

AIR WAR COLLEGE

AIR UNIVERSITY

**TECHNOLOGY, TERRORISTS, SURVEILLANCE**  
**AND**  
**THE RIGHT TO PRIVACY**

by

Kenneth M. Theurer, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

01 April 2007

*[Cleared for public release 6/7/2007, AU 07-197]*

## **DISCLAIMER**

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

# Contents

Certificate.....	i
Introduction.....	1
Technology and Terror.....	2
“Right to Privacy” versus “National Security”.....	3
Executive Power.....	4
Right to Privacy.....	5
First Amendment.....	7
Fourth Amendment.....	9
Surveillance—Current Legal Frameworks.....	11
Foreign Surveillance Conducted Overseas.....	12
Terrorist Surveillance Program.....	14
Foreign Intelligence Surveillance Act.....	16
Federal Wiretap Act.....	17
Privacy, Reasonable Expectations.....	18
Conclusion.....	21
Bibliography.....	24

## Introduction

Today, technology pervades every aspect of US society changing concepts of privacy and challenging the nation's legal system to keep pace with concepts the nation's forefathers never imagined. At the same time, technology has fostered the emergence and success of a new enemy, the non-state actor who recognizes neither the law nor national boundaries.<sup>1</sup> While US court systems have been flexing the "expectation of privacy" to address technological change,<sup>2</sup> they have been slower to recognize that societal changes like the advent of terrorism increase the need for government surveillance. As the legal system struggles to place new technology in the context of traditional notions of privacy, the system risks creating a legal safe haven where the nation's enemies operate with impunity. America's enemies, in essence, use US law, or "lawfare" as a defensive instrument of war.<sup>3</sup> Political leaders, rather than directly address the issue, have sought to remove the issue from public discussion and judicial review.<sup>4</sup> This paper addresses terrorist use of technology, the "right to privacy", current legal frameworks regarding surveillance, and whether it is time for a public reassessment of what constitutes a "reasonable expectation of privacy."

## Technology and Terror

Use of technology such as cellular telephones and the Internet allows terrorists to recruit, train, and execute operations against their enemies, including the United States. For example, recent news accounts are replete with examples of mysterious purchases of large numbers of

---

<sup>1</sup> David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future*, p. 188 ("Certain non-state actors are defined and exist as strategic players almost entirely due to cyberspace").

<sup>2</sup> *Kyllo v. United States*, 533 U.S. 37 (2001) (finding monitoring of thermal images a Fourth Amendment "search").

<sup>3</sup> Charles J. Dunlap, "The Role of the Lawyer in War: It Ain't No TV Show: JAGs and Modern Military Operations," 4 *Chi. J. Int'l L.* 479 (Fall, 2003) ("Lawfare is specifically the strategy of using, or misusing, law as a substitute for traditional military means to achieve an operational objective.").

<sup>4</sup> See e.g., James Risen & Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts", *N.Y. TIMES*, Dec. 16, 2005, at A1 (discussing the Terrorist Surveillance Program).

prepaid cell phones from multiple chain stores in various locations.<sup>5</sup> While many of the more sensational US cases have not resulted in prosecutions, use of cell-phones by terrorists remains a valid concern.<sup>6</sup> Disposable prepaid cellular telephones, with on-line registration, allow anonymous untraceable communication between terrorist cells. In Iraq, these same telephones are regularly used as remote triggers for improvised explosive devices. Prepaid cell-phones were instrumental in the 2004 Madrid train bombing that killed 191 people and resulted in a regime change in Spain.<sup>7</sup>

Like cell phones, the Internet and email provide an anonymous safe haven and tool for terrorists to conduct their operations. In large part, the September 11<sup>th</sup> attacks on the World Trade Center and the Pentagon were planned and coordinated by Al Qaeda cells both within and outside the US using the Internet.<sup>8</sup> “The September 11th hijackers made reservations via AmericaAirlines.com, exchanged e-mail via Yahoo!, and conducted online research about the effectiveness of crop-dusting aircraft as a means to disperse chemical agents.”<sup>9</sup> Today, more than 5,000 terrorist websites are present on the Internet, an increase of more than 50 times since prior to 1996.<sup>10</sup> The Internet allows terrorists to form a “leaderless resistance” sharing common ideology to promote their cause and plans.<sup>11</sup> Terrorist use of the Internet ranges from recruiting new members to conducting information operations such as transmitting video images of beheadings to inspire fellow terrorists and demoralize opponents. “How to Manuals” for suicide

---

<sup>5</sup> Anna Werner, “California Man Buys Nearly 3,000 Cell Phones,” Sep 8, 2006. *available at* [http://cbs5.com/investigates/local\\_story\\_251211250.html](http://cbs5.com/investigates/local_story_251211250.html).

<sup>6</sup> Christine House & David Stout, “Democrats Challenge Busch’s Anti-Terrorism Strategy,” *N.Y. TIMES*, Sep. 7, 2006, *available at* <http://www.nytimes.com/2006/09/07/washington/08prexycnd.html>.

<sup>7</sup> Anna Werner, “California Man Buys Nearly 3,000 Cell Phones,” Sep 8, 2006. *available at* [http://cbs5.com/investigates/local\\_story\\_251211250.html](http://cbs5.com/investigates/local_story_251211250.html).

<sup>8</sup> Bruno Nordeste and David Carment, “A Framework for Understanding Terrorist Use of the Internet,” Volume 2006-2, Carleton University, Ottawa, 2006, *available at*, <http://www.carleton.ca/CIFP>.

<sup>9</sup> Brian Levin, *Cyberhate*, Terrorism in Perspective, p. 262, Edited by Pamela L. Griset and Sue Mahan, Sage Publications: California 2003)

<sup>10</sup> Steve Coll and Susan Glasser, “Terrorists Turn to Web as Base of Operations”, *Washington Post*, 7 Aug 2005, 7pp.

<sup>11</sup> Brian Levin, *Cyberhate*, Terrorism in Perspective, p. 259.

bombers and remotely detonated explosive devices are available to terrorists online.<sup>12</sup> In addition, terrorists communicate via “virtual dead drops” using public free e-mail services, storing unsent draft e-mail messages and giving accomplices access to their account.<sup>13</sup> As President Bush has stated, “[t]he terrorists who want to harm America can now buy disposable cell phones, and open anonymous e-mail addresses. Our laws need to change to take these changes into account.”<sup>14</sup>

Within this context, intelligence professionals face perplexing challenges in surveilling terrorist use of these technologies. The rise of transnational non-state actors who challenge the United States both abroad and at home blur the previously clear distinction between national security and law enforcement. Domestic “right to privacy” jurisprudence, familiar in the law enforcement context, seems overly restrictive to those seeking intelligence regarding the terrorist threat. To many it seems that the courts have continually expanded an ill-defined “right to privacy” to advancements in technology. To the contrary, others argue that unrestricted domestic surveillance threatens the very societal values worthy of protection. These issues need to be addressed to protect the nation from non-state actors and at the same time preserve the values basic to American democracy.

