

---

---

# Electronic Surveillance: A Brief History and Examination of Present Legal Debate

BY WALKER FULTS\*

*On December 16, 2005, the New York Times revealed that the Bush Administration was engaging in the electronic surveillance of U. S. citizens on a large scale without court orders. The surveillance was done in the name of protecting the country from terrorist attacks like those committed on September 11, 2001, but the existence of the program also raised legal concerns, specifically concerning FISA and the Fourth Amendment.*

*I first examine the history of the issue of domestic electronic surveillance. Extensive programs with roots as early as WWII outgrew their originally intended scope, and many were finally exposed by the Church Committee in 1975, which also found grave evidence of abuse. Three years later, Congress resolved to legislate against such programs, and clearly established the guidelines to be used in conducting domestic surveillance in FISA.*

*A generation later, the George W. Bush Administration has conducted surveillance in an effort to fight terrorism that seems to run contrary to FISA. I consider the legal arguments that are advanced by prominent members of both schools of thought on the issue: to use a superficial distinction, those who believe the surveillance to be legal, and those who do not. My paper finally finds that the Administration's Terrorist Surveillance Program, or other programs which the Administration has not disclosed, are illegal by FISA and the Fourth Amendment because they employ warrantless domestic surveillance of citizens.*

*\* Walker Fults is a senior at Duke University, majoring in political theory. He also studies philosophy and Chinese. He was born in Dallas, Texas, where he lived until attending college. Mr. Fults has had interest in the law and legal matters for much of his life, and hopes to attend law school after he graduates. This paper was the product of an independent study conducted with Duke Law Professor Erwin Chemerinsky.*

INTRODUCTION.....	20
I. DEFINING THE TERMS: COMMON MISPERCEPTIONS ABOUT SURVEILLANCE.....	21
<i>A. The Face of Modern Surveillance</i> .....	21
<i>B. Electronic Surveillance Is Not Entirely in Response to the Sept. 11 Attacks</i> .....	22
II. HISTORY OF SURVEILLANCE IN THE UNITED STATES.....	22
<i>A. President Washington and the Revolutionary War</i> .....	22
<i>B. Presidents Lincoln, Wilson, and Roosevelt</i> .....	23
<i>C. Operation Chaos</i> .....	23
<i>D. Project Shamrock</i> .....	24
1. The History of Shamrock.....	24
2. Shamrock’s Infrastructure and Management.....	25
3. The Place of the Law.....	26
4. Comparison of Fall-Out Thirty Years Ago and Today.....	26
5. Industry Responsibility.....	26
<i>E. The Church Committee</i> .....	28
<i>F. The Road to FISA</i> .....	29
<i>G. 1978: Congress Passes the Foreign Intelligence Surveillance Act</i> .....	31
1. Surveillance Without Warrants, Not of US persons.....	31
2. Surveillance With a Warrant and the FISA Court.....	31
III. SURVEILLANCE AFTER SEPTEMBER 11, 2001.....	32
<i>A. “Massive Cultural Shift”: The Change From Prosecution to Prevention</i> .....	32
<i>B. The Threat Matrix and the Role of Law</i> .....	33
<i>C. The Modern Scope of Surveillance: The Story of NSA, AT&amp;T, and the Narus STA 6400</i> .....	34
<i>D. The Changing Role of Katz and Present Disagreement Over the Law</i> .....	36
IV. THE DEBATE ON THE LEGALITY OF MODERN ELECTRONIC SURVEILLANCE.....	37
<i>A. Advocates of Electronic Surveillance as Legal</i>	
1. John Eastman.....	37
(a). Unfair Ad Hominem Attack of CRS Bias and Disregard of DOJ Bias.....	37
(b). Jackson’s Framework of Executive Power in Youngstown.....	38
(c). The AUMF: Legitimate Authorization of Electronic Surveillance?.....	39
(d). Necessity Versus the Law.....	40
2. Robert Turner.....	41
(a). The Founders’ Conception of Executive Powers.....	41
(b). Executive Authority of Just Congress’s Lack Thereof?: Turner’s Misapplication of Legal Restraints on Congress.....	42

(c). Airport Security Comparison.....	42
3. Former Attorney General Alberto Gonzales: Wordplay and Deceit.....	43
B. Critics of Electronic Surveillance	
1. The Law Exists Even for Times of Necessity.....	44
2. The AUMF Does Not Mention or Approve of Electronic Surveillance.....	45
3. The Responsibility of Presidential Accountability.....	46
CONCLUSION.....	47

## INTRODUCTION

On December 16, 2005, *The New York Times* revealed that the George W. Bush Administration was engaging in electronic surveillance of citizens of the United States on a large scale without court orders.<sup>1</sup> The surveillance was done in the name of protecting the country from terrorist attacks like those committed on September 11, 2001, but the existence of the program also raised legal concerns. Specifically, critics feared that in its warrantless spying on citizens, the Bush Administration was acting extralegally of the Fourth Amendment to the Constitution of the United States and the Foreign Intelligence Surveillance Act of 1978 (FISA). Advocates of the Administration's surveillance activities defended their actions on the grounds that they were both legal and necessary;<sup>2</sup> some spoke of espionage and treason of those who made the program known to the public.<sup>3</sup> While those on either side of the debate argued about whether the President's actions were within the proper bounds of the law, the interchange itself raised larger questions as to the ultimate role of the law, specifically whether the President is always obligated to act within its limits, particularly in a time of war. No one would base an argument on the premise that the President is above the law, but some place tremendous emphasis on necessity in arriving at a legal justification for warrantless surveillance. This paper will address these questions, cover the history of the issue of surveillance in the United States, examine the legal arguments that have been advanced from the various positions, and conclude that the Bush Administration is guilty of acting outside the Fourth Amendment and FISA.

<sup>1</sup> James Risen and Eric Lichtblau, *Bush Lets U. S. Spy on Callers Without Courts*, N.Y. TIMES, December 16, 2005.

<sup>2</sup> *Is Congress the Real 'Lawbreaker'?: Reconciling FISA with the Constitution*: Hearing before the House Judiciary Committee, (2007) *Statement of Robert F. Turner*, September 5, 2007. Robert Turner, Professor of Law at the University of Virginia School of Law, is a Revolutionary Period Scholar and Expert on Presidential Powers. His legal opinions on the Administration's electronic surveillance activities are discussed later, starting in detail on page thirty-five.

<sup>3</sup> John C. Eastman, *Listening to the Enemy: The President's Power to Conduct Surveillance of Enemy Communications During Time of War*, ILSA J. INT'L & COMP. L. 13-1 (2006), at 9.

---

## I. DEFINING THE TERMS: COMMON MISPERCEPTIONS ABOUT SURVEILLANCE TODAY

### *A. The Face of Modern Surveillance*

The *New York Times* article was the first to announce the Administration's program of electronic surveillance, but many other news reports followed, covering other facets of the growing controversy. Many Americans think that the surveillance does not affect law-abiding citizens, that it targets only known terrorist operatives and associates, and that it is in direct response to the terrorist attacks of September 11, 2001. The Bush Administration has been making statements to that effect whenever questioned about its surveillance activities. For example, in a statement from May 2006 in response to questions about the National Security Agency (NSA) Terrorist Surveillance Program he authorized, President Bush himself said, "first, our international activities strictly target al Qaeda and their known affiliates. . . . second, the government does not listen to domestic phone calls without court approval. . . . fourth, the privacy of ordinary Americans is fiercely protected in all our activities."<sup>4</sup> It is easy to get the impression that surveillance involves only terrorists, and that the communication and privacy of ordinary citizens is not compromised in the process. Unfortunately, the matter is more complicated than just that; Bush's statements from May 2006 were skirting the border of truth, if not downright false. The general perception of the NSA's electronic Terrorist Surveillance Program and the description that the Administration has given of the program are both flawed and misguided in several ways.

At the outset, surveillance in the electronic age need not involve direct oversight by one person of another, listening to a phone line in real time. Due to the changing nature and volume of modern communication, surveillance may be carried out with the help of private companies. The December 16, 2007 *New York Times* article "Wider Spying Fuels Aid Plan For Telecoms" reveals how the changing face of technology in communication necessarily involves industry carriers. The article states:

The federal government's reliance on private industry has been driven by changes in technology. Two decades ago, telephone calls and other communications traveled mostly through the air, relayed along microwave towers or bounced off satellites. The N. S. A. could vacuum up phone, fax and data traffic merely by erecting its own satellite dishes. But the fiber optics revolution has sent more and more international communications by land and undersea cable, forcing the agency to seek company cooperation to get access.<sup>5</sup>

---

<sup>4</sup> President George W. Bush, Address on the NSA Surveillance Program, The White House (May 11, 2006) Available at [www.whitehouse.gov/news/releases/2006/05/20060511-1.html](http://www.whitehouse.gov/news/releases/2006/05/20060511-1.html).

<sup>5</sup> Eric Lichtblau, James Risen, and Scott Shane, *Wider Spying Fuels Aid Plan for Telecoms*, N.Y. TIMES, December 16, 2007.

With such a high volume of phone and email records, the NSA does not seek to target known individuals, but rather to prevent trouble through data-mining algorithms that make use of the tremendous processing power of modern supercomputers. For example, if a certain email passes through an NSA computer and contains a certain number of keywords, it could be flagged and examined by NSA officials. Although this is exactly the kind of driftnet enterprise that former NSA director Michael Hayden denied was operating,<sup>6</sup> evidence of its existence in association with at least one communications company, AT&T, has surfaced.<sup>7</sup> Thus, electronic surveillance can be carried out on a large scale—and, in fact, has been—with the invasion of privacy of innocent Americans being collateral damage.

