Lighting the back alleys of the Internet: A review of Barack Obabma's surveillance policies against the background of the national security state

by Sunny Skye Hughes
Assistant Professor of Communications and Journalism
College of Liberal Arts and Sciences
University of Maine

As the ten-year anniversary of the September 11th terrorist attacks on the World Trade Center draw near, the United States government has announced it killed public enemy number one, Osama Bin Laden. As the mastermind of the attacks, Bin Laden's war on the west has been cited in post 9/11 rhetoric as justification for expanded surveillance powers in America, often at the expense of long-recognized protections for civil liberties. Although many covert surveillance programs have existed for decades, the expansion of these programs under former President George W. Bush was well publicized in the U.S. media, leading to calls to limit presidential wiretapping powers that encroached upon constitutional protections for privacy and free speech. In both political rhetoric and mainstream news accounts, these measures were said to be necessary to secure the safety of the American people. The "War on Terror" is not a traditional war, but also an ongoing ideological battle against Bin Laden's Al Qaeda and other terrorist organizations. President Bush first declared this war on September 20, 2001, in a speech to Congress where he identified the terrorists responsible for the attacks as "heirs of all the murderous ideologies of the 20th century… sacrificing human life to serve their radical visions." During the 2008 election cycle, presidential candidates, including Barack Obama, hotly debated the War on Terror and the expanded surveillance powers that came with it. To an extent, the War on Terror was seen as a temporary political strategy that might come to an end with the dismantling of Al Qaeda, or possibly with the political change brought by the inauguration of a new president. Rather than end, surveillance programs under the current American President Barack Obama have continued and to an extent, expanded.

This paper offers a review of Obama's surveillance policies, beginning in 2004 before he was sworn in as a U.S. Senator. By examining the current President's speeches, Congressional votes and laws signed during his tenure, as well as other legal actions, a comprehensive analysis of his surveillance policies begin to emerge. While election promises made by Obama led many to think he would end the Bush era wiretapping policies, the record shows that the current U.S. president has in many ways continued the legacy of his predecessor. This is hardly groundbreaking information, but it does reveal certain patterns in U.S. surveillance policy that move the country towards what can be called a "security state." In an 18-month review of the Obama Administration, the American Civil Liberties Union suggested that the Administration presided over a "new normal" where "adherence to our nation's fundamental principles make us safer, not less safe," (ACLU, p. 2). The audit suggested that the current Administration's stance on civil liberty and national security issues continued practices considered "extreme and unlawful" under the previous administration. The audit went on to say the Obama Administration was "reluctant to yield any of the expansive surveillance powers claimed by the Bush Administration (p. 16). Rather than a temporary period of increased security and surveillance, this period in U.S. history follows historical trends in the expansion of surveillance initiatives.

This paper will review Obama's record on surveillance through the lens of Harold Lasswell's theory of a security state where civilian supremacy and individual liberties are eroded at the hands of a security elite. Lasswell, writing in the 1950's, identified communism as an ominous force leading to a world crisis of insecurity. Lasswell suggested this crisis could last for a generation. Over sixty years later, terrorism now stands in for communism as the national threat, but also as the foil to civilian supremacy and individual liberty that Lasswell identified as key principles in our democracy. This paper will review the concept of a security state, before reviewing Obama's policies to demonstrate that the latest

Administration's actions are just a continuation of the United States's transition to a security state—the "new normal."

The Security State
Threats to Free Society: The Garrison State

Harold Lasswell, when cited for surveillance, is most often referenced for his theory of media functions where media conduct surveillance of society, however, in the mid-20th century he identified the "continuing crisis of national defense" and addressed the delicate balance between national security and individual freedom (Lasswell, 1950, p. 1). Although much of Lasswell's analysis is based on the Cold War struggles of an America trying to suppress communism, the theories he advances in the 1950 book, *National Security and Individual Freedom,* can easily be applied to our contemporary national circumstances by replacing the threat of "communism" with the threat of "terrorism". Lasswell said the solution to balancing national security and individual freedom was finding a way to "endure the crisis with the least loss of fundamental freedoms," (p. 1). Lasswell was firm in saying the world crisis of insecurity could last for a generation, with public alarm about the danger of war rising and falling with the headlines.