### **“Right to Privacy” versus “National Security”**

Objections to government surveillance are based on the notion that government surveillance intrudes upon a constitutional “right to privacy.” Supporters counter that the Executive Branch has plenary power in the field of national security, including the power to

---

<sup>12</sup> Steve Coll and Susan Glasser, “Terrorists Turn to Web as Base of Operations”, *Washington Post*, 7 Aug 2005, 7pp.

<sup>13</sup> Steve Coll and Susan Glasser “Terrorists Turn to Web as Base of Operations”, *Washington Post*, 7 Aug 2005, 7pp.

<sup>14</sup> Christine House & David Stout, “Democrats Challenge Busch’s Anti-Terrorism Strategy,” *N.Y. TIMES*, Sep. 7, 2006.

conduct foreign surveillance free from judicial oversight. The tension between the Executive Branch charged with protecting the national security and the Judicial Branch charged with protecting civil liberties has played out in US courts for much of the nation's history.

### **Executive Power**

“The executive Power shall be vested in a President of the United States of America,”— from this simple sentence Article II of the Constitution delegates to the President legal authority to perform a wide range of duties, including the power to conduct foreign affairs.<sup>15</sup> As a result of the President's responsibility to conduct foreign affairs, he possesses “inherent” authorities requiring neither specific constitutional provisions nor a specific grant of authority from Congress.<sup>16</sup> In fact, in areas of international relations the courts have described the “very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations.”<sup>17</sup> The Supreme Court has consistently recognized a very limited role for the judiciary in the area of foreign affairs.<sup>18</sup> “[T]he very nature of executive decisions as to foreign policy is political, not judicial. Such decisions are wholly confided by our Constitution to the political departments of the government, Executive and Legislative.”<sup>19</sup> The President's authority in the area of foreign affairs includes the power to employ spies and conduct intelligence operations.<sup>20</sup> For many decades Presidents, including

---

<sup>15</sup> U.S. CONST. Article II, § 1.

<sup>16</sup> William F. Brown and Americo R. Cinquegrana, “Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment,” 35 *Cath. U. L. Rev.* 97, 105 (1985) (“Warrantless electronic surveillance has been used by the Executive to collect intelligence information since at least the mid-1800s . . . Warrantless physical searches have been used for a much longer period of time.”).

<sup>17</sup> *United States v. Curtiss-Wright*, 299 U.S. 304, 320 (1936).

<sup>18</sup> *See, e.g., United States v. Curtiss-Wright*, 299 U.S. 304, 320 (1936) (discussing the “very delicate, plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations”).

<sup>19</sup> *Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corporation*, 333 U.S. 103, 111 (1948).

<sup>20</sup> *See United States v. Totten*, 92 U.S. 105, 106 (1875) (“We have no difficulty as to the authority of the President in the matter. He was undoubtedly authorized...as commander-in-chief of the armies of the United States, to employ secret agents...and obtain information respecting the strength, resources, and movements of the enemy.”).

President Bush, have justified warrantless wiretaps to conduct national security operations on this constitutional underpinning.<sup>21</sup>

Nonetheless, the President's authority is not unlimited, and is subject to constitutional restraints.<sup>22</sup> For example, both Congress and the Courts have weighed in on the issue of domestic surveillance by the Executive Branch. Congress has passed, and the courts have interpreted statutory schemes regulating electronic surveillance by the Executive Branch of foreign powers within the United States.<sup>23</sup> However, Congress has not regulated and the Supreme Court has never specifically addressed the constitutionality of warrantless electronic surveillance conducted overseas. In other cases dealing with executive power the Supreme Court has opined "a systematic, unbroken, executive practice, long pursued to the knowledge of the Congress and never before questioned, engaged in by Presidents who have also sworn to uphold the Constitution, making as it were such exercise of power part of the structure of our government, may be treated as a gloss on 'Executive Power' vested in the President by § 1 of Art. II."<sup>24</sup> Consistent with this, lower courts have found that while constitutional protections apply to American citizens abroad, exceptions to the warrant requirement of the Fourth Amendment apply to electronic surveillance conducted overseas.<sup>25</sup>

### **Right to Privacy**

While the United States Constitution does not contain any explicit references to a generic "right to privacy," the Bill of Rights was drafted to guarantee American citizens basic civil liberties. In addition to the enumerated rights, the Supreme Court has determined that the

---

<sup>21</sup> *Zweibon v. Mitchell*, 516 F.2d 594, 634-36 (D.C. Cir. 1975)(en banc)(plurality opinion).

<sup>22</sup> See *United States v. Robel*, 389 U.S. 258, 264 (1967) ("It would indeed be ironic if, in the name of national defense, we would sanction the subversion of one of those liberties--the freedom of association--which makes the defense of the Nation worthwhile.").

<sup>23</sup> Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. §§ 1801-1811 (2000 & Supp. II 2003) and in scattered sections of 18 U.S.C. (2000 & Supp. III 2003)) (FISA).

<sup>24</sup> *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 610 (1952).

<sup>25</sup> *United States v. Bin Laden*, 126 F. Supp. 2d. 264, 277 (S.D.N.Y. 2000).

“specific guarantees in the Bill of Rights have penumbras, formed by emanations from those guarantees that help give them life and substance.”<sup>26</sup> These “emanations” include civil liberties founded in British common law and later adopted by American courts. When interpreting the “right to privacy” the Supreme Court often cites an English common law case decided in 1765 as historical precedent. In *Entick v. Carrington*, Lord Camden laid down basic principles establishing individual civil liberties, and placing restraints on unfettered executive power.<sup>27</sup> “It is not the breaking of his doors, and the rummaging of his drawers, that constitutes the essence of the offence; but it is the invasion of his indefeasible right of personal security, personal liberty and private property, where that right has never been forfeited by his conviction of some public offence, -- it is the invasion of this sacred right which underlies and constitutes the essence of Lord Camden's judgment.”<sup>28</sup>

The “right to privacy” as it applies to government surveillance inextricably involves principles of the First and Fourth Amendments to the Constitution. “The Bill of Rights was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.”<sup>29</sup> Today, opponents often argue that domestic surveillance violates the “right to privacy” emanating from both the First Amendment “right of association” and the Fourth Amendment guarantee against unreasonable searches and seizures. Unfortunately, these same constitutional rights cannot discriminate between patriotic citizens and terrorists.