### *B. Electronic Surveillance Is Not Entirely in Response to the Sept. 11 Attacks*

The public has a misguided belief that electronic surveillance is entirely in response to the foreign terrorist attacks of 2001. Nevertheless, the NSA had approached communications companies well before the September 11, 2001 attacks. In addition, surveillance is currently being used against not only terrorism, but also crime. On October 14, 2007, *New York Times* reporter Scott Shane revealed that Qwest Communications was approached by the NSA in February 2001. When asked for their customers' call records, Qwest refused, and as a result, "the agency retaliated by depriving Qwest of lucrative outsourcing contracts" as asserted by Qwest executive Joseph P. Nachio.<sup>8</sup> And the *Times* article "Wider Spying" later addressed the link between electronic surveillance and fighting crime, not terrorism.<sup>9</sup> Clearly, the relationship between the Bush Administration's surveillance programs and fighting terrorism is not one-to-one.

## II. THE HISTORY OF SURVEILLANCE IN THE UNITED STATES

### *A. President Washington and the Revolutionary War*

In order to better understand the legal arguments defending or attacking the Bush Administration's electronic surveillance program, it is important to look at the history of the issue of surveillance. Many advocates of the NSA's Terrorist

---

<sup>6</sup> *FOX News Sunday* (Fox Television Broadcast February 5, 2006) available at [www.foxnews.com/story/0,2933,183844,00.html](http://www.foxnews.com/story/0,2933,183844,00.html).

<sup>7</sup> *Spying on the Homefront*, Frontline (PBS Television Broadcast) available at [www.pbs.org/wgbh/pages/frontline/homefront](http://www.pbs.org/wgbh/pages/frontline/homefront).

<sup>8</sup> Scott Shane, *Former Phone Chief Says Spy Agency Sought Surveillance Help Before 9/11*, N.Y. TIMES, October 14 2007.

<sup>9</sup> Lichtblau, *supra* note 5. The article reported that "to detect narcotics trafficking, for example, the government has been collecting the phone records of thousands of Americans and others inside the United States who call people in Latin America, according to several government officials who spoke on the condition of anonymity because the program remains classified."

Surveillance Program have cited historical examples meant to be used as precedent for Bush's program, going as far back as the American Revolution. These historical examples, cited by those who believe the Administration's surveillance legal, are meant to be taken as appropriate precedent. However, perhaps these events from the past should be seen not as lessons, but as mistakes. For example, former Attorney General Alberto Gonzales, in his February 6, 2006 hearing before the Senate Judiciary Committee on wartime executive power and the NSA's surveillance authority, said that General George Washington ordered a type of surveillance that was much akin to Bush's NSA program. Gonzales said, "General Washington, for example, instructed his army to intercept letters between British operatives, copy them and allow those communications to go on their way."<sup>10</sup> Robert Turner, a Revolutionary period scholar and advocate of the legality of the NSA program, backs up Gonzales's claim, saying, "General Washington ordered the opening and reading of all mail from England to gather intelligence during the American Revolution."<sup>11</sup> However, this historical example is not as determinative as Gonzales and Turner may suppose. Legal precedent and mere history are two different things. The fact that President Washington was previously involved in surveillance may have better informed him of the dangers to private liberties upon which the United States was founded. Asserting that a person endorsed a certain activity and pointing out that he himself engaged in such an activity are two different things. Moreover, the historical anecdote that Gonzales references in his testimony is not directly relevant to the present understanding of the law today. Today's legal issues are decided by the laws on today's books and the courts' interpretations of those laws.

### *B. Presidents Lincoln, Wilson, and Roosevelt*

Gonzales, in the same part of his testimony, gives other examples from history that are intended to serve the same purpose as his example of Washington's order to open private letters during the Revolution. All his examples come from times of war, as officially declared by Congress. Gonzales notes that Lincoln ordered "warrantless wiretapping of telegraph messages during the Civil War," that during World War I President Wilson "authorized the military to intercept each and every cable, telephone and telegraph communication going into or out of the United States," and that during World War II President Roosevelt "authorized the military to intercept each and every cable, telephone and telegraph communication going

---

<sup>10</sup> *Wartime Executive Power and the NSA's Surveillance Authority: Hearing Before the U. S. Senate Judiciary Committee*, (2006) (statement of Alberto Gonzales, Att'y Gen. of the United States) Transcript available at [www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html). [Hereinafter *hearing*].

<sup>11</sup> Robert F. Turner, *The Federalist Society Online Debate Series: FISA*, The Federalist Society, December 11, 2007, posts one and two. Available at [www.fed-soc.org/debates](http://www.fed-soc.org/debates).

into or out of the United States.”<sup>12</sup> As with the example from President Washington, Gonzales’s argument would carry more legal force if he were citing Supreme Court opinions rather than merely pointing out isolated actions of past Presidents of the United States, whose actions may or may not have been legal in their time. Such cases led Congress to pass the Foreign Intelligence Surveillance Act (FISA) in 1978.

### C. Operation Chaos

However, the passing of the FISA came more specifically in response to a series of scandals in the 1970s which involved surveillance. After news of the Watergate scandal broke, culminating in Nixon’s resignation in 1974, the issue of surveillance and the government’s part in illegally obtaining private information was pushed to the forefront. The 1976 *New York Times* article “Johnson, Nixon Linked to Spying in U. S.” made the connection between both Presidents Johnson and Nixon and covert CIA operations that were found to be illegal and corrupt. The article states, “Presidents Johnson and Nixon applied pressure on the Central Intelligence Agency that brought about a domestic spy operation that the agency’s director, Richard Helms, knew violated its charter . . .”<sup>13</sup> The article later explains that the program, named Operation Chaos, “designed to uncover the foreign influence behind domestic unrest, lasted from 1967 to 1974 despite repeated findings that student and racial demonstrations at home were not directed or financed from abroad.”<sup>14</sup> The scope of the program was not small, and it did not target select individuals. An article from one year prior, simply entitled “‘Operation Chaos’ . . .,” opines that “it is horrifying to learn that the C. I. A. had undercover contacts monitor the meetings of groups such as the Southern Christian Leadership Conference and the Washington Urban League. It maintained files on nearly a thousand organizations.”<sup>15</sup>

### D. Project Shamrock

1. *The History of Shamrock* - A similar surveillance program, Project Shamrock, was conducted for even longer than Operation Chaos. Former CIA Inspector General Britt Snider, in his piece “*Unlucky Shamrock: Recollections from the Church Committee’s Investigation of NSA*,” recounts that Shamrock was the means through which the government obtained international telegrams that left the country from New York City. A source within the NSA told Snider that the “NSA had had access for many years to most of the international telegrams leaving New York City for

---

<sup>12</sup> Hearing, *supra* note 10 (statement of Alberto Gonzales, Att’y Gen. of the United States).

<sup>13</sup> Associated Press, *Johnson, Nixon Linked to Spying in U. S.*, N.Y. TIMES, May 19, 1976.

<sup>14</sup> *Id.*

<sup>15</sup> ‘Operation Chaos’ . . . , N.Y. TIMES, June 11, 1975.

foreign destinations.”<sup>16</sup> There was no individualized suspicion that triggered the interception of the telegrams; rather, it was simply a matter of the course that had been carried over from World War II. Snider states that:

Every day, a courier went up to New York on the train and returned to Fort Meade<sup>17</sup> with large reels of magnetic tape, which were copies of the international telegrams sent from New York the preceding day using the facilities of three telegraph companies. The tapes would then be electronically processed for items of foreign intelligence interest, typically telegrams sent by foreign establishments in the United States or telegrams that appeared to be encrypted.<sup>18</sup>

Snider later met with Dr. Louis Tordella, one of the only men who knew the full scope of Shamrock, to get more details about its conception and operations. The former civilian Deputy Director at the NSA, Tordella, told Snider that “Shamrock actually predated NSA, which was created by President Truman in 1952. It had essentially been a continuation of the military censorship program of World War II.”<sup>19</sup> It seems that nothing big ever came of the program, and it was eventually shut down in the 1970s by the Secretary of Defense because it “just wasn’t producing very much of value.”<sup>20</sup>

2. *Shamrock’s infrastructure and management* - More interesting than Project Shamrock’s failure to produce valuable intelligence was its oversight. Although researching the inner workings of a covert government operation that was intended to be shrouded in secrecy will never be entirely fruitful, Snider was able to glean some information from Tordella about how the project was run. Tordella said “that while many NSA employees were aware of Shamrock, only one lower-level manager—who reported to him directly—had had ongoing responsibility for the program over the years.”<sup>21</sup> In addition, since its original briefing with President Truman, Tordella did not know if any President or Attorney General had even been made aware of the program.<sup>22</sup> The infrastructure of the project was entirely lacking, leading to the potential for abuse of information of the same kind that occurred in association with Operation Chaos. Fortunately, Snider reports no such abuse. However, a scenario in which a few government individuals have access to the personal and private correspondence of masses of people without any accompanying responsibility is

---

16 L. Britt Snider, *Unlucky SHAMROCK: Recollections from the Church Committee’s Investigation of NSA*, CSI Studies in Intelligence, Winter 1999-2000. Available at <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/docs/v43i3a04p.htm>.

17 NSA headquarters was established at Fort Meade in the 1950s.

18 Snider, *supra* note 16.

19 *Id.*

20 *Id.*

21 *Id.*

22 *Id.*

surely dangerous.

3. *The Place of the Law* - The attitudes toward the legality of Project Shamrock of those connected to it are of note as well. Those in charge of running the program viewed legality as a foreign concept, one that did not involve them. Snider recalls of Tordella, “When I asked if it was legal for NSA to read the telegrams of American citizens, he replied, ‘You’ll have to ask the lawyers.’”<sup>23</sup> The same dubious understanding of the role of the law can be seen concerning surveillance today.