Lasswell developed the communication theory of interacting systems, saying that individuals should have an increased role in controlling the governing process. This individual control is a response to what Lasswell described as a "central nervous system" controlling the country's communications. Lasswell said that civilian supremacy is a "characteristic of democratic government" evident in the intentions of the forefathers to protect individual freedom against "arbitrary official action." Lasswell said that the First Amendment is most the most essential protection of the political process because it guarantees free expression. During Lasswell's time, courts used the "clear and present danger" test to evaluate First Amendment protections for speech tempered by national security concerns. Lasswell said that the application of this test required an "independent estimate of the necessities of the situation." This estimate is only possible if the courts have all the information about the programs that may be limiting constitutional rights. Lasswell urged continued judicial review of such information through the "National Security Council" in order to limit security threats. Lasswell said that relying upon judicial interpretation would limit the abuse of power by a garrison state. Lasswell said that when intelligence agencies are allowed to operate beyond judicial review, civil liberties might be threatened by political agendas.

Lasswell introduced four principles to generally govern national security programs and protect against the move towards a Garrison State:

> Is there a threat to the principle of civilian supremacy in the U.S. system of government?
> Does the policy involve a threat to freedom of information and disclosure of government activities?
> Is there danger to the civil liberties of the individual?
> Does the policy violate the principle of a free—as opposed to a controlled—economy?

For the purposes of this paper, only the first three principles will be reviewed, as the fourth is outside of the scope of this paper. Lasswell said that an affirmative answer to any of these questions triggers a "potential loss of freedom," which can be avoided or reduced by changing the national security program in question. Lasswell said reducing the reach of government security programs might preserve the American goal of individual dignity.

The Security Elite

Harold Nagan and Craig Hammer applied Lasswell's concept of interacting systems to international law and communication, placing a greater emphasis on the role and contributions of the individual. Lasswell describes a "central nervous system" controlling the state's communications. Nagan and Hammer suggest that a "security elite" has stepped up to fill this roll, as they manage war, in addition to security. This security elite is made up of intelligence organizations and military officers, often operating without the consent, or even direct knowledge of state sovereigns.
The authors also apply Lasswell's classic communication model to all levels of law, providing a framework for legal analysis:

> Who created the law? A government official, judge, administrator, legislator, international civil servant? Which states support the law?
> What does the law say? What are the "expectations for future conduct?"
> To whom is the law addressed? Who is the target of the law and who must follow it?
> In what channel is the law communicated to the audience?
> What is the effect of the law? Are new expectations created?

The National Surveillance State

Beyond Congressional law making, agency expansion and subsequent actions can also signal the move towards a security state. The National Security Agency's post 9/11 surveillance programs can be seen as part of a new, twentieth century form of governance known as the "National Surveillance State," that "was already well in gear" in the 1990s, (p. 3, 7). Jack Balkin conceptualizes and identifies this state as a government that "uses surveillance, data collection, collation, and analysis to identify problems, to head off potential threats, to govern populations, and to deliver valuable social services," (p. 3). Balkin argues that the National Surveillance State is "neither the product of emergency nor the product of war," both being temporary conditions. Rather the Surveillance State is a necessary evolution in governance, where surveillance is conducted and analyzed by private parties, and the line is "blurred" between public and private surveillance (p. 4,7).