---

<sup>26</sup> *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

<sup>27</sup> *Entick v. Carrington*, 19 Howell's State Trials 1030 (1765).

<sup>28</sup> *Boyd v. United States*, 116 U.S. 616, 630 (1885).

<sup>29</sup> *Marcus v. Search Warrants*, 367 U.S. 717, 730 (1961).

## First Amendment

The First Amendment's guarantee of "freedom of speech" and "freedom of assembly" limits the government's ability to regulate speech absent "a showing of a paramount or vital governmental interest" and use of means "least restrictive of freedom of belief and association."<sup>30</sup> Free speech enjoys its greatest freedom when expressed in the public forum. For example, in *Hague v. Committee for Industrial Organization*, the Supreme Court determined "[w]herever the title of streets and parks may rest, they have immemorially been held in trust for the use of the public and, time out of mind, have been used for purposes of assembly, communicating thoughts between citizens, and discussing public questions."<sup>31</sup> On the other hand, less public forums such as schools, libraries, and airport terminals are more susceptible to government regulation. Broadcast media such as television and radio have long been subjected to government regulation by the Federal Communications Commission. However, in 1997, the Supreme Court decided the Internet was more like a public square than broadcast media, and therefore entitled to the greatest First Amendment protection against government regulation. In *Reno v. American Civil Liberties Union*, the Supreme Court struck down the Communications Decency Act's attempt to regulate pornography on the Internet.<sup>32</sup> As a result of that decision, the government will have to meet a heavy burden to show any Internet regulation is narrowly tailored to meet a compelling government interest.

Though the Internet may be a public forum, not all categories of speech enjoy constitutional protection. Internet messages that constitute specific crimes are not protected. For example, threats, fraud, conspiracies, and solicitation to commit criminal activities may all be committed via the Internet and are not protected by the First Amendment. Nonetheless, political

---

<sup>30</sup> *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984).

<sup>31</sup> *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939).

<sup>32</sup> *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

speech that merely threatens the American system of government is protected. As early as the Sedition Act of 1798, the government made it a crime, punishable by a \$5,000 fine and five years in prison, "if any person shall write, print, utter or publish . . . any false, scandalous and malicious writing or writings against the government of the United States, or either house of the Congress . . . , or the President . . . , with intent to defame . . . or to bring them, or either of them, into contempt or disrepute; or to excite against them, or either or any of them, the hatred of the good people of the United States."<sup>33</sup> While the Supreme Court never ruled on the Act, Congress recognized the law was unconstitutional and repaid defendant's fines. Many subsequent court decisions recognized the inconsistency of the Act with the First Amendment.<sup>34</sup>

Government surveillance of protected speech has been found to violate the First Amendment because it has a "chilling effect" on exercise of an organization's First Amendment rights.<sup>35</sup> "National security cases...often reflect a convergence of First and Fourth Amendment values not present in cases of "ordinary" crime. Though the investigative duty of the executive may be stronger in such cases, so also is there greater jeopardy to constitutionally protected speech."<sup>36</sup> History is replete of examples of the Executive Branch invoking "national security" as a justification for questionable surveillance operations.<sup>37</sup> The Kennedy Administration used allegations that Dr. Martin Luther King was a "communist sympathizer" to justify domestic surveillance of him and other civil rights activists.<sup>38</sup> The Nixon Administration, likewise, justified burglaries and warrantless wiretaps of newsmen, government workers, and political

---

<sup>33</sup> Sedition Act of 1798, 1 Stat. 596.

<sup>34</sup> *New York Times v. Sullivan*, 376 U.S. 254, 276 (1964).

<sup>35</sup> *Zweibon v. Mitchell*, 516 F.2d 594, 634-36 (D.C. Cir. 1975)(en banc)(plurality opinion).

<sup>36</sup> *United States v. United States District Court*, 407 U.S. 297, 316 (1972).

<sup>37</sup> *Zweibon v. Mitchell*, 516 F.2d at 636.

<sup>38</sup> US Senate. Select Committee to Study Governmental Operations With Respect to Intelligence Activities of the United States Senate, Book II: Intelligence Activities and the Rights of Americans, S. REP. NO. 94-755, at 5-20 (1976) (The Church Report).

opponents under the cloak of “national security.”<sup>39</sup> Within this context, courts have consistently held that domestic surveillance implicates the First Amendment’s freedom of speech and association. As a result, the Internet remains a safe haven for terrorist information operations if not for criminal activities.

## **Fourth Amendment**

The Fourth Amendment and more than 700 Supreme Court cases have defined the “right to privacy” in the context of unlawful searches and seizures by the government.<sup>40</sup> For most of the first 200 years, the Fourth Amendment was primarily thought to protect the individual from unwarranted physical trespass by the government.<sup>41</sup> With advances in technology, notions of what constituted a “physical trespass” became too problematic and the Supreme Court abandoned the approach and re-examined the philosophy behind the Fourth Amendment.<sup>42</sup>

In 1967, the Supreme Court in *Katz v. United States* determined that the “right to privacy” in the Fourth Amendment was designed to protect the individual rather than property rights.<sup>43</sup> The focus of the Fourth Amendment right to privacy was reduced to a two prong test: i) whether the individual had a subjective expectation to privacy, and; ii) whether the expectation was legitimate and one which society found reasonable to recognize.<sup>44</sup>

In dispensing with the requirement of physical trespass, the *Katz* case extended Fourth Amendment protection to include electronic surveillance. While cell phones, e-mail, and the Internet were only imagined at the time, courts since have expanded Fourth Amendment

---

<sup>39</sup> *Id.* at 11-13.

<sup>40</sup> See, Keck, Mathew C., “Cookies the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet,” 13 *Alb. L.J. Sci. & Tech.* 83, 95 (2002).

<sup>41</sup> See, e.g. *Goldman v. United States*, 316 U.S. 129 (1942) (detectaphone placed against wall of adjoining room; no search and seizure); *Silverman v. United States*, 365 U.S. 505 (1961) (spike mike pushed through a party wall until it hit a heating duct)

<sup>42</sup> *Warden v. Hayden*, 387 U.S. 294, 304 (1967).

<sup>43</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>44</sup> 389 U.S. at 353 (1967).

protection to these new technologies. Lower courts have gone so far as to hold that a military member has a reasonable “expectation to privacy” for her government e-mail account on her government-owned computer, despite banners warning that her computer use constituted a valid consent to monitoring.<sup>45</sup> However, the Fourth Amendment does not protect the individual from anyone but the government. Commercial companies monitor Internet use and mine information. “Personal information about your salary, neighbors, credit history, hobbies, social security number, major bank account numbers, and the name of your family dog can all be found online for a price, some even for free.”<sup>46</sup> In other words, the current “right to privacy” protects citizens from the government but not against other governments, commercial businesses, or other non-state actors. In a sense, the Fourth Amendment jurisprudence has created a safe haven where terrorists can and do operate, protected by US law in a war against the US.