4. *Comparison of Fall-Out Thirty Years Ago and Today* - As for official handling of the matter when it came to light, President Ford claimed the right of executive privilege to prevent disclosure of Project Shamrock to Congress, or worse, the press.<sup>24</sup> The same attitude of summarily claiming legality without much discussion of either justification or specific legal support can be seen today in the Bush Administration. In the same statement from May 11, 2006 mentioned earlier, President Bush said, “the intelligence activities I authorized are lawful and have been briefed to appropriate members of Congress, both Republican and Democrat.”<sup>25</sup> When asked in an interview about the legality of the President’s Terrorist Surveillance Program, Vice President Cheney said, “we believe that we have all the legal authority we need.”<sup>26</sup> Finally, then-Attorney General Gonzales said in his hearing before the Senate Judiciary Committee, that the President’s surveillance program was legally consistent with his powers under the Constitution.<sup>27</sup> Those in the Executive Branch both in the 1970s and today appear to simply subscribe to the school of thought that the President has the “inherent authority,”<sup>28</sup> to use Gonzales’s term, to conduct surveillance which he feels is necessary to national security matters. According to them, much more explanation would compromise national security, the very end of the program itself.

5. *Industry Responsibility* - Lastly, there is a final comparison between the events of three decades ago and today. The attitude of those involved with the intelligence collection towards the companies that cooperate with the government programs is one of assumed exoneration or downright innocence. Snider reports that Tordella was surprisingly ready to meet with him to speak about Project Shamrock, and was good-tempered throughout their interview. However, when the topic of company responsibility in the affair came up, the conversation became tense. Tordella said that the companies cooperated with the government for singularly “patriotic reasons.”<sup>29</sup>

---

23 *Id.*

24 Robert M. Smith, *President Blocks Security Records Sought in House: Invokes Executive Privilege on F. B. I. and N. S. A. Data in Surveillance Inquiry*, N.Y. TIMES, February 25, 1976.

25 *Id.*

26 Interview with Vice President Richard Cheney, Vice President of the United States, February 2006.

27 Hearing, *supra* note 10.

28 *Id.*

29 Snider, *supra* note 16.

And, when Snider suggested that the companies must bear some responsibility for “providing the wherewithal for the government to use [the records] however it wanted,”<sup>30</sup> Tordella’s temper flared for the first time. In Tordella’s opinion, that of the man who had had the most oversight of Project Shamrock throughout the years, the companies’ patriotic and selfless intentions more than cleared them of any potential legal responsibility for the consequences of their actions. Moreover, if they were to be exposed by the upcoming Church Committee,<sup>31</sup> “it would discourage other companies from cooperating with US intelligence for years to come.”<sup>32</sup> Good intentions and necessity in fighting for the nation’s security, two admittedly important concerns, had pushed legality to the backseat.

Today, the Bush Administration is actively seeking immunity for companies which cooperated in providing communication information to the NSA Terrorist Surveillance Program, and possibly other government programs still completely classified. In a December 10, 2007 op-ed piece in the *New York Times*, Director of National Intelligence Mike McConnell wrote that “those in the private sector who stand by us in times of national security emergencies deserve thanks, not lawsuits.”<sup>33</sup> And industry officials echo the same sentiment.<sup>34</sup> However, the motives of these companies may not be as singularly patriotic as they seem. With an administration that has earned a reputation more for its retaliatory practices than being aboveboard,<sup>35</sup> companies may simply cooperate because they fear the negative consequences that may be doled out to them if they do not. It is hardly surprising that Qwest executive Joseph P. Nacchio now asserts that the Bush Administration retaliated against Qwest when it did not immediately get the cooperation it was seeking.<sup>36</sup> This does not necessarily change the legal responsibility that the companies who cooperated with the Administration may bear; each case should be decided on its own facts. To say that these companies are simply doing their part to serve America and its interests is not entirely truthful. During the Ford Presidency, nothing much in the

---

30 *Id.*

31 The Church Committee was a Senate assemblage formed as a result to the abuse of programs such as Operation Chaos and Project Shamrock. The Committee produced a report that detailed abuse of such programs (discussed soon hereafter), and led the way to the passing of the landmark legislation of FISA, the Foreign Intelligence Surveillance Act.

32 Snider, *supra* note 16.

33 Mike McConnell, *Help Me Spy on Al Qaeda*, N.Y. TIMES, December 10, 2007.

34 Lichtblau, *supra* note 5.

35 The leaking of the identity of CIA agent Valerie Plame in retaliation for her husband’s lack of cooperation with the Administration in finding intelligence favorable to an invasion of Iraq is perhaps the clearest example of the Bush Administration’s retaliatory tactics. After alleging in his 2003 State of the Union address that Iraq had tried to obtain uranium from Africa, Plame’s husband Joseph Wilson wrote an op-ed article in the *New York Times*, published on July 6, 2003, entitled “What I Didn’t Find in Africa,” in which he presented his findings and set the record straight. Although it is not certain whether the Administration intended to make the scandal as public as it became, many soon learned from this example that the Administration was not necessarily afraid to strong-arm in order to get the cooperation it wanted.

36 Shane, *supra* note 18.

way of consequences came to these companies.<sup>37</sup> Let us hope that in this regard, history is not repeated. Companies that potentially cooperated with the government in illegal activities should stand test under the law and be acquitted or found guilty as appropriate, not given a retroactive pardon for unlawful actions.

### *E. The Church Committee*

Operation Chaos and Project Shamrock are two of the clearer examples of secret surveillance at home on the part of the government, but other CIA, NSA, or similar FBI domestic surveillance programs also came to the public eye in the mid-1970s, and were summarily dissolved. The Senate created a committee, chaired by Idaho Senator Frank Church, and gave it the specific charge of investigating “the conduct of domestic intelligence, or counterintelligence operations against United States citizens.”<sup>38</sup> The findings of the Church Committee, in its own words, were “disturbing.”<sup>39</sup> The Committee found gross abuses of the government’s surveillance powers, including the spying of too many people and the gathering of too much information. The government even used “wiretaps, microphone ‘bugs,’ surreptitious mail opening, and break-ins,” to accomplish its own political goals, in absence of any threat, domestic or foreign.<sup>40</sup>

The secret government programs that the Church Committee Report mentions include the famous Operation Chaos, but also involve other programs such as the FBI’s Counter Intelligence Program (COINTELPRO), and Projects Minaret and Shamrock. The report finds evidence not only of inappropriate domestic surveillance, but also subsequent abuse of the information after it had been gathered:

Unsavory and vicious tactics have been employed—including anonymous attempts to break up marriages, disrupt meetings, ostracize persons from their professions, and provoke target groups into rivalries that might result in deaths. Intelligence agencies have served the political and personal objectives of presidents and other high officials. While the agencies often committed excesses in response to pressure from high officials in the Executive branch and Congress, they also occasionally initiated improper activities and then concealed them from officials whom they had a duty to inform.<sup>41</sup>

Information is power, and unfortunately it would seem that the abuse of it has not

37 Amidst strong pressure from President Bush to pass a bill granting retroactive immunity to telecommunication companies for their possible role in granting records to government programs like the Terrorist Surveillance Program before the 2007 Christmas recess, the Senate delayed voting on the bill, with Connecticut Senator Chris Dodd threatening a filibuster if the bill did come to a vote. See Lichtblau, *supra*.

38 The Church Committee Report, Book II, April 26, 1976. Available at [www.icdc.com/~paulwolf/cointelpro/churchfinalreport.htm](http://www.icdc.com/~paulwolf/cointelpro/churchfinalreport.htm).

39 *Id.*

40 *The Church Committee Report*, See *supra* note 38.

41 *Id.* at 4.

been below those who have been placed in charge of domestic spying programs in our nation's history.

Few Americans are probably aware of the extent to which domestic surveillance has been carried out in the past. Gonzales was historically correct when he cited the examples of past Presidents, and venerated ones such as Washington, Lincoln, and Roosevelt at that, who directed that surveillance be instituted when they thought it necessary. But what do these examples really show? Evidence that past Presidents have engaged in certain activities does not condone those activities by law. Furthermore, after knowing the kind of abuse that can occur when governmental domestic surveillance is put into practice on a large scale, should we really wish to repeat the same history? Any reasonable person should surely see the danger in the Attorney General's kind of logic. History has informed us of the dangers of such surveillance, not condoned it.

#### *F. The Road to FISA*

Lack of oversight has led to abuse of power: this much is clear. Proper management was a central issue to the legal problem of surveillance in the early and middle 1970s. If the President has power over foreign affairs, and the Supreme Court holds that a disinterested court must issue a warrant for wiretapping or other means of electronic surveillance, then there is the issue of real potential for clash in jurisdiction when addressing surveillance that involves both foreign and domestic elements. Before 1978, this issue was unsatisfactorily decided unilaterally by the President and other parts of the executive branch. And as the Church Committee Report can attest, unsupervised and unrestricted domestic surveillance often outgrows its original purpose, and even begins to work against the appropriate privacy of a great number of American citizens. In his paper "The System of Foreign Intelligence Surveillance Law," Peter Swire explains how both critics and supporters of surveillance stood to gain by the institution of law on the issue. He writes:

Supporters of surveillance could gain by a statutory system that expressly authorized foreign intelligence wiretaps, lending the weight of Congressional approval to surveillance that did not meet all the requirements of ordinary Fourth Amendment searches. Critics of surveillance could institutionalize a series of checks and balances on the previously unfettered discretion of the President and the Attorney General to conduct surveillance in the name of national security.<sup>42</sup>

Appropriate legislation could define exactly how surveillance would be carried out,

---

<sup>42</sup> Peter Swire, *The System of Foreign Intelligence Surveillance Law*, *George Washington Law Review* 4 (72d ed. 2004).

making it both respectable and subject to proper scrutiny, thus solving the issue of oversight.