One tactic of the National Security State is "expanding intelligence agencies," (p. 6). Balkin metaphorphically compares the National Security State to the Welfare State; whereas the Welfare State spurred the demand for data processing technologies used to identify individuals, the National Security State creates the need for "effective intelligence collection and data analysis," (p. 6). This facilitates the use of "prediction and prevention" technologies, which augment the traditional model of "prosecution and deterrence," (p. 10). Prediction and prevention, hallmarks of the security state, are achieved through the use of database collaborations between private companies and government agencies, (p.10). Balkin suggest that by employing ubiquitous surveillance methods, "governments and private organizations could discourage behavior they deemed unusual or abnormal,' (p. 12). This "ubiquitous" surveillance goes beyond the watching and measuring that Michael Foucault envisioned in his interpretation of Jeremy Bentham's Panopticon model. The National Surveillance State's most important technique of control is "analyzing and drawing connections between data," (p. 12) that can be used to make inferences about a person's "motives, desires, and behaviors," (p. 13). Balkin goes so far as to say, "As technology improves and storage costs decline, the National Surveillance State becomes the State that Never Forgets," (p. 14).

Balkin identifies three major dangers that the National Security State poses to freedom:
The government will create a parallel track of preventative law enforcement that routes around the traditional guarantees of the Bill of Rights. Through the emphasis of "ex ante prevention rather

than ex post apprehension and prosecution," (p. 15). He references the NSA's surveillance program as an example of this sort of danger where the president was using military intelligence to fight terrorism, rather than engaging in criminal prosecutions (p. 16).

Traditional law enforcement and social services will "increasingly resemble the parallel track" as the government uses its political power to normalize the use of surveillance and data mining technologies in "everyday" law enforcement (p. 16). As an example, Balkin suggests that surveillance technologies could identify suspects who threaten security and create a "system of preventive detention outside the ordinary criminal justice system," (p. 16).

Government reliance on private parties to collect and generate information is incentivized because private companies are not bound by the Constitution (p. 16). Collection of customer data by private companies is also incentivized because they can sell the information they collect to the government (p. 17).

Balkin says "authoritarian states are information misers because they try to keep the information they collect—and their own operations—secret from the public (p. 17). Embarrassing information is treated as a "state secret" thus allowing the government to "avoid accountability for violating people's rights and for their own policy failures" p. 17).

A Review of Obama's Surveillance Policies

Obama as Candidate and Senator

On July 12, 2004, a couple of weeks before he would deliver his historic keynote address at the Democratic National Convention, Barack Obama issue a press release saying,

"We should strengthen and improve intelligence capabilities. We must reform our domestic intelligence capabilities in a manner that balances the risks of impeding on the civil liberties of our citizens and increase international cooperation on all fronts. We should also give the Director of Intelligence the authority he or she needs over budget and personnel to be effective and accountable," (Renewal Press Release, 2004).

Barack Obama was still months away from being sworn in as the United States Senator from Illinois, but as a candidate, he was identifying the important balance that exists between intelligence gathering and civil liberties. This balance, identified by Lasswell as national security versus individual freedom, is reflected in Obama's statement, which calls for the Director of Intelligence to oversee government actions in monitoring the "central nervous system" of American communications. However, the oversight by the Director of Intelligence, and not the state sovereign—the President—seems to indicate a shift toward intelligence oversight by the "security elite" identified by Nagan and Hammer. This intelligence oversight also heralds the expansion of intelligence agency powers developed by Balkin as a criteria in his National Security State.

Patriot Reauthorization Act of 2005

Obama won the race for Senate and a year later found himself a member of the Congress that approved the PATRIOT Reauthorization Act (H.R. 3199) in July of 2005 (The Senate bill was S. 1389). The USA PATRIOT Improvement and Reauthorization Act of 2005 made permanent many of the sunset provisions built into the PATRIOT Act of 2001, including:

1) section 203 regarding information sharing by law enforcement;
2) section 207 regarding the duration of wiretaps;
3) section 209 regarding the seizure of voice mail;
4) section 212 regarding emergency disclosures of communications content or related records to

authorities;
5) section 214 extending the use of pen registers to Internet communications;
6) section 218 regarding the FISA wall between criminal and foreign intelligence investigations; and
7) section 225 providing telecommunications carriers immunity when executing a FISA warrant.

Two provisions, section 206 governing FISA court orders for roving wiretaps and section 215 governing access to business records requested under FISA were extended to sunset on December 31, 2009.