Nonetheless, the Fourth Amendment cases do consider that in some circumstances the special needs of society outweigh any expectation of privacy. The Supreme Court has approved warrantless and even suspicionless searches in extraordinary cases where the government had “special needs, beyond the normal need for law enforcement.”<sup>47</sup> For example, the Court has endorsed random drug testing of custom agents and even student athletes.<sup>48</sup> Likewise, searches at borders and sobriety checkpoints are special needs beyond ordinary law-enforcement.<sup>49</sup> However, the Court has rejected the use of warrantless, suspicionless searches where the primary purpose was “to uncover evidence of ordinary criminal wrongdoing.”<sup>50</sup> In *City of Indianapolis v.*

---

<sup>45</sup> See, e.g., *United States v. Long*, 2006 CAAF Lexis 1216 (C.A.A.F. 2006).

<sup>46</sup> Keck, 13 Alb. L.J. Sci. & Tech. at 84.

<sup>47</sup> *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995) (quoting *Griffin v. Wisconsin*, 483 U.S. 868, 873 (1987) (internal quotation marks omitted)); *In re: Sealed Case No. 02-001*, 310 F.3d at 745.

<sup>48</sup> *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 670-71 (1989); *Vernonia School Dist. 47J v. Acton*, 515 U.S. at 873.

<sup>49</sup> *Michigan Dep’t of State Police v. Sitz*, 496 U.S. 444 (1990); *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976).

<sup>50</sup> *City of Indianapolis v. Edmond*, 531 U.S. 32, 41-42 (2000).

*Edmond*, the Supreme Court found a highway checkpoint with the purpose of detecting drug dealers did not fit into the “special needs” category. The Court focused on the programmatic purpose of the search—finding that the purpose needs to be something other than ordinary law enforcement. The Court contemplated that appropriately tailored roadblocks “to thwart an imminent terrorist attack” would withstand judicial scrutiny.<sup>51</sup> Certainly, terrorism constitutes a “special need” threatening society in ways unlike common criminal pursuits.

### **Surveillance--Current Legal Frameworks**

The Executive Branch has conducted warrantless electronic surveillance, with varying amounts of judicial oversight, for foreign intelligence purposes since the mid-1800’s—when electronic communications first came into general use.<sup>52</sup> Government surveillance of the terrorist threat is currently based on four different conceptual frameworks. First, government surveillance of foreign powers or agents conducted overseas is commonly recognized as an exception to the warrant requirement of the Fourth Amendment.<sup>53</sup> Second, the National Security Agency’s (NSA) Terrorist Surveillance Program (TSP) is based on the Commander-in-Chief Clause in Article II of the Constitution, and allows electronic monitoring without a warrant or judicial oversight for transmissions originating or terminating outside the United States—though the administration has recently voluntarily submitted the program to judicial oversight.<sup>54</sup> Third, the Foreign Intelligence Surveillance Act (FISA) of 1978, amended by the Patriot Act, allows domestic monitoring of foreign powers or their agents within the US after approval by the

---

<sup>51</sup> 531 U.S. at 44.

<sup>52</sup> *Id.* at 103

<sup>53</sup> *See, e.g. United States v. Bin Laden*, 126 F. Supp. 2d. 264, 273 (S.D.N.Y. 2000).

<sup>54</sup> George W. Bush, President of the U.S., President’s Radio Address (Dec. 17, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/20051217.html>; Eric Lichtblau and David Johnston, “Court to Oversee U.S. Wiretapping in Terror Cases,” N.Y. TIMES, January 18, 2007, at A1.

special FISA court.<sup>55</sup> Finally, Title III of the Omnibus Crime Control and Safe Streets Act of 1968 (Federal Wiretap Act) allows electronic surveillance with a court issued warrant based on probable cause that criminal activity has occurred.<sup>56</sup> Each of these frameworks attempt to deal with the “right to privacy” ensconced in the Fourth Amendment’s prohibition against unreasonable searches.<sup>57</sup> All four frameworks suffer shortcomings and demand an open and public discussion over whether the current terrorist threat to the United States requires a reassessment of what constitutes a “reasonable expectation of privacy.”

### **Foreign Surveillance Conducted Overseas – Exception to the Warrant Requirement**

When the President authorizes the conduct of electronic surveillance for national security purposes outside the United States, he enjoys the least congressional and judicial oversight and is in the realm of maximum executive power. Agencies that conduct electronic surveillance derive their authority, not from statute, but from presidential Executive Order.<sup>58</sup> While FISA and the Federal Wiretap Act govern domestic electronic surveillance, Congress has not attempted to place statutory constraints on the President for overseas surveillance. Courts have interpreted congressional acquiescence as a tacit admission that the President’s authority flows from his inherent executive power.<sup>59</sup> Even so, at least as applied to US citizens, the Bill of Rights, to include the Fourth Amendment, applies extraterritorially.<sup>60</sup> On the other hand, “[t]here is...no

---

<sup>55</sup> Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § § 1801-1811 (2000 & Supp. II 2003) and in scattered sections of 18 U.S.C. (2000 & Supp. III 2003)).

<sup>56</sup> 18 U.S.C. § § 2510-2520 (2000) (Federal Wiretap Act).

<sup>57</sup> U.S. CONST. amend. IV .( “The right of the people to be...against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause....”).

<sup>58</sup> Exec. Order No. 12,333, 46 F.R. 59941 (December 8, 1981).

<sup>59</sup> *United States v. Bin Laden*, 126 F. Supp. 2d. 264, 273 (S.D.N.Y. 2000); *United States v. Curtiss-Wright*, 299 U.S. 304, 320 (1936).