At roughly the same time, the Supreme Court looked at the issue of warrantless domestic electronic surveillance involving homeland security (to borrow today's term) for the first time. In *United States v. United States District Court*, (or The Keith Case, as it is more commonly known), the Court identified the central issue as "the delicate question of the President's power, acting through the Attorney General, to authorize electronic surveillance in internal security matters without prior judicial approval."<sup>43</sup> Those familiar with the present-day controversy over warrantless surveillance will recognize the similarity between the issue facing the Court in 1972 and today's debate over surveillance. In the Keith Case, the defendant was accused of bombing a government building, and some of the evidence used against him had been obtained through surveillance, although without a warrant.<sup>44</sup> The defendant asked that the United States disclose the surveillance reports, and petitioned for a hearing to determine if the evidence was admissible in court, since it had been obtained without a warrant.<sup>45</sup> However, the Government argued that "the surveillance was lawful, though conducted without prior judicial approval, as a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security."<sup>46</sup> Thirty-four years later, the Attorney General argued that "many, many presidents have exercised their inherent authority under the Constitution to engage in electronic surveillance of the enemy, particularly during a time of war."<sup>47</sup> Later, on the subject of electronic surveillance under the NSA Terrorist Surveillance Program, he said, "we do believe the president has inherent authority under the Constitution."<sup>48</sup> The exact same argument, that the President has the inherent authority under the Constitution as Commander-in-Chief to conduct electronic surveillance at home is being made today as was made in 1972.

In the Keith Case, the Court upheld the decision of a lower court that the surveillance evidence to be used against the defendant, Lawrence (Pun) Plamondon, was unlawful.<sup>49</sup> The Court stated:

As the surveillance of Plamondon's conversations was unlawful, because conducted without prior judicial approval, the courts below correctly held that

---

43 *United States v. United States District Court*, 407 U.S. 297 (1972). [hereinafter *The Keith Case*].

44 *Id.* at 299.

45 *Id.* at 301

46 *Id.* at 301.

47 *Newshour with Jim Lehrer*, interview with Alberto Gonzales (Television broadcast January 23, 2006) Transcript available at [www.pbs.org/newshour/bb/law/jan-june06/gonzales\\_1-23.html](http://www.pbs.org/newshour/bb/law/jan-june06/gonzales_1-23.html).

48 *Id.*

49 *The Keith Case*, *supra* note 42, at 407.

*Alderman v. United States*, 394 U. S. 165 (1969), is controlling, and that it requires disclosure to the accused of his own impermissibly intercepted conversations.<sup>50</sup>

In a very logically constructed argument, it is with this that the Court says, “It is as if the Court says outright, “if no prior judicial approval, then surveillance unlawful.” In addition to ruling on the specific case of *Plamondon*, the Court in this situation “invited legislation,”<sup>51</sup> as Swire puts it. The Court said, “Given these potential distinctions between Title III criminal surveillances and those involving the domestic security, Congress may wish to consider protective standards for the latter which differ from those already prescribed for specified crimes in Title III.”<sup>52</sup> Recognizing that there was not sufficient legislation in the area of domestic surveillance, especially the new technologies of electronic surveillance, the Court asked Congress to make the law on the subject clear. Three years later, the Church Committee Report, in exposing the abuses of programs such as Project Chaos, made abundantly clear that an Act of Congress was well in order.

### *G. 1978: Congress Passes the Foreign Intelligence Surveillance Act*

*1. Surveillance Without Warrants, Not of US Persons* - Another three years later, Congress responded to the Keith Case’s invitation and to the stunning findings of the Church Committee Report. In 1978, Congress passed the Foreign Intelligence Surveillance Act (FISA).<sup>53</sup> The law specifically addresses domestic electronic surveillance and provides two scenarios in which it can be carried out: the first without a court order, and a second with one. In the first scenario, the law grants the President, through the Attorney General, the power to “authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for periods of up to one year.”<sup>54</sup> However, the law is clear that there must be no reasonable chance that the surveillance will invade the privacy of a United States person.<sup>55</sup> The law does not grant warrantless surveillance lightly, either. The Attorney General must certify to several provisions in each case under oath.<sup>56</sup>

*2. Surveillance With a Warrant and the FISA Court* - In the second scenario, electronic surveillance may be carried out by obtaining a warrant. The law establishes a special court that would approve surveillance operations on United States citizens or legal residents, known as the FISA court.<sup>57</sup> The law establishes that there must

<sup>50</sup> *Id.*

<sup>51</sup> Swire, *supra* note 41, at 16.

<sup>52</sup> The Keith Case, *id.*

<sup>53</sup> *The Foreign Intelligence Surveillance Act 1978*, 50 U.S.C. §1801-1811, 1821-29, 1841-46, and 1861-62. Electronic surveillance is the focus of §1802. Available at [www.cnss.org](http://www.cnss.org).

<sup>54</sup> *Id.* at §1802(a), §1802(1).

<sup>55</sup> *Id.* at §1802(a), §1802(1), §1802(B).

<sup>56</sup> *Id.* at §1802(a), §1802(1).

<sup>57</sup> *See Id.* §1802(b).

be probable cause to issue a warrant, and specifies the “necessary findings” prerequisite to surveillance being approved.<sup>58</sup> FISA even recognizes the possibility that some cases might arise in which surveillance must be conducted immediately, and as a result recognizes a possibility of retroactive legal warrants. It terms such grants “emergency orders,”<sup>59</sup> and recognizes the legality of such surveillance “if an application in accordance with this subchapter is made to [a judge of the FISA Court] as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance.”<sup>60</sup> These two main provisions governed legal thinking on electronic surveillance in order to gain foreign intelligence in the United States for many years until they were shaken, together with America’s trust in its ability to prevent foreign assault, by the September 11, 2001 terrorist attacks.

### III. SURVEILLANCE AFTER SEPTEMBER 11, 2001

#### A. “Massive Cultural Shift”: The Change From Prosecution to Prevention

Although the catastrophic consequences of the September 11 attacks are well understood in terms of human life and damages, their full impact on the thinking of America’s leaders is not. In an interview on PBS’s Frontline special program “Spying on the Homefront,” former Attorney General John Ashcroft says that within hours of the attacks, President Bush told him to “never let this happen again.”<sup>61</sup> Ashcroft describes how the President’s words invoked a “massive cultural shift”<sup>62</sup> in the paradigm of law enforcement from prosecution to prevention. Ashcroft says, “the volume of information that must be handled, that must be managed, that must be understood is exponentially greater to assess the potentials of various threats that are coming in together as compared to proving a specific incident in the past.”<sup>63</sup> In retrospect, it seems that once law enforcement is framed in the terms of prevention and of amassing an “exponentially greater” “volume of information,” the nature of surveillance will also change with it. In an interview with same program, Michael Woods, FBI National Security Attorney between 1997-2002, expounds on how this shift from prosecution to prevention affects the way the government conducts surveillance. He explains:

When you talk about prevention, you’re saying to people, well, you can’t just focus on one person. You have to cast the net a bit more broadly, and

<sup>58</sup> See *Id.* §1805(a), §1802(b).

<sup>59</sup> See *Id.* §1805(f).

<sup>60</sup> *Id.*

<sup>61</sup> *Spying on the Homefront: Interview with John Ashcroft* (PBS television broadcast March 12, 2007) Available at [www.pbs.org/wgbh/pages/frontline/homefront/interviews/ashcroft.html](http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/ashcroft.html).

<sup>62</sup> *Id.*

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

you have to start to work with situations where you are going to collect a lot of data and then try to connect the dots. But that means you're going to collect a lot of data, and that means you're going to end up holding a lot of data about ordinary people who have nothing to do with your threat.<sup>64</sup>

This new method of collecting and holding data was necessary to the Bush Administration's goal of preventing another attack at all costs. The events of September 11, 2001 changed how the United States government viewed the prevention of foreign attack, and the way it uses surveillance to accomplish that end.

### *B. The Threat Matrix and the Role of Law*

In his book *The Terror Presidency*, Jack Goldsmith recounts what it was like to work inside the Administration as the Assistant Attorney General, Office of Legal Counsel from October 2003 until he resigned less than ten months later, in July of 2004.<sup>65</sup> The Office of Legal Counsel (OLC) is a division under the Attorney General's Office, and "holds an exalted status within [the government] as the chief advisor to the President and the Attorney General about the legality of presidential actions."<sup>66</sup> As head of the OLC and an insider in the Administration, Goldsmith saw firsthand the effect of what is called the "threat matrix."<sup>67</sup> In his article "FBI-CIA matrix is key to tracking terror threats," Curt Anderson reports that the matrix "details every sign of a threat, from intercepted e-mails to satellite photos to clandestine whispers of spies."<sup>68</sup> "Running up to thirty pages," Anderson says that the report "has become part of President Bush's morning routine in the fight against terror."<sup>69</sup> The threat matrix, then, is an influential contributor to how administration officials perceive the threat posed to the United States.

At a glance, the threat matrix seems to indicate an appropriately cautious attitude towards the threat of foreign and domestic attack on the part of America's leaders. Goldsmith tells that reading the matrix every day can eventually bombard a person, engendering an unfounded paranoia springing from a laundry list that contains "obviously false accusations."<sup>70</sup> Goldsmith writes, "it is hard to overstate the impact that the incessant waves of threat reports have on the judgment of people

---

<sup>64</sup> *Spying on the Homefront: Interview with Michael Woods* (PBS television broadcast February 1, 2007) Available at <http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/woods.html>.