The 2005 PATRIOT Act amendment requires the Attorney General to include additional information in his semiannual report to Congress, including not just the number of requested and approved warrants for FISA-authorized surveillance, but also the number of requests "granted, modified, or denied for the production of library records, book sale records, firearm sale records, tax return records, educational records and medical records." Additionally, the 2005 PATRIOT Reauthorization Act expanded the types of offenses that trigger the authorization to obtain a court order for wire, oral or electronic wiretaps. The expanded list of crimes include activities relating to: 1) biological weapons; 2) violence at international airports; 3) nuclear and weapons of mass destruction threats; 4) explosive materials; 5) receiving terrorist military training; 6) terrorist attacks against mass transit; 7) arson within U.S. special maritime and territorial jurisdiction; 8) torture; 9) firearm attacks in federal facilities; 10) killing federal employees; 11) killing certain foreign officials; 12) conspiracy to commit violence overseas; 13) harboring terrorists; 14) assault on a flight crew member with a dangerous weapon; 15) certain weapons offenses aboard an aircraft; 16) aggravated identity theft; 17) "smurfing," a money laundering technique involving a large monetary transaction that is separated into smaller transactions to evade federal reporting requirements on large transactions; and 18) criminal violations of certain provisions of the Sherman Antitrust Act.

While the bill was awaiting the President's signature, Obama, in a Senate floor speech on December 15, 2005 spoke on an issue that would become a national scandal in the following days. Obama said, "soon after the PATRIOT Act passed, a few years before I ever arrived in the Senate, I began hearing concerns from people of every background and political leaning that this law didn't just provide law enforcement the powers it needed to keep us safe, but powers it didn't need to invade our privacy without cause or suspicion. Supporters of this Conference Report have argued that we should just hold our noses and support the legislation, because it's not going to get any better. That does not convince me that I should support this report. I believe we owe it to the nation to do whatever we can to make this legislation better. We don't have to settle for a PATRIOT Act that sacrifices our liberties or our safety - we can have one that secures both. I Voted YES on reauthorizing the PATRIOT Act but I voted NO on extending the PATRIOT Act's wiretap provision," (Senate Floor Speech, December 15, 2005).

Obama's statement, much like his 2004 press release reflects his desire to achieve the Lasswellian balance of security and freedom by revising the PATRIOT Act to keep America safe, while also honoring individual privacy. The 2005 Act passed the House 257-171, with 214 Republicans and 43 Democrats voting in favor. The Act unanimously passed the Senate. The original purpose of the PATRIOT Act (2001) was to "deter and punish terrorists acts in the United States and around the world," and "to enhance law enforcement investigatory tools." The law outlines future conduct for law enforcement officials and therefore is addressed to both federal agents, as well as terrorist who might pose harm to America. Additionally—and most importantly to this analysis—the law was addressed to American citizens, who would surrender some privacy protections in the War on Terrorism. During the summer of 2005 when Congress was considering the legislation, the American public showed awareness of the law, which seems to indicate that the law was well publicized to the American people. The Gallup organization conducted a poll in June 2005 and found that 64% of Americans said they were "very" or "somewhat" familiar with the law, while a quarter of those polled said they were "not

too familiar." In looking at the effects of the law, the first Lasswellian principle to govern national security programs can be applied to evaluate the threat to the principle of civilian supremacy. As described by Lasswell, civilian supremacy is defined by checks and balances in government, limiting of peacetime armies, free flow of information to the public about defense programs and government responsiveness to the will of the people. The 2005 Reauthorization Act seems to honor this principal by providing for a check on government intelligence gathering through the requirement that the Attorney General expand his semiannual report to Congress to include more detailed information about FISA-authorized surveillance. This provision also seemed to honor the second Lasswellian principle calling for freedom of information and disclosure of government activities.