<sup>60</sup> *Reid v. Covert*, 354 U.S. 1, 5-6 (1957) (plurality opinion) (stating, in a case that the "shield" provided to an American citizen by the Bill of Rights "should not be stripped away just because he happens to be in another land").

indication that the Fourth Amendment was understood by contemporaries of the Framers to apply to activities of the United States directed against aliens in foreign territory....”<sup>61</sup>

While the Supreme Court has never specifically addressed the issue, several courts have addressed whether the government could use evidence obtained from overseas warrantless electronic surveillance in the prosecution of an American citizen. In the *United States v. Bin Laden*, Wadih El-Hage, an American citizen and alleged member of al Qaeda, moved to suppress evidence obtained from a wiretap placed on his phone in Nairobi, Kenya.<sup>62</sup> El-Hage, and other defendants including Osama Bin-Laden, was charged in United States District Court for events surrounding the terrorist bombing of the United States embassies in Nairobi, Kenya and Dar es Salaam, Tanzania.<sup>63</sup> El-Hage claimed that, as a US citizen, the Fourth Amendment protected him against warrantless wiretaps regardless of where the wiretap was placed.<sup>64</sup>

The district judge agreed that El-Hage was entitled to the protection of the Fourth Amendment.<sup>65</sup> However, given the national security context, the protection was more limited than traditional Fourth Amendment analysis. Based on the President’s power over foreign affairs, the burden on the Executive Branch imposed by requiring a warrant and the lack of a warrant procedure—the judge believed the circumstances justified an exception to the warrant requirement.<sup>66</sup> Without Supreme Court or Second Circuit precedent to rely on, the judge adopted a narrow exception to the warrant requirement based on the Fourth Circuit’s ruling in *United States v. Truong Dinh Hung*.<sup>67</sup> The district judge determined an exception to the warrant requirement required a showing that: i) the defendant was an agent of a foreign power; ii) the

---

<sup>61</sup> *United States v. Verdugo-Urquidez*, 494 U.S. 259, 267 (1990).

<sup>62</sup> *United States v. Bin Laden*, 126 F. Supp. 2d. 264, 268 (S.D.N.Y. 2000).

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

<sup>65</sup> *Id.* at 270.

<sup>66</sup> *Id.* at 271-7.

<sup>67</sup> *United States v. Truong Dinh Hung*, 629 F.2d 908, 913 (4th Cir. 1980)

surveillance was primarily conducted for national security purposes; and, iii) the surveillance was authorized by the President or Attorney General.<sup>68</sup> Accordingly, El-Hage's motion to suppress evidence was denied and the results of the wiretaps were admitted. Using this analysis, courts grant US citizens only limited Fourth Amendment protections through ex post facto judicial review of electronic surveillance—and aliens receive no protections.

### **Terrorist Surveillance Program**

The Terrorist Surveillance Program (TSP) presents the most difficult balance between executive authority and civil liberties. It exists in the twilight neither wholly foreign nor wholly domestic. The TSP is a largely secret program conducted by the National Security Agency (NSA) at least since 2002 with no checks and balances and little transparency.<sup>69</sup> The TSP allows the NSA to monitor communications without a warrant if the communication originates or terminates outside the United States. The legality of the program is based on the assumption that the warrant requirement of the Fourth Amendment does not apply to extraterritorial communications.<sup>70</sup> Although there is legal precedent for this assumption, the TSP seeks to further sidestep the issue by ignoring that one party to the communication may be domestic.<sup>71</sup> Further, while the NSA has insisted that all intercepted messages either originate or terminate outside the United States, there is evidence to the contrary.<sup>72</sup> The administration argues that the

---

<sup>68</sup> *Bin Laden*, 126 F. Supp. 2d. at 277-80.

<sup>69</sup> James Risén & Eric Lichtblau, *Spying Program Snares U.S. Calls*, N.Y. TIMES, Dec. 21, 2005, at A1. *American Civil Liberties Union v. National Security Agency*, Case Number 06-C-10294, p.1 (E.D. Mich, August 17, 2006)

<sup>70</sup> *See, United States v. Bin Laden*, 126 F. Supp. 2d. 264 (S.D.N.Y. 2000)(Finding that the Fourth Amendment applies to US citizens overseas, but that there is a "foreign intelligence exception" to the warrant requirement of the Fourth Amendment. To apply the surveillance must be: (i) of a foreign power, or agent thereof; (ii) primarily for a foreign intelligence purpose, and; (iii) authorized by the President or Attorney General.)

<sup>71</sup> *United States v. United States District Court (Keith)*, 407 U.S. 297, 321-22 (1972) (holding that there is no warrant exception for "domestic security" surveillances but explicitly stating that the Court had "not addressed, and expressed no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents").

<sup>72</sup> Gen. Michael Hayden, Principal Deputy Dir. for Nat'l Intelligence, Press Briefing (Dec. 19, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1.html> ("I can assure you, by the physics of

very generic Authorization for the Use of Military Force passed after 9/11 provides Congressional approval for the program.<sup>73</sup>

To justify the program, the administration relies on the fact that domestic laws and constitutional protections generally do not apply to the nation's enemy overseas. Relying on his Article II powers, the President has the flexibility to monitor and react to external threats to national security unencumbered by domestic law. While the government concedes that the TSP program monitored electronic transmissions that originate or terminate within the United States, they deny that rules regarding domestic surveillance apply. However, success of the TSP requires confidence that the Executive Branch is self-policing and not susceptible to abuse of power. American society and jurisprudence are most comfortable relegating unfettered discretion to the Executive Branch when dealing with issues of national security and relations with other nation states.

In January 2006, the American Civil Liberties Union (ACLU) filed suit seeking to enjoin NSA from conducting surveillance pursuant to the TSP.<sup>74</sup> The ACLU contended that the TSP violated their members' First and Fourth Amendment rights under the Constitution.<sup>75</sup> On August 17, 2006, a federal district judge in the Eastern District granted the plaintiff's request and permanently enjoined the NSA from conducting surveillance under the TSP. The district judge concluded that the NSA's TSP program was warrantless domestic surveillance violating both the

---

intercept, by how we actually conduct our activities, that one end of these communications are [sic] always outside the United States of America.").

<sup>73</sup> Pub. L. No. 107-40, 115 Stat. 224 (2001).

<sup>74</sup> Complaint, *American Civil Liberties Union v. National Security Agency*, complaint filed, Case Number 06-C-10294 (E.D. Mich., January 17, 2006).

<sup>75</sup> *Id.* at 56.

First and Fourth Amendment.<sup>76</sup> The Sixth Circuit Court of Appeals has stayed enforcement of the injunction pending an appeal by the United States.<sup>77</sup>

On January 17, 2007 the Bush administration announced a voluntary agreement to give the FISA court jurisdiction over the TSP.<sup>78</sup> Though the decision was announced less than two weeks before the Sixth Circuit was due to hear arguments in the ACLU case, the administration denied the surprise reversal was in any way related.<sup>79</sup> Further, the Justice Department continues to maintain that warrantless surveillance in these cases continues to be legal.<sup>80</sup> However, the Justice Department also announced plans to argue the ACLU case in the Sixth Circuit was moot as a result of the administration's new position.<sup>81</sup> The ACLU response was that "the president is still claiming the 'inherent authority' to engage in warrantless eavesdropping — even his own attorneys acknowledged that nothing would stop him from resuming warrantless surveillance at any time."<sup>82</sup> Without a court ruling and without any legislation, nothing prevents the administration from adopting a secret new "TSP II" program tomorrow.