<sup>65</sup> Jack L. Goldsmith, *The Terror Presidency: Law and Judgment Inside the Bush Administration* 9 (W. W. Norton & Company ed., 2007).

<sup>66</sup> *Id.* at 9.

<sup>67</sup> *Id.* at 71.

<sup>68</sup> Curt Anderson, *FBI-CIA matrix is key to tracking terror threats*, LAREDO MORNING TIMES, May 25, 2003.

<sup>69</sup> Goldsmith, *supra* note 65, at 72.

<sup>70</sup> *Id.* at 72.

inside the executive branch . . .”<sup>71</sup> He continues, “Jim Comey, the most levelheaded person I knew in government, says that reading about plans for chemical and biological and nuclear attacks over days and weeks and years causes you to ‘imagine a threat so severe that it becomes an obsession.’”<sup>72</sup> Perhaps, then, the threat matrix stirs up more frenzy and panic than appropriate caution in the minds of America’s leaders.

An illustration of the real effect that the threat matrix has on the minds of policy makers in the Administration is Goldsmith’s attempt to put “an important counterterrorism initiative on a proper legal footing.”<sup>73</sup> After months, Goldsmith had been able to find no way to legally justify the initiative and was forced to report to Alberto Gonzales and David Addington, Cheney’s long time aide, that he had no choice but to rule unfavorably: to rule that the initiative was not legally sound. When told the news, Addington reacted with disgust, saying “if you rule that way, the blood of the hundred thousand people who die in the next attack will be on *your* hands.”<sup>74</sup> Goldsmith writes that the effect of the threat matrix “is why Addington lost it when I told him and Gonzales that I could not bless the initiative they thought crucial to preventing the next attack.”<sup>75</sup> Under worry of constant danger beating at the door, it’s a small wonder that top government officials have marginalized unbiased legal judgments that they think hinder them from doing all they can to keep America safe. Stopping the next attack became more important than strictly obeying the law.

### *C. The Modern Scope of Surveillance: The Story of NSA, AT&T, and the Narus STA 6400*

The most unknown facet of modern electronic government surveillance is that it is now carried out domestically on a large scale. This aspect of surveillance is not well known because the debate about surveillance has largely been framed in terms that cause people to believe that it is targeted against terrorists and their known associates, and that ordinary people’s privacy rights are not compromised in the process. As mentioned earlier, President Bush<sup>76</sup> and other government officials<sup>77</sup> have made direct and specific statements in that vein. The Frontline special “Spying on the Homefront” frames the discussion in very different terms. In interviews with

---

71 *Id.* at 72.

72 *Id.* at 71.

73 *Id.* at 71.

74 *Id.* at 76.

75 *Id.* at 76.

76 See discussion of public misperceptions of surveillance. See *supra* note 4.

77 Michael Hayden, former director of NSA, asserted that surveillance was not a driftnet. See *supra* note 6. Alberto Gonzales also stated in his testimony that the President’s Terrorist Surveillance Program did not use driftnet tactics. An examination of his exact statements and careful wordplay in his testimony can be found on pages 43-44.

influential players from former Attorney General John Ashcroft to AT&T technician Mark Klein, who first discovered a secret NSA communications splitter room at his workplace in San Francisco,<sup>78</sup> the program sheds new light on how modern electronic surveillance is actually conducted.

Mark Klein worked for more than two decades as a technician at AT&T, and shortly before retiring in May 2004, he started to find evidence of things at his workplace that were out of the ordinary. Summer 2002, in the wake of the Defense Department's Advanced Research Project Agency's (DARPA) Total Information Awareness program,<sup>79</sup> Klein was told by his manager that a man associated with the NSA was beginning work on building a secret NSA room inside the AT&T office. Klein says that only those with NSA clearance, of which there was only one at AT&T, were allowed inside the room.<sup>80</sup> Next, Klein happened upon wiring plans which showed a data splitter set up to copy communications data. Klein says that "the documents clearly show the splitter cabinet, which is in the seventh-floor Internet room, is connected down to the secret room on the sixth floor."<sup>81</sup> Lastly, Klein saw a supercomputer capable of enormous processing power in an equipment shipment to the AT&T branch. Called the Narus STA (Semantic Traffic Analyzer) 6400, Klein found that it was a machine "designed for high-speed sifting through high-speed volumes of data, [and] looking for something according to various program algorithms."<sup>82</sup> Klein says "So when I saw all that, it all clicked together to me: 'Oh, that's what they're doing. This is a spy apparatus. I'm not just imagining things.'"<sup>83</sup> Internet expert Brian Reid, one of the first ones to see Klein's documents, says of the Narus "what this thing was is a very full-scale device to take all communication, voice and data, and send it both wherever it was supposed to go but also shunted off to a little listening room."<sup>84</sup> Considering the processing power of the Narus and the fact that it was connected to a data splitter inside a secret room to which only those with NSA clearance had access, it is not hard to connect

---

78 *Spying on the Home Front: Interview with Mark Klein* (PBS television broadcast January 9, 2007) Available at [www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html](http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html).

79 After the terrorist attacks of September 11, the Bush Administration started a great effort to collect any information that might prevent another terrorist attack. One of the most ambitious programs was the Defense Department's Advanced Research Projects Agency's Total Information Awareness program, or TIA. New York Times article "Taking Spying to Higher Level, Agencies Look for More Ways to Mine Data" from February 25, 2006, reports that "In the wake of 9/11, the potential for mining immense databases of digital information gave rise to a program called Total Information Awareness, developed by Adm. John M. Poindexter." Nevertheless, due to widespread hue and cry, the same article reports that "Congress abruptly canceled the program in October 2003." However, stories like Klein's confirm Spying on the Homefront's conclusion that "the ultimate effect was to push elements of the program into other agencies, behind closed doors."

80 See *supra* note 78.

81 *Id.*

82 *Id.*

83 *Id.*

84 *Spying on the Home Front: Interview with Brian Reid* (PBS television broadcast) Available at [www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html](http://www.pbs.org/wgbh/pages/frontline/homefront/etc/script.html).

the dots to Klein's "spy apparatus" conclusion. When asked why AT&T might put a Narus inside a room in its San Francisco office to which NSA has access,<sup>85</sup> Vice President of Narus Marketing Steve Bannerman stuttered, "That's not a question that I-I-I- so as far as I know, no one's ever proved anything. I don't know—I don't know the answer to that question. I have no idea if that's ever been done or not."<sup>86</sup> One can see why there is now an immunity bill for telecommunications companies that cooperated with the government in this type of operation before the Senate.<sup>87</sup> The threat of legal prosecution looms large in the minds of those who helped the government advance its surveillance activities. And though the prospect of a single NSA secret room in San Francisco is uncomfortable enough for some, there may be many others around the nation as well. J. Scott Marcus, Senior Advisor for Internet Technology at the FCC from 2001-2005, estimates from declarations of Klein's and AT&T documents "an overall national deployment to from 15 to 20 sites, possibly more."<sup>88</sup> It would seem to make sense, in the spirit of "total information awareness," that the government would push its surveillance as far as it could possibly reach.

#### *D. The Changing Role of Katz and Present Disagreement Over the Law*

The government's electronic data mining through the use of powerful supercomputers in association with AT&T raises serious questions about the legality of the President's surveillance actions. Since it was decided in 1967, the Supreme Court case *Katz v. United States* has been the legal precedent on electronic surveillance. Swire even calls the case "the king of Supreme Court surveillance cases"<sup>89</sup> in his paper "*Katz is Dead. Long Live Katz.*" In the case, Charles Katz was convicted of illegal gambling through evidence obtained from an electronic surveillance device installed in a phone booth. The Court ruled that because he was inside a closed phone booth, Katz had a "reasonable expectation of privacy,"<sup>90</sup> and as such the Fourth Amendment applied to his own person and not only the physical place.<sup>91</sup> Chiding the government, the Court says that if a court-issued warrant had been obtained before the surveillance was conducted, there would be no question that the surveillance would have been legal.<sup>92</sup> However, without a warrant, electronic surveillance that is conducted in circumstances of reasonable supposed privacy are

---

85 *Spying on the Home Front: Hendrick Smith, in an interview with Steve Bannerman* (PBS television broadcast).

86 *Id.*

87 See *supra* note 36.

88 J. Scott Marcus, "Declaration of J. Scott Marcus in Support of Plaintiffs' Motion for Preliminary Injunction," 8 June 2006.

89 Peter Swire, *Katz is Dead. Long Live Katz*, MICH. L. REV. 1, (January 20, 2004).

90 *Katz v. United States*, 389 U. S. 347 (1967). This exact quote is taken from Justice Harlan's concurrence, but it reflects the opinion of the Court, given by Justice Stewart.

91 *Id.*

92 *Id.*

in violation of the Fourth Amendment.

However, as the title of Swire's paper suggests, *Katz* no longer holds the same legal force it once did: he writes "if *Katz* is the king of Fourth Amendment surveillance cases, then that king is dead."<sup>93</sup> Because of the quickly changing pace of technology used to carry out electronic surveillance, decisions like *Katz* and laws such as FISA are now called outdated. In signing the Protect America Act of 2007, President Bush sought to modernize FISA, and the White House website even lists four main ways that the new law will do so.<sup>94</sup> The new law amends FISA to give the President the authority to order surveillance of conversations in which one party is outside the United States, as long as the acquisition does not constitute purely domestic surveillance, among other provisions.<sup>95</sup> However, the law does not clearly enumerate which powers the President has, and which ones he does not. *Katz*'s test of a reasonable expectation of privacy is no longer the standard for judging the legality of warrantless surveillance. Moreover, there is ambiguity on exactly what kind of surveillance the President is legally able to conduct (not to mention confusion on how much domestic surveillance actually exists today in America). As a result, there is a widely differing set of opinions on the legality of the Bush Administration's electronic surveillance programs.