Section 225, providing telecommunication carrier immunity, is an example Balkin's incentivized danger of government reliance on private parties to collect and generate information. Section 215 can also be seen as an expansion of private party power because it allows the government to collect business records—including library patron records, tax returns, educational and medical records—from private entities that collect and store information not statutorily authorized for collection by the government. This expansion of power can also be seen in the extended section 209, allowing for the seizure of voicemail under the Electronic Communications Privacy Act, instead of the previous Wiretap Act. Whereas before, the government needed an order to intercept your voice mail, now it can be accessed with search warrants, subpoenas, or sometimes simply by asking the phone company for the records. Section 212 of PATRIOT removed the requirement that agents seek ECPA orders, warrants and subpoenas for disclosure of communication content records, instead, law enforcement agents can now acquire records as long as they convince the communication provider that there is a reasonable belief of an immediate life threatening danger if the records are not surrendered (Section 225 of the Homeland Security Act of 2002, which does not expire, changed this to a "good faith belief," changed law enforcement agents to any government entity and removed the requirement of an "immediate" threat).

Many of the PATRIOT provisions extended under the 2005 Act create what Balkin described as a parallel track of preventative law enforcement, circumventing the guarantees of the Bill of Rights. Most notably, Section 218 removes "the wall" between criminal and foreign intelligence investigations by allowing for FISA surveillance when foreign intelligence is only a partial motivation for the investigation. Furthermore, federal investigators can use national security as a justification for warrantless surveillance in criminal matters, circumventing 4th Amendment privacy protections. Under Section 214, the FBI no longer must demonstrate that a target is an international terrorist or spy in order to intercept communications, as long as the pen intercept is executed as part of an intelligence investigation. Under Section 218, the FBI does not need FISA Court approval, since the Court must issue an order if the FBI certifies the pen intercept is part of an intelligence investigation. Both of these subsections relate to another danger that Balkin described: Traditional law enforcement and social services will increasingly resemble the parallel track as the government uses its political power to normalize the use of surveillance and data mining technologies in everyday law enforcement.
The expansion of surveillance powers can be seen as the parallel track of law enforcement because they circumvent long-standing constitutional safeguards and erode the traditional wall between criminal and foreign intelligence investigations. Under Section 203, foreign intelligence information gathered in criminal investigations by domestic law enforcement agents can be shared throughout the intelligence community. Although this section can be seen as improving law enforcements' communication between agencies—a problem that many say led to the successful execution of the September 11th attacks—it also allows for more ambiguous standards in intelligence gathering and the opportunity for exploitation of less stringent standards in criminal investigations. Section 206 allows for roving wiretaps, essentially allowing FISA court orders to monitor all forms of communications and all carriers used by a single target. Since the order is targeted at a person and not a single device or line, it increases the likelihood that innocent citizens will be monitored by the government, even though they

are not investigation targets.

The third criteria Lasswell suggested was an evaluation of danger to the civil liberties of the individual. Although the PATRIOT and subsequent reauthorization Act led to a cries of civil liberty infringement by advocates, the American public does not seemed concern with the impending dangers to civil liberties. Forty-one percent of those polled said the law "is about right in terms of protecting civil liberties," but only thirty-percent felt it went too far. Of those who identified themselves as "very familiar" with the law, 45% thinks it goes to far in restricting civil liberties. The poll found that partisanship determined public opinion about the PATRIOT Act, with a third of Democrats and 40% of independents thinking it went to far in restricting civil liberties versus twelve percent of Republicans. Although the changes in the law that Obama voted for could pose danger to the civil liberties of the individual, the concern is not something that is nationally recognized by the American citizenry.

The USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006

The next PATRIOT revision introduced in the Senate was the USA PATRIOT Act Additional Reauthorizing Amendments Act of 2006, S. 2271, to safeguard civil liberties not addressed in the original bills passed in 2005. On February 16, 2006, Obama took the floor in the Senate to address the USA PATRIOT Act Reauthorization, a renewal of the USA PATRIOT Act that he said gave law enforcement the tools they needed to track down terrorist who were looking to exploit American security. Obama said that often the issue of privacy vs. intelligence degenerated into an "'either-or" type of debate framing the protection of American people against "cherished principles" (Speech, February 16, 2006). He said this "false choice" was recognized by the Senate in its 2005 debate about the PATRIOT Act Reauthorization Act, but the House's resistance to change was the reason that Congress was currently considering a compromise bill. Obama said the compromise, S. 2271, was not as good as the Senate version, nor was it as good as the SAFE Act that he sponsored, but it was better than what the House proposed because it "modestly" improved the PATRIOT Act by "strengthening civil liberties protection without sacrificing the tools that law enforcement needs to keep us safe." Obama encouraged his Congressional colleagues to "continue working on ways to improve the civil liberties protections in the PATRIOT Act" after reauthorization." On March 1, 2006, the Senate passed the USA PATRIOT Act Additional Reauthorization Amendments and Obama voted in support of the bill. Then President Bush signed the House bill and the second Senate bill on March 9, 2006.

The USA PATRIOT Act Additional Reauthorization Act of 2006 amended FISA and other federal wiretapping statutes. The 2006 Act amended five federal statutes and further clarified the use of national security letters by federal intelligence investigators. The Act gave letter recipients the right to petition a FISA judge to eliminate or modify the nondisclosure order. Section three of the Act requires a judge to conduct an initial review of the order within 72 hours of the request by the recipient of the national security letter to remove the nondisclosure requirement. The judge must provide the recipient with a written statement justifying his or her decision to modify the nondisclosure order. The judge must evaluate the requested disclosure of the existence of a national security letter to determine if it would 1) endanger national security; 2) interfere with criminal, counterterrorism or counterintelligence investigations; 3) interfere with diplomatic relations; or 4) endanger the life or physical safety of a person. If the Attorney General, Deputy Attorney General, Assistant Attorney General or FBI Director certify the letter, then the judge reviewing the order must show the federal official's decision to certify the letter was made in bad faith in order to eliminate the order. Section 4 of the 2006 PATRIOT Reauthorization Act states that recipients of national security letters are excused from having to give the government authorities the name of the attorney counselling them whether to comply with the national security letter. Furthermore, the Act revised guidelines for libraries, clarifying that services like Internet access for patrons are not subject to national security letters unless they are electronic communication service providers.

Obama's speech on the Senate floor recognizing the "false choice" between privacy and intelligence acknowledges Lasswell's solution to the security-freedom balance of enduring the security "crisis" with a minimal loss of fundamental freedoms. When he evaluated the bill, he said that it was not the ideal legislation, but it did improve civil liberty protections, while giving law enforcement important tools to fight terrorism. The Act passed the House 280-137, with 214 Republicans and 41 Democrats in favor. In the Senate, the Act passed 95-3, with 54 Republicans and 41 Democrats in favor. The Act's purpose was to "clarify that individuals who receive FISA orders can challenge nondisclosure requirements, that individuals who receive national security letters are not required to disclose the name of their attorney, that libraries are not wire or electronic communication service providers unless they provide specific services, and for other purposes." The law, like the 2005 Reauthorization Act, outlines behavior for federal agents and libraries, and is of course, addressed at American citizens. In January of 2006, another Gallup poll found that 76% of Americans polled were either "very familiar" or "somewhat familiar" with the PATRIOT Act. This seems to indicate that the government, even as Congress debated reauthorization, did a good job of communicating the law to the American public.

The 2006 Reauthorization Act provided increase protections for civil liberties, before unseen in the original 2001 PATRIOT Act, or the 2005 Reauthorization. In line with Lasswell's first principle of civilian supremacy, the 2006 Act provided better checks and balances on government intelligence gathering. For example, section three of the Act required judicial review of nondisclosure by recipients of national security letters, requiring proof that disclosure of the letter's existence would endanger national security or interfere with an investigation. This also, in a minor way, reversed the move towards a parallel track of government, providing better oversight in law enforcement intelligence gathering. This also—more so than the 2005 Reauthorization—better aligned with Lasswell's second principle of honoring freedom of information and disclosure. Furthermore, section 4 removed the mandate that national security letter recipients must give government authorities the name of their attorney.

