in lawful activity without being troubled by oversight.

441 Id.
442 Id.
443 Id.
of any other branch of government nor being troubled by being held accountable. The government has unlimited discretion in conducting this type of surveillance, which garners the government a great deal of power, ripe for being abused.

There are similarities between the constant surveillance of Big Brother of *1984* and FISA surveillance in that under FISA the government can surreptitiously conduct surveillance of the suspect without the suspect able to discover the government surveillance. There are similarities between Kafka’s *The Trial* and FISA surveillance in that the individual discovers that the bureaucracy has made him a suspect, yet he is unable to discover the process to which he is subject nor the evidence the bureaucracy has against him. Consider the combination of a zealous prosecutor with political motives, arrogant law enforcement officers, someone conducting business in a foreign market, and the availability of a FISA court order. Someone who has been wiretapped will not know and will not have any way of discovering unless the government commits a misstep and reveals the wiretapping in some way. An individual’s access to the court system to correct errors of the executive branch is not meaningful if the individual does not know that the communications have been intercepted and, if the individual does know of the interception, has no access to the information. Given broad criminalization, innocent conduct can easily be interpreted as having a sinister motive.

Why should someone trust that the government is doing the right thing? The assumption is that the government is ethical and benevolent. It is necessary for the government to stay in power. It is easier emotionally to believe that suspects are guilty than that the government is corrupt. What are the circumstances that call for extraordinary measures? What should the limits be on the federal government? The government has power, with a grave imbalance between the power of the government and the people and the knowledge of the government and the people. An individual typically has a childlike trust that the government will do the right thing. How naïve is it to believe that the government is not tempted to use the information for an improper purpose? The typical innocent suspect, who believes this will never happen, has a psychological reaction of disbelief that the suspect is being investigated. Mayfield is an example of a typical innocent individu-

---

al. The case was egregious as demonstrated by the government paying two million dollars. A co-defendant may lie to receive a shorter prison term. The prosecution can threaten an indictment if someone refuses to testify. The prosecution may be politically motivated. If Mayfield could be prosecuted, so could another innocent individual.

The commonly-held presumption is that the average citizen is un-connected to any terrorism or illegal activity and there is no prosecutorial abuse that might cause the average innocent citizen to be the target of FISA wiretapping. “[P]opular notions that intelligence can provide a fail-safe mechanism have created false expectations as to just what intelligence can deliver.” Thus far, the stories of people who have been innocent FISA targets are well known to their families and immediate friends. In a few instances, such as Mayfield, the story of a person wrongly targeted for a FISA wiretap has travelled beyond the first degree of separation; however, the average citizen believes that everything possible should be done to stop terrorism. The fear of terrorism could be likened to an emotional stampede or epidemic. Consider the unintended consequences of FISA amendments in an atmosphere that any and all action is necessary to prevent terrorism.

One knowledgeable about terrorism could have anticipated the fervor leading to the quick passage of the USA Patriot Act and the pressure on the federal government to do whatever was necessary to combat terrorism. A terrorism expert might analyze the resulting legislation to determine where the balance is struck between national security and the individual’s privacy. One of the tools the government uses to combat the potential threat of terrorism is to conduct broad-ranging surveillance to collect information on those who might have terrorist tendencies. The USA Patriot Act provisions appeared necessary in the climate of fear that gripped the country after 9/11; however, the public may not be fully aware of the extent to which its civil liberties have been eroded in the process. The belief may be that 9/11 could have been prevented if the government had had more information, and this belief justifies the government gaining access to otherwise private conversation. The idea that terrorism is preventable serves the purpose of allowing government activity. It is in the government’s best interest to promote this idea because it guarantees the continued funding of the intelligence community within the government.