#### IV. THE DEBATE ON THE LEGALITY OF MODERN ELECTRONIC SURVEILLANCE

##### *A. Advocates of Electronic Surveillance as Legal*

*1. John Eastman: (a). Unfair Ad Hominem Attack of CRS Bias and Disregard of DOJ Bias* - President Bush asserts that his surveillance activities are both legal and necessary, but there also exists a school of thought in the legal community which asserts that the President has inherent authority under the Constitution to carry out surveillance activities that he deems necessary to the protection of the nation. One such advocate of Bush's surveillance programs is law professor John C. Eastman. In his paper "Listening to the Enemy: The President's Power to Conduct Surveillance of Enemy Communications During Time of War," Eastman broadly defends the President's authority under the Constitution to conduct necessary surveillance during a time of war. He starts his argument by analyzing the competing reports of the Congressional Research Service (CRS)<sup>96</sup> and the Department of Justice

---

<sup>93</sup> Swire, *supra* note 89 at 30.

<sup>94</sup> These reasons appear below Bush's statement concerning the law from August 5, 2007, but lack any citation. Available at [www.whitehouse.gov/news/releases/2007/08/20070806-5.html](http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html).

<sup>95</sup> *The Protect America Act*, August 5, 2007 available at ([www.cryptome.org/s1927.htm](http://www.cryptome.org/s1927.htm)).

<sup>96</sup> Elizabeth B. Bazan and Jennifer K. Elsea, *Presidential Authority to Conduct Warrantless Electronic Surveillance to Gather Foreign Intelligence Information*, Congressional Research Service, January 5, 2006.

(DOJ).<sup>97</sup> Though Eastman acknowledges that the reports of both the CRS and DOJ may have institutional bias, he attacks the CRS report as biased without closely looking at its content. He especially uses charged language such as “subservient”<sup>98</sup> to describe the CRS’s relationship to Congress and the formation of the service as brought about by Congressional “client[s].”<sup>99</sup> On the other hand, he never calls the Executive Branch clients of the DOJ report, and he simply affirms that “the DOJ’s conclusions are much better grounded . . . than those reached by the authors of the CRS report.”<sup>100</sup> Behind Eastman’s name-calling, however, is no real argument. His *ad hominem* way of attacking the source of an argument instead of its content foreshadows the rest of what he says on the matter.

(b). *Jackson’s Framework of Executive Power in Youngstown*—Having disenfranchised the CRS because of its Congressional tilt, Eastman goes on to consider the DOJ report, though it answers only to the Executive and thus could be criticized in the same fashion. He analyzes the famous Supreme Court case *Youngstown Sheet and Tube Co. v. Sawyer*,<sup>101</sup> in which the Court rebuffed President Truman’s attempt to seize private property in a time of emergency. Justice Jackson’s opinion, though only a concurrence, contains a system by which to gauge Executive power that is still used to this day. Justice Jackson writes that “the actual art of governing under our Constitution does not and cannot conform to judicial definitions of the power of any of its branches based on isolated clauses or even single Articles torn from context.”<sup>102</sup> To that end, he devises a framework which describes when the President’s power is at its zenith, when it is at an unclear level of ambiguity, and when it is at its lowest level. In Category I, in which the President acts in concert with Congress, his power is at its highest.<sup>103</sup> In Category II, the President acts neither with nor against Congress, and Jackson writes that in this category “there is a zone of twilight in which he and Congress may have concurrent authority, or in which its distribution is uncertain.”<sup>104</sup> Lastly, Category III is when the President’s power “is at its lowest ebb,” and is in effect when the President acts against the will of Congress, either stated or implied.<sup>105</sup> So the President’s power does not stand on its own authority under the Constitution, but instead is fundamentally connected to Congress.

97 U. S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President*, January 19, 2006.

98 John C. Eastman, *Listening to the Enemy: The President’s Power to Conduct Surveillance of Enemy Communications During Time of War*, ILSA J, INT’L & COMP. L. 2, 13-1 (2006).

99 *Id.* at 3.

100 *Id.*

101 *Youngstown Sheet and Tube Co. v. Sawyer*, 343 U. S. 579 (1952).

102 *Id.* at 635.

103 *Youngstown Sheet and Tube Co. v. Sawyer*, *Supra* note 100, at 635.

104 *Id.* at 637.

105 *Id.*

Eastman's reading of *Youngstown* advances quite a different conclusion. He describes the President's authority under the first category, which is acting pursuant to Congress, as the time when his power is obviously most clear. However, he describes the President's power under the second category, which is in the absence or silence of Congress, as "no less certain"<sup>106</sup> than under the first category. In reality, Jackson clearly describes the President's power under this second category as a "zone of twilight," and the distribution of power between the President and Congress as "uncertain," the exact opposite of what Eastman makes it out to be. Eastman claims that the DOJ's reasoning is compelling, but his own defense of Presidential authority is better described as contradictory. It is in the third category where Eastman's description most differs from Jackson's. Jackson's point is that under Category III, the President's power is at its lowest. Eastman argues this to mean that the President still has his own constitutional powers, which is true, of course; however, the message of this opinion is not, as Eastman states, that "Congress cannot pass a law that curtails Presidential powers which come directly from the Constitution itself."<sup>107</sup> Eastman uses Jackson's framework to advance the conclusion that the President has certain inviolate authority, which cannot be encroached upon by Congressional statute, such as FISA. It is true that the President does have certain powers separate from Congress, but in steadfastly arguing this position, Eastman misses Jackson's entire point: that the legal authority of the branches of government is dynamic, relying on each branch working together, and is not decided by single clauses or Articles alone.

(c). *The AUMF: Legitimate Authorization of Electronic Surveillance?* - But which of Jackson's categories does President Bush now occupy? Eastman argues that the Authorization for Use of Military Force, (AUMF)<sup>108</sup> passed one week after the terrorist attacks of September 11, 2001, puts President Bush squarely into Category I.<sup>109</sup> Firstly, the AUMF is extremely broad, and in no specific language authorizes any type of surveillance whatsoever. Are we to assume, then, that the AUMF authorizes the President to do whatever he will in the war on terror? Clearly this line of logic could extend ad infinitum, granting the President powers that no one would concede that he has. Because of its extremely broad nature and severe brevity (the authorization itself being only three sentences in length), the AUMF does not express the approval of Congress necessary to put President Bush's power into Category I.

Secondly, the AUMF is now more than six years old, and it no longer

---

106 Eastman, *supra* note 97, at 4.

107 *Id.* at 4.

108 Authorization for Use of Military Force, Pub. L. No. 107-40, S. J. RES. 23 (2001).

109 Eastman *id.*, at 5.

expresses the sentiment of Congress towards Bush's surveillance programs. Congress is ignorant of what exactly Bush has secretly authorized and what he has not, and has asked to be informed of how far electronic surveillance is being carried out.<sup>110</sup> In this position, it makes no sense to say that Bush's power is at its zenith. Because Congress is unaware of what Bush is doing and has in fact demanded accountability from the, Bush is now in Jackson's Category II, if not III. At best, President Bush's power is in a state of dubious unevenness.

Eastman's final legal justification for the President's surveillance comes from the Supreme Court case *Hamdi v. Rumsfeld*.<sup>111</sup> He says that the Court found that the AUMF gave the President "authority to detain U.S. citizens as enemy combatants even though such detentions were not explicitly authorized."<sup>112</sup> Here Eastman is clearly wrong; in fact, the Court vacated and remanded the Fourth Circuit's decision to that effect. The Supreme Court found, contrary to what Eastman says, that "due process demands that a citizen held in the United States as an enemy combatant be given a meaningful opportunity to contest the factual basis for that detention before a neutral decision maker."<sup>113</sup> Eastman then finally ties his argument back to surveillance, saying that if the President has the authority to detain citizens (a premise already invalid), he surely has the authority needed for "the much lesser intrusion on personal liberty at issue with surveillance of international calls made to or received from our enemy."<sup>114</sup> However, the issues of holding citizens who have been labeled enemy combatants by the government and surveillance are in no way related. Eastman's legal argument is based on faulty evidence, and the way it proceeds is no better. With nothing more than his own opinion that the government should be able to conduct surveillance, Eastman's argument crumbles.

(d). *Necessity versus the Law* - Eastman next takes a new tact, arguing that the President's surveillance is not only legal, but necessary. With the attacks on America on September 11, 2001, Eastman states that America has become a "theater of war," and that "the full panoply of presidential powers in time of war comes into play . . ."<sup>115</sup> However, the Constitution clearly delegates the power to declare war to Congress,<sup>116</sup> and Congress has made no such declaration of war. A vague "war on terror" does not give the President any special wartime powers any more than America's

---

110 This refers to the repeated attempts of Congressmen to learn from Alberto Gonzales how far surveillance was being carried out at one of their only opportunities to fully discuss the issue, at Gonzales's hearing before the U. S. Senate Judiciary Committee, referenced earlier in this paper (see *supra* note 10.) Gonzales refused to answer questions about any program other than the President's Terrorist Surveillance Program, making it impossible to know how much surveillance is actually being conducted by the Administration (see pages 43-44).

111 *Hamdi v. Rumsfeld*, 542 U. S. 507 (2004).

112 Eastman *supra* note 97, at 5.

113 *Hamdi v. Rumsfeld id.* at 509.