### **Foreign Intelligence Surveillance Act -- FISA**

The FISA program provides a middle ground, allowing domestic surveillance of "agents of a foreign power" with judicial oversight—regardless of where the transmission originates or terminates. Prior to 2001, a FISA application could not be approved unless the primary purpose

---

<sup>76</sup> *American Civil Liberties Union v. National Security Agency*, Case Number 06-C-10294, p.44 (E.D. Mich, August 17, 2006).

<sup>77</sup> Court Order, *American Civil Liberties Union v. National Security Agency*, court order, No. 06-2095/2140 (6th Cir., October 4, 2006).

<sup>78</sup> Eric Lichtblau and David Johnston, "Court to Oversee U.S. Wiretapping in Terror Cases," N.Y. TIMES, January 18, 2007, at A1

<sup>79</sup> *Id.*

<sup>80</sup> *Id.*

<sup>81</sup> *Id.*

<sup>82</sup> *Id.*; American Civil Liberties Union, "Safe and Free: Restore Our Constitutional Rights." ACLU. <http://www.aclu.org/safefree/nsaspying/index.html> (accessed 1 April 2007).

was to gather foreign intelligence, not criminal prosecution.<sup>83</sup> The FISA program was hampered by a perceived legal barrier impeding foreign intelligence and law enforcement cooperation.<sup>84</sup> This misapprehension was not based on statutory language but was self-imposed in positions taken by the Department of Justice in the 1980s and later adopted by the FISA court, eventually becoming the *de facto* “law.”<sup>85</sup> The Patriot Act, passed in 2001, attempted to affirmatively eliminate any barrier in the original statute.<sup>86</sup> In a rare 2002 opinion, the Foreign Intelligence Surveillance Court of Review determined that there was no longer, and may never have been, a statutory “wall” between intelligence and law enforcement. Further, the court held that the statute as amended was constitutional, going so far as to suggest that FISA procedures even “if they do not meet the minimum Fourth Amendment warrant standards, certainly come close.”<sup>87</sup>

While the FISA program provides judicial oversight, any arguments that the court has hampered Executive Branch efforts to conduct surveillance are belied by the fact that between 1978 and 2005 the court approved 19,000 warrants and rejected only five.<sup>88</sup> The administration’s reluctance to use the FISA program for transmission originating or terminating outside the United States may well be a reluctance to inadvertently expand the FISA court jurisdiction. Recognizing FISA court jurisdiction over these semi-foreign TSP transmissions would in essence be ceding the President’s Article II, Commander-in-Chief power to Congress and the Judicial branches. Certainly, the earlier experience with the FISA “wall” supports this

---

<sup>83</sup> *In re: Sealed Case No. 02-001*, 310 F.3d 717, 721 (US Foreign Int. Surv. Ct. Rev. 2002).

<sup>84</sup> *Id.* at 721.

<sup>85</sup> *Id.* at 723-4.

<sup>86</sup> *Id.* at 728-9.

<sup>87</sup> *Id.* at 746.

<sup>88</sup> Katherine Wong, “Recent Development: The NSA Terrorist Surveillance Program,” 43 *Harv. J. on Legis.* 517, 518 (Summer, 2006); James Bamford, “The Agency That Could Be Big Brother,” *N.Y. TIMES*, Dec. 25, 2005, § 4, at 1. (“The court rarely turns the government down. Since it was established in 1978, the court has granted about 19,000 warrants; it has only rejected five.”).

concern. As easy as obtaining an order from the FISA court has proven to be, the Executive Branch values flexibility and nimbleness in combating the terror threat to the nation.

### **Federal Wiretap Act**

The Federal Wiretap Act, with its 38-year history, provides the most solid statutory and constitutional foundation for domestic surveillance. However, the statute is ill-suited to address the war on terror. Congress passed the Federal Wiretap Act in response to a Supreme Court decision that electronic surveillance constituted a “search” under the Fourth Amendment.<sup>89</sup> Under the Act, Title III warrants will be issued when the government shows probable cause that a crime “has been, is being, or is about to be committed” at a particular location.<sup>90</sup> In addition, Title III warrants are limited to 30-days and at the expiration the target must be notified. Precautions are required to prevent inadvertent intercepts of non-targets. Further, the Supreme Court has insisted that in domestic cases not involving foreign powers or agents, this Title III process requiring judicial review is a prerequisite to conducting domestic surveillance operations.<sup>91</sup> This statutory regime has proven reliable in the context of traditional law enforcement because the focus is on solving crimes that are in progress or already complete. On the other hand, fighting terrorism needs to be preventative to be effective.<sup>92</sup> As the Supreme Court has recognized in other contexts, probable cause determinations are not particularly helpful in preventing the occurrence of dangerous conditions.<sup>93</sup> In short, Title III warrants are of

---

<sup>89</sup> *Katz v. United States*, 389 U.S. 347 (1967).

<sup>90</sup> 18 USC § 2516 (2000).

<sup>91</sup> *United States v. United States District Court*, 407 U.S. 297, 324 (1972).

<sup>92</sup> See, Hoffman, Grayson A., “Note: Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment,” 40 *Am. Crim. L.Rev.* 1655 (Fall, 2003).

<sup>93</sup> *Union v. Von Raab*, 489 U.S. 656, 665-66 (1989).

limited value because as well-suited as they are for enforcing criminal law, they lack the flexibility that allows the government to detect and prevent terrorist acts.

Attempts to judicially regulate domestic surveillance are complicated by the nature of terrorism and technology. Terrorists, as non-state actors, owe their allegiance to a cause instead of a nation. US laws, on the other hand, differentiate between foreign and domestic criminals. Terrorists operate transnationally without regard to borders frustrating legal theories based on borders. In further aggravation, modern technology allows electronic communications, e-mail and the Internet to bounce world-wide without regard to national borders. With each advancement in technology, society's expectation of privacy expands. Perhaps another approach is to redefine what constitutes a reasonable expectation of privacy in light of changes in technology and threats to national security.