Finally, in regards to Lasswell's third principle on civil liberties, the 2006 Act restored previously eroded First Amendment and privacy rights for library patrons by ending the use of national security letters to obtain library records. This is more in line with traditional guarantees provided in the Constitution and indicates a rejection of the parallel track of preventative law enforcement described by Balkin.

The Protect America Act of 2007

The Protect America Act of 2007 (Pub. L. 110-55) amended the Foreign Intelligence Surveillance Act by eliminating surveillance warrant requirements for foreign intelligence targets "reasonably believed" to be outside of the United States. The bill passed the Senate on August 3, 2007, and the House on August 4, 2007. Obama voted in support of the Act. President George Bush signed the bill into law on August 5, 2007. The law expired on February 17, 2008, due to a sunset clause.

On February 12, 2008, Senator Obama voted to strike provisions providing civil liability immunity to electronic service providers for assistance they provided to the government in the post-9/11 surveillance era from the original Amendment 3911 (S. Amdt. 3907). The same year, candidate Obama, continued his consistency in supporting compliance with existing laws requiring judicial warrants for national security surveillance (Boston Globe, 2008). He was quoted in a 2008 Boston Globe candidate comparison, saying, "As president, I will follow existing law, and when it comes to U.S. citizens and residents, I will only authorize surveillance for national security purposes consistent with FISA and other federal statutes."

The Protect American Act greatly expanded government intelligence gathering capabilities. Obama's pledge that he would follow these laws if elected President seem to indicate his support for the law. The 2007 Act passed the House 227-183, with 186 Republicans and 41 Democrats in favor. In the Senate, where the Act passed 60-28, 42 Republicans and 17 Democrats were in favor. The law's purpose is to "amend the Foreign Intelligence Surveillance Act of 1978 to provide additional procedures for authorizing certain acquisitions of foreign intelligence information and for other purposes." These amendments were all scheduled to expire 180 days after enactment.

The law greatly expanded government surveillance capabilities allowing the government to monitor foreign targets without a warrant. This can be seen as meeting Balkin's criteria for a parallel track of government that normalizes the use of surveillance in everyday law enforcement. The Act also triggers Balkin's criteria for routing around traditional Bill of Rights guarantees, as it also allows warrantless monitoring of communications where one party is in the United States, as long as a no specific U.S. individual is targeted. A FISA Court order is no longer required to conduct this kind of surveillance, rather the Attorney General or the Director of National Intelligence can provide a one-year authorization. Although the program requires Attorney General oversight, it does not require the DOJ to review how American's calls are intercepted or stored, it only mandates the Attorney General report on targets overseas.

While the warrantless surveillance of foreign and domestic targets poses a threat to American civil liberties, the Act's reliance on private parties to collect and share intelligence information undermines Lasswell's principle of civilian supremacy, while it also triggers Balkin's criteria of reliance on private parties. The Act allows the government to issue orders for communication providers to provide assistance to government intelligence gathering, and the ability to seek a FISA Court order to compel provider compliance. The Act formalized immunity from civil litigation for providers who cooperated with the government during the investigation.

Campaign Platform and Issues

During the 2008 election campaign, then Senator Barack Obama's spokesman Bill Burton issued a statement about the potential filibuster of legislation that would offer immunity to telephone companies:

> Senator Obama has serious concerns about many provisions in this bill, especially the provision on giving retroactive immunity to the telephone companies. He is hopeful that this bill can be improved by the Senate Judiciary Committee. But if the bill comes to the Senate floor in its current form, he would support a filibuster of it (Sargent, 2007).

The next day, Burton added, "To be clear: Barack will support a filibuster of any bill that includes retroactive immunity for telecommunications companies" (Sargent 2, 2007).