114 Eastman, *supra* note 97, at 5.

115 Eastman, *supra* note 97, at 5.

116 U.S. CONST. art. I, § 8.

war on drugs or war on crime. After all, terror itself is a concept or an ideology, not an entity. Finally, Eastman mentions John Marshall's famous quote before the House of Representatives, repeated by the Court in *United States v. Curtiss-Wright*: "The President is the sole organ of the nation in its external relations, and its sole representative with foreign nations."<sup>117</sup> Eastman says:

As 'sole organ' in the foreign affairs arena, the President has inherent constitutional authority—indeed, the constitutional duty—to conduct surveillance of communications with enemies of the United States and people he reasonably believes to be working with them, in order to prevent attacks against the United States.<sup>118</sup>

However, *Curtiss-Wright* uses the phrase to say that the President has the sole authority to negotiate treaties.<sup>119</sup> Clearly, extrapolating this to all areas of foreign policy would be a bad application of the case's precedent.

Space does not allow one to flesh out the entirety of Eastman's argument. Ultimately, his thesis is that surveillance is necessary in the war against terror, and for this reason it is legal under the Constitution. However, with controversy swirling around every facet of the Administration's newly discovered electronic surveillance programs, there is no agreement that surveillance is legal, or even that it is necessary. Eastman places undue emphasis on necessity, and in so doing inevitably relegates the role of the law to a non-compelling concern. Because what is necessary is open to debate, it should never serve as such a weighty legal justification for the actions of the government. Instead, the law should serve as the guide for what the President, or anyone for that matter, is free to do. Disagreement in that arena can be settled by the courts.

2. *Robert Turner: (a). The Founders' Conception of Executive Power* - Belonging to the same school of thought as Eastman is Robert F. Turner, a Revolutionary period scholar and distinguished professor at the University of Virginia School of Law. Turner argues in favor of very broad presidential authority in all foreign affairs issues, and is a strong proponent of the President's inherent power to conduct surveillance that involves foreign concerns in almost any way. He bases his argument on the interpretation that the Constitution gives the Executive nearly exclusive control over all foreign affairs, including, of course, surveillance that is not purely domestic. His ideas are buttressed by many quotes from founding fathers and Supreme Court opinions from the time of the Constitution's ratification. For example, in a debate series<sup>120</sup> on the issue, Turner mentions Benjamin Franklin,

---

<sup>117</sup> Eastman, *supra* note 97, at 3-4.

<sup>118</sup> *Id.* at 7.

<sup>119</sup> *United States v. Curtiss-Wright Expo. Co.*, 299 U. S. 304, 319 (1936).

<sup>120</sup> Turner, *supra* note 11.

John Jay and the other authors of *The Federalist Papers*, Washington, and Jefferson. All, he argues, in one way or another advocated a singular power, the Executive, in the foreign affairs theater. To the same effect, in a hearing<sup>121</sup> before the House Judiciary Committee, Turner recalls the *Curtiss-Wright* case from 1936. He quotes the Court:

Not only, as we have shown, is the federal power over external affairs in origin and essential character different from that over internal affairs, but *participation in the exercise of the power is significantly limited*. In this vast external realm, with its important, complicated, delicate and manifold problems, the President alone has the power to speak or listen as a representative of the nation. He makes treaties with the advice and consent of the Senate; but he alone negotiates. *Into the field of negotiation the Senate cannot intrude, and Congress itself is powerless to invade it.*<sup>122</sup>

Turner goes to great lengths in order to show that the President is constitutionally the sole agent of the country in all foreign affairs, and other branches of government thus cannot encroach upon that authority.

*(b). Executive Authority of Just Congress's Lack Thereof?: Turner's Misapplication of Legal Restraints on Congress* - Turner next tries to connect this conclusion to FISA in order to show that it actually is not in agreement with the Constitution, and is thus invalid. For if Turner disarms the legal force of this statute, he will disarm much of the legal argument against the President's surveillance programs. He claims, "I believed FISA was unconstitutional when I first read it as a Senate staffer thirty years ago,"<sup>123</sup> and even titles one of his headings in his hearing before the Senate Judiciary Committee "FISA Was Essentially a Gentleman's Agreement Between Congress and President Carter."<sup>124</sup> However, Turner's entire argument contains a subtle logical flaw. Turner attempts to prove that the President has the singular authority to conduct all foreign affairs policy, and that the other branches of government cannot interfere. However, all his evidence actually only supports the claim that other branches of government cannot conduct some foreign policy that the President can. In other words, there exists the possibility that there is some sort of foreign policy which is prohibited by the Constitution, and which the Legislative and Judicial Branches, or even the Executive, cannot conduct. Warrantless electronic surveillance which involves Americans in the United States, though it may also involve foreign concerns, is this category. The Fourth Amendment and FISA condemn such surveillance as illegal.

*(c). Airport Security Comparison* - Turner does not base his entire argument on old

<sup>121</sup> *Id.*

<sup>122</sup> *Id.* at 10-11 (emphasis added by Turner himself).

<sup>123</sup> Turner, *supra* note 11, at 5.

<sup>124</sup> Turner, *supra* note 11, at 35.

evidence, however. In defending electronic surveillance as reasonable search and seizure,<sup>125</sup> he draws a comparison to airport security searches. In a discussion with other experts, Turner posed the argument:

Every time any of us goes to the airport we get our baggage and our persons searched. That's a 4<sup>th</sup> Amendment search and the Court held that, because of a threat of a high jacked airliner or an exploded airliner is so great, the search is per se reasonable...So I just don't see the problem here.<sup>126</sup>

However, Turner's comparison between airport searches and electronic surveillance is a bad one for at least two reasons. Firstly, passengers at an airport are aware of being searched, and they know to what extent. Electronic surveillance is clearly not the same: one is not aware of how often, to what extent, or if at all one is being monitored. Secondly, airport searches are optional. If a person objects to such searches, he may choose other means of travel. However, again, electronic surveillance is not the same: someone cannot simply choose not to have his communications secretly monitored by the government. And as Turner's comparison of the issues is weak, so then is his legal justification, the 1974 case *United States v. Edwards*,<sup>127</sup> in which airport searches were found to be constitutional under the Fourth Amendment.

3. *Former Attorney General Alberto Gonzales: Wordplay and Deceit* - An examination of those who claim that the President's surveillance activities are legal would be incomplete without considering what the Attorney General has said on the subject. During his February 6, 2006 hearing before the Senate Judiciary Committee, Alberto Gonzales consistently defended the NSA Terrorist Surveillance Program (TSP) as legal under both the Constitution and FISA. Unlike Turner, Gonzales did not argue that the President had the inherent authority to conduct surveillance in contradiction to FISA. Instead, he said, "I've tried to make clear today that we looked at this issue carefully, decided that neither the Constitution nor FISA, which contemplated a new statute, would prohibit this kind of activity from going forward."<sup>128</sup> Exactly what type of surveillance activity is Gonzales talking about? In his testimony, Gonzales makes several large scale denials of driftnet type

---

<sup>125</sup> The distinction of "reasonable" from "unreasonable" searches is important because the Fourth Amendment reads, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." So, if a search is considered reasonable, it may not violate the Fourth Amendment.

Robert F. Turner, *Surveillance, new executive powers, and how the Democrats got blindsided*, The Scribe, August 7, 2007. Available at [prairieweather.typepad.com/the\\_scribe/2007/08/surveillance-ne.html](http://prairieweather.typepad.com/the_scribe/2007/08/surveillance-ne.html).

<sup>126</sup> *Id.*

<sup>127</sup> *United States v. Edwards*, 498 F.2 d 496 (1974).

<sup>128</sup> Hearing, *supra* note 10.

surveillance. However, each time he does so, he is sure to attach the words “this program,” meaning the TSP. When asked by Senator Feinstein, “Has the president ever invoked [any other secret order or directive] with respect to any activity other than the program we’re discussing, the NSA surveillance program?” Gonzales refused to answer.

In an interview with “Spying on the Homefront,” Swire suggests that Gonzales’s denials of illegal surveillance were not true denials, but only a careful semantic distraction, a word game. Swire says:

I looked at the Attorney General’s testimony very carefully, and every time he gave the big denials, they were attached to the words “this program.” . . . the Attorney General was speaking very carefully, but I think there could be lots of room after you read his testimony for *other programs* to be doing really unprecedented things.<sup>129</sup>

In a letter following his testimony, the *Washington Post* reports that Gonzales wrote, “I did not and could not address [ . . . ] any other classified intelligence activities [ . . . ] I was confining my remarks to the Terrorist Surveillance Program as described by the President.”<sup>130</sup> The article continues to quote former government lawyer Bruce Fein, saying, “it seems to me he is conceding that there are other NSA surveillance programs ongoing that the president hasn’t told anyone about.”<sup>131</sup> It would seem that the Administration has selected a certain surveillance program, termed the TSP, and testified that this one program is not in contravention of the law. However, many other programs, such as the kind of which Mark Klein found evidence in his workplace at AT&T, may very well be in full operation. Purely domestic, driftnet electronic surveillance may be taking place under a secret government program, different from the TSP. Since the Administration does not reveal the scope of its surveillance, there is no way to know how much surveillance, legal or not, is now being conducted.

### *B. Critics of Electronic Surveillance*

*1. The Law Exists Even for Times of Necessity* - The arguments of those, on the other hand, who argue that the President’s surveillance is illegal, are less complicated.

---

<sup>129</sup> Spying on the Home Front: An interview with Peter Swire (PBS Television Broadcast January 17, 2007) Available at [www-c.pbs.org/wgbh/pages/frontline/homefront/interviews/swire.html](http://www-c.pbs.org/wgbh/pages/frontline/homefront/interviews/swire.html)

<sup>130</sup> Charles Babington and Dan Eggen, *Gonzales Seeks to Clarify Testimony on Spying: Extent of Eavesdropping May Go Beyond NSA Work*, WASHINGTON POST, March 1, 2006.