### **Privacy—Reasonable Expectations**

The underlying issue is the degree to which American society wants to recognize the “right to privacy” in light of changing technology and threats. Government monitoring of Internet, e-mail, and cell-phones for terrorist activity can certainly be reconciled with the Fourth Amendment privacy concerns. It is only the advent of technology that has even made these types of communications private. In the past, users of messengers, telegraphs, and multi-party telephone lines understood the limitations on their privacy. Even today, with the advent of data mining, scanners and hackers, most technologically savvy individuals understand the lack of security in their communications. Many Americans would, no doubt, forego some degree of privacy in their electronic communications in order to achieve greater security against the terrorist threat. However, secret programs and abuse of executive powers create a climate of

distrust between members of a democracy and their elected leaders.<sup>94</sup> The solution is public debate and legislation that removes the issue from the shadows. As technology rapidly advances, and as the nation's enemies become more sophisticated, the nation cannot allow its laws and constitution to be exploited by those who wish to destroy that society.

In the last few years, political leaders have submitted at least four bills proposing legislative fixes to address programs such as the TSP that exist in the shadows between FISA and unfettered executive power.<sup>95</sup> These bills range from essentially a congressional endorsement of the TSP program as it existed prior to January 2007 to intermediate versions that provide a minimal amount of congressional notification, to the most restrictive version that in most circumstances applies rules similar to those already contained within FISA. With the exception of the latter, all the bills are sponsored by Republicans. The administration's reversal of its position on TSP oversight in January 2007 has removed much of the impetus for legislative solutions. Further, with Republicans losing control of both the House and Senate in the 2006 elections, the future of these legislative changes is doubtful. Special interests groups such as the ACLU have launched lobbying campaigns against the Republican sponsored bills. These groups point out that the Bush administration has failed to articulate why compliance with legislative and judicial oversight will hinder efforts to track terrorists. By reversing its position on the TSP without acknowledging that the program was illegal, and with the acknowledgement that warrantless wiretaps could resume in the future, the administration has further removed an important issue from public debate.

---

<sup>94</sup> See generally US Senate, Select Committee to Study Governmental Operations With Respect to Intelligence Activities of the United States Senate, Book II: Intelligence Activities and the Rights of Americans, S. REP. NO. 94-755, at 5-20 (1976) (The Church Report).

<sup>95</sup> See, Senate, Terrorist Surveillance Act of 2006, 109th Congr., 2nd Sess., 2006, S. 2455; Senate, Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006, 109th Congr., 2nd Sess., 2006, S. 3001; Senate, Terrorist Surveillance Act of 2006, 109th Congr., 2nd Sess., 2006, S. 3931; House, Electronic Surveillance Modernization Act, 109th Congr., 2nd Sess., 2006, H.R. 5825.

Perhaps a more radical approach is legislation that removes certain types of technology from the debate over privacy. If terrorist use of technologies such as the Internet and cell-phones presents a fundamental threat to society, perhaps the expectation of privacy in these mediums is misplaced. After all, the analogy of the Internet or electronic media to the public square is already a stretch. The public square promotes assembly and the free exchange of ideas—the physical interaction of people in a public setting. In contrast, the internet promotes anonymous and clandestine communications. Political dissent and freedom from an overreaching government do require the most protection, but not in every forum, and the public square is still available. Further, declaring the Internet, e-mail, and cell-phones subject to monitoring does not eliminate other protected methods of expression and assembly. Electronic monitoring would not inhibit the majority of communications. As most employers can attest, monitoring far from eliminates employee use of workplace e-mail and the internet for personal use. However, there is a fundamental difference between engaging in communications you know are being monitored, and having your private communications secretly surveilled. As a nation of laws, a democracy is free to craft laws to achieve an appropriate balance between civil liberties and national security.

Any legislation subjecting cell-phones, and the Internet to monitoring would need to be subject to very public debate. Any legislation that allows national security monitoring of electronic transmissions would require safeguards to address legitimate public concerns. If the underlying fear is that the government will misuse intercepted information for political or other non-national security reasons, such concerns need to be addressed. Any legislation would have to include severe criminal and civil penalties for misuse of collected information—holding

public officials accountable for their actions. In a sense, this would still provide judicial oversight, but only in the cases of abuse by the Executive Branch.

The alternative is the status quo—a patchwork of statutes and legal precedents that are ill-suited to fight the modern terrorist who uses US technology and US laws to his asymmetrical advantage. The terrorist wins by forcing the Executive Branch to fight a shadow war where programs like the Terrorist Surveillance Program destroy trust between elected officials and the American public. The solution is to remove certain technologies from the arsenal of the terrorist. If cell phones, the Internet, and e-mail are subject to lawful monitoring, they lose some of their attraction to the enemy. The sheer volume of transmissions will remain a technological hurdle, but this doesn't need to be compounded by unnecessary legal impediments. Modern US society differs from that of the drafters of the Constitution, not only because technology has changed the ways people communicate, but because it has reduced the nation's isolation from threats both internal and abroad—US society's expectation of privacy needs to flex as well.

## **Conclusion**

Technology will continue to evolve and in unforeseen ways that benefit both the nation and its enemies alike. In an age of increasing globalization, technology is no longer a monopoly in the hands of the elite nation states. Terrorists throughout the ages have exploited whatever technology was available—they do so now, and will continue to do so in the future. In addition, they will continue to exploit perceived weaknesses in a democratic society. The secular democratic society and rule of law that they abhor, many times offers the nation's enemies a protected base from which to operate. In the area of domestic surveillance, the “right to privacy” as currently interpreted offers terrorists a safe haven. However, US law does not have

to be a static, unyielding Maginot Line easily circumvented by the nation's adversaries but needs to flex and adapt to changes both in technology and in the tactics of its enemies. To the consternation of many, jurists often describe the Constitution as a "living, breathing document." While the words have changed only through amendment, how courts apply these constitutional provisions to changing technologies and circumstances, unimagined by the nation's forefathers, requires considered forethought. Defining "reasonable expectations of privacy" needs to reflect today's technology and today's threat. The strength of an open democratic society is its ability to flex and change its laws to protect its constitutional values and society.