Gill & Phythian, supra note 377, at 103.
One might examine the relationship between federal law enforcement and FISA. The history of FISA legislation shows that the original intent of the legislation was to place certain limits on surreptitious tapping of conversations while legitimizing such intelligence gathering if undertaken in conformity with the legislation. Federal law enforcement was apparently able to operate within FISA strictures until the warrantless wiretapping following 9/11. An unsettling circumstance arises if federal law enforcement is determined to justify its existence by announcing its success in preventing terrorist acts and gathers wiretapped information with this goal in mind. The result may be that "the urge to act pre-exists the search for information, and the significance of what is collected will be judged in terms of its ability to support a chosen course of action rather than to inform it." 446

Government control can be based on knowledge gained through electronic surveillance without the awareness of the individuals whose communication is being monitored. The communication can be copied, digitally stored indefinitely, manipulated, and transferred around the world. The copied communication can be data mined to make inferences among otherwise innocent and widely disparate pieces of communication. Thus, innocuous bits of information can be combined with other information at the government’s disposal, possibly to create a reasonable suspicion of some type of activity that may be a prelude to a terrorist act. When viewed from a different perspective, this information might not appear to be so innocuous. Inaccuracies, errors, and unsubstantiated theories can creep into surveillance information, with the individual whose communication was surveilled unable to correct the information. The government has the potential to use the communication, once analyzed, against those whose communication was monitored as well as against those mentioned in the communication. A longitudinal record of one’s communication may be used as a tool to predict what someone will do in the future.

Given technological capabilities, federal law enforcement can easily gather evidence of a connection between two individuals. In fact, network analysis can provide evidence of a connection between a known terrorist and an individual with no terrorist leanings, who thus becomes a new terrorist target. Federal law enforcement can have wiretapping tapes in its possession documenting the connection be-

446 Id. at 33.
between a terrorist and an otherwise innocent individual; the difficulty lies in gauging the true implications of the connection. The paradox is that an innocent individual is more likely to be open in disclosing information and less wary of the way in which communication may appear to a law enforcement officer than a terrorist who is constantly on the alert for a conversation being taped. Thus, it may be easier to gather evidence on those who are not terrorists and extrapolate from that to find something that appears to be terrorist activity than it would be to gather evidence needed to foil a terrorist plot. Wiretapped information from an innocent individual may be construed by the officer to be direct evidence of the prelude to terrorist activity, while a terrorist's wiretapping conversations may appear to concern perfectly innocuous behavior where the terrorist is actively concealing the dangerous intent of the conversations.

There is a problem of false positives. An individual's actions may seem suspicious or questionable if viewed by a government agent intent on snuffing out terrorist behavior. A criminal case can be built against someone who is unaware of the potential danger of being accused of terrorist leaning. A case could be put together by a computer, which could create artificial connections or make it appear that there were ties that were not previously there. Statements can be taken out of context and used as the basis of proffers. What are we going to give up to stop terrorism? Our government terrorizes us into doing what it wants. How is this different than what a terrorist does? The fear of another 9/11 makes people willing to give up rights to ensure government can deal with terrorism. Prevention may in some instances be less costly than punishing after a crime has been committed but the invasion of privacy and loss of civil liberties is much more costly to society.

The American colonists harbored great mistrust of government monitoring and control, a suspicion borne largely of the colonists' experiences with the English monarchy, the British generalized searches and their writs of assistance.\textsuperscript{447} Hence, the Fourth Amendment's prescription against generalized searches and seizures is intended to abate unease and ensure "the right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."\textsuperscript{448} "[D]eep-seated uneasiness and apprehension that [surveil-
lance] will be used to intrude upon cherished privacy of law-abiding cit-
izens[449] are concerns that continue to pervade American thought and
supply disquiet not wholly without merit.

In three decades, legislation balancing Americans’ civil liberties
and America’s security has eroded, and the current legal trends indicate
little recovery as the United States’ attempts to improve national securi-
ty and tips the equilibrium in that direction. A consequence of this shift
is visible when we consider the evolution of federal surveillance prac-
tices with an emphasis on the current state of those practices after
9/11. Justice Robert H. Jackson recognized that “times of fear or hys-
teria” present special challenges in that it is especially in these times that
civil liberty may be at risk.450 As America reacts to fear wrought by the
terrorists and as well as the fear perpetuated by the administration, the
contagion demands that protection efforts grow ever more zealous,
Americans’ privacy guarantees diminish proportionately, increasing the
likelihood that more and more innocent citizens will fall victims to sur-
reptitious surveillance.

---

449 United States v. United States District Court for the Eastern District of Michigan, South-
er Division, 407 U.S. 297, 312 (1972).
450 Jackson, supra note 321, at 19.