<sup>131</sup> *Id.*

Though the Patriot Act indeed amended FISA in 2001,<sup>132</sup> even such amendments do not begin to authorize some of the surveillance that has been conducted by the Executive branch in the Bush Administration. It is clear even upon cursory inspection that even with its 2001 updates, broad, purely domestic surveillance is in contravention of FISA. And unless a court ruling changes the meaning of what we regard as an “unreasonable” search, such warrantless surveillance is still illegal under the Fourth Amendment. Even if advocates of the legality of the Bush Administration’s surveillance programs and the Administration itself claim that such surveillance is necessary to the safety of the nation, actions which are in disaccord with the law are not desirable. If it was in fact clear that the warrantless electronic surveillance was necessary, surely it would not be a problem to pass legislation that allowed it. However, with no consensus in Congress that such necessity does in fact exist and no new ruling on the issue by the courts, it is manifestly unclear as to whether this surveillance is truly necessary, as the President claims that it is.

2. *The AUMF Does Not Mention or Approve of Electronic Surveillance* - The AUMF, the Congressional authorization and approval that the Administration cites as part of its legal justification for the President’s surveillance programs,<sup>133</sup> does not even mention surveillance. Katherine Wong observes of the critics of the surveillance’s legality, “they cite the analysis in *Youngstown* in which general statutory language (such as the AUMF) authorizes nothing when Congress has already spoken on the issue, especially when it has done so through a carefully drawn statute such as FISA.”<sup>134</sup> Yet Congress has not made a significant attempt to curtail the President’s surveillance. William Banks even goes so far as to say that “Congress essentially ceded its role in crafting legislation and in national leadership, while the executive branch seized the initiative to fight the global war on terror at home and abroad with the tools it could fashion.”<sup>135</sup> Congress has indeed largely taken the role of spectator towards the issue, failing to collectively demand real accountability from the Executive.

---

132 Peter Swire lists the three changes of the Patriot Act which granted the President the most new authority as “the permission for FISA orders to have only a ‘significant purpose’ of foreign intelligence; the use of FISA orders to get any ‘tangible object,’ and the expansion of national security letters.” (“The System of Foreign Intelligence Surveillance Law,” 38) These changes were important ones, perhaps even drastic steps, but they do not begin to include the broad surveillance of the Bush Administration, especially the driftnet type programs, like one discussed earlier in association with AT&T.

133 Alberto Gonzales, in a prepared statement, says “the NSA’s focused terrorist surveillance program falls squarely within the broad authorization of the AUMF . . .” (Alberto Gonzales, *Prepared Statement of Hon. Alberto R. Gonzales, Attorney General of the United States*, February 6, 2006. Available at [www.usdoj.gov/ag/speeches/2006/ag\\_speech\\_060206.html](http://www.usdoj.gov/ag/speeches/2006/ag_speech_060206.html)) This idea has always underpinned the Administration’s legal justification of the TSP. See pages 38 and 39 for a discussion of the AUMF’s overbroad nature and failure to mention surveillance in any way, and how it places the President into Jackson’s Category II, if not III, from *Youngstown*.

134 Katherine L. Wong, *The NSA Terrorist Surveillance Program*, Harvard Journal on Legislation 43, no. 2 (2006): 525. In this quote Wong cites through footnotes J. Frankfurter’s concurrence in *Youngstown* and also notes that “the legislative history and context of FISA’s enactment suggest FISA was carefully constructed”.

135 William C. Banks, *The Death of FISA*, MINN. L. REV. 91 (2007): 1212.

3. *The Responsibility of Presidential Accountability* - Perhaps providing accountability is the President's own responsibility. Jack Goldsmith argues that President Bush is not alone among Presidents in taking measures that were technically against the law, but ones he thought necessary for the greater good of the nation. In a meeting with Gonzales and Addington, Goldsmith once explained that the President had the option to act extralegally. An ideology rooted in legal reasoning from Locke and Jefferson, Goldsmith tells in his book that it has been acceptable in the past, and ostensibly still would be today, to break a law. But, there is an important caveat; Goldsmith says that "in order to prevent abuse, the leader who disregards the law should do so publicly, throwing himself on the mercy of Congress and the people so that they could decide whether the emergency was severe enough to warrant extralegal action."<sup>136</sup> Goldsmith lists the example of Lincoln, who acted glaringly in disregard of the Constitution in at least six different ways, from asserting powers the Constitution allotted to Congress to even ignoring Supreme Court orders.<sup>137</sup> "No President before or since Lincoln has acted in such disregard of constitutional traditions,"<sup>138</sup> he writes. When seen in this light, perhaps Bush's transgressions of FISA and the Fourth Amendment are not so unprecedented.

However, Goldsmith tells that "Lincoln nonetheless informed Congress about all of these acts, publicly defended them as necessary to meet the crisis, and asked Congress to approve them."<sup>139</sup> Lincoln even waited until Congress was in session before acting, so that they could officially either approve or reject his plans of action.<sup>140</sup> Roosevelt in the same way took action he thought necessary to win the war of his time. Goldsmith writes that Roosevelt compromised with Congress by asserting his power "in a way that forced Congress itself to act,"<sup>141</sup> and he was "extremely reluctant"<sup>142</sup> to take action that normally fell to the legislature; breaking away from the past. Senior members of Bush's Administration, such as Vice President Cheney and his advisor Addington, have long since had an "underlying commitment to expanding presidential power" that "distinguishes the Bush Administration from the Lincoln and Roosevelt Administration s."<sup>143</sup> It was this attitude, perhaps, that contributed to President Bush feeling that he, unlike Lincoln and Roosevelt, did not have to reveal his lawbreaking to Congress and to the people, especially if "national security" serves as his panacea to all legal criticisms. Bush does not belong to the presidents who have had the courage to break the law and throw themselves on the

---

136 Goldsmith, *supra* note 64, at 81.

137 *Id.* at 82.

138 *Id.* at 82.

139 *Id.* at 82-83.

140 *Id.* at 85.

141 *Id.* at 85.

142 *Id.* at 84.

143 *Id.* at 89.

mercy of the people for it. He takes the credit for keeping America strong, yet he flees the legal consequences of the means he has supposedly used to bring about that goal.

## CONCLUSION

Ever since it was made public in 2005, Bush's Terrorist Surveillance Program has become the subject of much discussion and criticism in both the public sphere and the legal community. It appears that there are programs which go beyond the scope of the TSP, programs which engage in domestic data mining and electronic surveillance on a large scale. America has seen widespread domestic surveillance before, and it has also seen presidents seize powers which were not lawfully theirs. However, the Bush Administration has gone further than before in both capacities by ordering even wider surveillance than has occurred in the past with the help of new technologies, and by keeping its activities secret, even during active investigation. As an administration obsessed with fear delivered from a daily threat matrix and a lethargic Congress and citizenry, the Church Report and legislation from three decades past may not see their current day counterparts.

Brian Decker writes of those who conduct government electronic surveillance, "if their interference with the private conversations of innocent individuals is minimized, and if they appropriately target those who harm society, wiretaps by law enforcement officials are so effective and vital that the risk of use is acceptable."<sup>144</sup> And so responsible legal thinking has been replaced with a sort of cost/benefit analysis, weighing necessity and the safety of the nation against inflexible laws. In fact, electronic surveillance poses a far more vast scope than Decker supposes, and history demonstrates examples of continuing expansion and abuse. The core of the argument of advocates of surveillance is that it is necessary for the protection of the nation. However, law and necessity are not mutually exclusive. Were the necessity so clear and so compelling, America undoubtedly would already have laws in place granting the President all the legal authority needed to carry out electronic surveillance, even if it meant amending FISA and changing the present interpretation of the Fourth Amendment.

However, until the law is changed, the law holds. If the President chooses to act in disregard of the law, he simply cannot do so in secret. Even if he means well and is firm in his conviction, it is exactly this scenario and its potential for abuse that the Constitution anticipates and proscribes through its mandate of checks and balances. In the future, America might decide that the protection electronic

---

<sup>144</sup> Brian R. Decker, *'The War of Information': The Foreign Intelligence Surveillance Act, Hamdan v. Rumsfeld, and the President's Warrantless Wiretapping Program*, U. PA. J. CONST. L. 9, (2006): 2.

surveillance affords is worth the imposition upon civil liberties and potential for abuse that it risks. Congress could possibly pass a law granting the President the power to engage in the kind of surveillance President Bush already does, or the Supreme Court could rule that warrantless computer analysis of domestic communications is not “unreasonable” under the Fourth Amendment or a broach of reasonable expectation of privacy. However, that time has not yet come.

Among the theoretical pillars upholding the society and the nation of America are those of liberty and justice. As Americans we are proud to be a nation of laws, not of men. Ironically, it may be when the laws are broken in the name of the nation’s security that justice and liberty are most in peril. Abraham Lincoln (coincidentally one of Bush’s great heroes<sup>145</sup>) famously said “America will never be destroyed from the outside. If we falter and lose our freedoms, it will be because we destroyed ourselves.” Let us hope that President Bush’s disregard for law does not set a presidential precedent that finally leads to our unraveling.

---

<sup>145</sup> Michael A. Fletcher, *Bush Honors President Lincoln*, Washington Post April 20, 2005—Bush’s aides say that he admires Lincoln more than any other president. Also: Kenneth T. Walsh, *Bush’s reading list: heavy on bios and baseball*, U. S. News and World Report August 17, 2006—Lincoln is called Bush’s “political hero.”