## Bibliography

1. *American Civil Liberties Union v. National Security Agency*, Case Number 06-C-10294, p.44 (E.D. Mich., August 17, 2006).
2. American Civil Liberties Union, "Safe and Free: Restore Our Constitutional Rights." ACLU. <http://www.aclu.org/safefree/nsaspying/index.html> (accessed 1 April 2007).
3. Bamford, James, "The Agency That Could Be Big Brother", *N.Y. TIMES*, Dec. 25, 2005.
4. *Boyd v. United States*, 116 U.S. 616 (1885).
5. Brown, William F. and Cinquegrana, Americo R., "Warrantless Physical Searches for Foreign Intelligence Purposes: Executive Order 12,333 and the Fourth Amendment," 35 *Cath. U. L. Rev.* 97, 105 (1985).
6. Bush, George W., President of the U.S., President's Radio Address (Dec. 17, 2005), available at <http://www.whitehouse.gov/news/releases/2005/12/20051217.html> (accessed 9 October 2006).
7. *Chicago & Southern Air Lines, Inc. v. Waterman S.S. Corporation*, 333 U.S. 103 (1948).
8. *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).
9. Coll, Steve and Glasser Susan B., "Terrorists Turn to Web as Base of Operations", *Washington Post*, 7 Aug 2005.
10. Complaint, *American Civil Liberties Union v. National Security Agency*, complaint filed, Case Number 06-C-10294, p.44 (E.D. Mich., January 17, 2006).
11. Court Order, *American Civil Liberties Union v. National Security Agency*, court order, No. 06-2095/2140 (6th Cir. October 4, 2006).
12. Dunlap, Charles J., "The Role of the Lawyer in War: It Ain't No TV Show: JAGs and Modern Military Operations", 4 *Chi. J. Int'l L.* 479 (Fall, 2003).
13. *Entick v. Carrington*, 19 Howell's State Trials 1030 (1765).
14. Executive Order 12,333, "United States Intelligence Activities," 46 F.R. 59941 (December 8, 1981).
15. *Goldman v. United States*, 316 U.S. 129 (1942).
16. *Griffin v. Wisconsin*, 483 U.S. 868 (1987).
17. *Griswold v. Connecticut*, 381 U.S. 479 (1965).
18. *Hague v. Committee for Industrial Organization*, 307 U.S. 496 (1939).

19. Hayden, Gen. Michael, Principal Deputy Dir. for Nat'l Intelligence, Press Briefing (Dec. 19, 2005), *available at* <http://www.whitehouse.gov/news/releases/2005/12/print/20051219-1>.
20. Hoffman, Grayson S., "Note: Litigating Terrorism: The New FISA Regime, the Wall, and the Fourth Amendment," 40 *Am. Crim. L.Rev.* 1655 (Fall, 2003).
21. House, Christine and Stout, David, "Democrats Challenge Busch's Anti-Terrorism Strategy," *N.Y. TIMES*, Sep. 7, 2006.
22. House, *Electronic Surveillance Modernization Act*, 109th Congr., 2nd Sess., 2006, H.R. 5825.
23. *In re: Sealed Case No. 02-001*, 310 F.3d 717, 721 (US Foreign Int. Surv. Ct. Rev. 2002).
24. *Katz v. United States*, 389 U.S. 347 (1967).
25. Keck, Mathew C., "Cookies the Constitution, and the Common Law: A Framework for the Right of Privacy on the Internet," 13 *Alb. L.J. Sci. & Tech.* 83, 95 (2002).
26. *Kyllo v. United States*, 533 U.S. 37 (2001).
27. Levin, Brian, "Cyberhate," in Pamela L. Griset and Sue Mhan, Eds., *Terrorism in Perspective*, Claifornia, Sage Publications, 2003, p. 262.
28. Lichtblau, Eric and Johnston, David "Court to Oversee U.S. Wiretapping in Terror Cases," *N.Y. TIMES*, January 18, 2007, at A1
29. Lonsdale, David J., *The Nature of War in the Information Age: Clausewitzian Future*, London, Frank Cass, 2004.
30. *Marcus v. Search Warrants*, 367 U.S. 717 (1961).
31. *Michigan Dep't of State Police v. Sitz*, 496 U.S. 444 (1990).
32. *National Treasury Employees Union v. Von Raab*, 489 U.S. 656, 670-71 (1989).
33. *New York Times v. Sullivan*, 376 U.S. 254 (1964).
34. Nordeste, Bruno and Carment, David, "A Framework for Understanding Terrorist Use of the Internet," *Integrated Threat Assessment Centre Volume 2006-2*, Carlton University, Ottawa, 2006.
35. Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. § § 2510-2520 (2000) (Federal Wiretap Act).
36. Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. § § 1801-1811 (2000 & Supp. II 2003) and in scattered sections of 18 U.S.C. (2000 & Supp. III 2003)).

37. Pub. L. No. 107-40, 115 Stat. 224 (2001).
38. *Reid v. Covert*, 354 U.S. 1 (1957).
39. *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).
40. Risen, James and Lichtblau, Eric, "Bush Lets U.S. Spy on Callers Without Courts," *N.Y. TIMES*, Dec. 16, 2005, at A1
41. Seditio Act of 1798, 1 Stat. 596.
42. Senate, *Terrorist Surveillance Act of 2006*, 109th Congr., 2nd Sess., 2006, S. 2455.
43. Senate, *Foreign Intelligence Surveillance Improvement and Enhancement Act of 2006*, 109th Congr., 2nd Sess., 2006, S. 3001.
44. Senate, *Terrorist Surveillance Act of 2006*, 109th Congr., 2nd Sess., 2006, S. 3931.
45. *Silverman v. United States*, 365 U.S. 505 (1961).
46. *Union v. Von Raab*, 489 U.S. 656, 665-66 (1989).
47. U.S. CONST. Article II, § 1.
48. U.S. CONST. amend. IV.
49. United States Congress, Senate. *Select Committee to Study Governmental Operations With Respect to Intelligence Activities of the United States Senate, "Book II: Intelligence Activities and the Rights of Americans,"* S. REP. NO. 94-755, at 5-20 (1976).
50. *United States v. Bin Laden*, 126 F. Supp. 2d. 264 (S.D.N.Y. 2000).
51. *United States v. Curtiss-Wright*, 299 U.S. 304 (1936).
52. *United States v. Long*, 2006 CAAF Lexis 1216 (C.A.A.F. 2006).
53. *United States v. Martinez-Fuerte*, 428 U.S. 543 (1976).
54. *United States v. Robel*, 389 U.S. 258 (1967).
55. *United States v. Totten*, 92 U.S. 105 (1875).
56. *United States v. Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980).
57. *United States v. United States District Court (Keith)*, 407 U.S. 297, 324 (1972).
58. *United States v. Verdugo-Urquidez*, 494 U.S. 259 (1990).
59. *Vernonia School Dist. 47J v. Acton*, 515 U.S. 646, 653 (1995).

60. *Warden v. Hayden*, 387 U.S. 294 (1967).
61. Werner, Ann, "California Man Bus Nearly 3,000 Cell Phones," Sep 8, 2006. *available at* [http://cbs5.com/investigates/local\\_story\\_251211250.html](http://cbs5.com/investigates/local_story_251211250.html).
62. Wong, Katherine, "Recent Development: The NSA Terrorist Surveillance Program," 43 *Harv. J. on Legis.* 517 (Summer, 2006).
63. *Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579 (1952).
64. *Zweiben v. Mitchell*, 516 F.2d 594 (D.C. Cir. 1975) (en banc).