Obama's campaign website outlined his commitment to balancing national security and civil liberties. Two campaign promises, in particular, outlined his intended strategies to balance security and liberty: *Improve Intelligence Capacity and Protect Civil Liberties:* Improve Information Sharing and Analysis: Barack Obama will improve our intelligence system by creating a senior position to coordinate domestic intelligence gathering; establishing a grant program to support thousands more state and local level intelligence analysts and increasing our capacity to share intelligence across all levels of government. *Give Real Authority to the Privacy and Civil Liberties Board:*
Created by Congress and recommended by the 9/11 Commission, the Privacy and Civil Liberties Board needs to be substantially reformed and empowered to safeguard against an erosion in American civil liberties. As president, Barack Obama will support efforts to strengthen the Board with subpoena

powers and reporting responsibilities, will give the Board a robust mandate designed to protect American civil liberties and will demand transparency from the Board to ensure accountability.

The FISA Amendments Act of 2008

The FISA Amendments Act of 2008 was enacted on July 10, 2008, repealing the *Protect American Act*, except for existing orders, authorizations and directives that were set to sunset (Section 403). The FISA Amendments Act is set to expire on December 31, 2012. Senator Obama voted for the FISA Amendments Act of 2008, granting immunity to telecommunications companies from lawsuits for cooperation (past, present or future) with law enforcement or intelligence officials investigating the plans of terrorists. Immunity would be granted through a certification process, subject to judicial review. The Act passed the House (293 to 129) and the Senate (69 to 28), after a Senate filibuster by Senators Russ Feingold and Chris Dodd who said granting immunity would undermine the rule of law. Most notably, the FISA Amendments Act of 2008 reinstates FISA as the exclusive law governing domestic electronic surveillance, specifically preventing the use of actions such as the Authorization for the Use of Military Force to circumvent FISA (Section 102). This can be seen as a rejection of Balkin's parallel track of government indicative of a national security state. The Act prohibits the intentional targeting of American citizens on American soil, consistent with the Constitution, restoring many civil liberties eroded by previous PATRIOT provisions. Furthermore, the Act required the Attorney General to adopt guidelines for monitoring this type of surveillance. When targeting U.S. persons outside the United States, it limits the court order to a period no longer than 90 days, and requires FISA Court determination of probable cause (Section 703 and 704). The Attorney General is also required to submit semiannual reports to congressional intelligence committees reviewing compliance, the number of applications made, granted, modified, denied, as well as emergency acquisitions of intelligence authorized by the Attorney General (Section 707). These last three statutory updates provide the checks and balances, as well as the disclosure that is necessary for civilian supremacy in government.

The FISA Amendments grant immunity to electronic communication service providers who participated in President Bush's Terrorist Surveillance Program, as long as the district court in the pending cases certify the Attorney General's recommendation for liability protection based on "substantial evidence,"(Section 202). To qualify for immunity, the companies must have cooperated with the government during the Terrorist Surveillance Program between September 1, 2001 and January 17, 2007. They must also have received a written request from the Attorney General of the head of an intelligence organization. The request must indicate the program was lawful and authorized by the president. Again, this immunity is subject to court approval, as is the immunity for individuals who helped the government in response to a court order. Although the immunity process is formalized in this Act, government reliance on private parties for what essentially amounts to intelligence gathering heralds a move toward the National Security State.

The FISA Amendments Act of 2008 (Sec. 801 (1) defines "assistance" as the provision of access—to facilities or otherwise—to information including communication contents, communications records, or other information relating to a customer or communication. The Act also defines electronic communication service provider as a telecommunication carrier engaged as a common carrier for hire, in interstate or foreign communication by wire or radio or interstate or foreign radio transmission of energy (Communications Act of 1934 Section 3; Section 801(6)). The Act expanded the definition to include providers of electronic communication service, providers of remote computer service, communication service providers with access to wire or electronic communications (including stored communications), parent companies, subsidiaries, affiliates, successors, assignees, officers, employees and agents of service providers.

The Obama campaign issued a statement in June 2008 to explain Senator Obama's reversal in voting for the FISA Amendments Act of 2008 (Huffington Post, 2008). Obama identified the dilemma early on in the statement saying "national security agencies must have the capability to gather intelligence and track down terrorists before they strike, while respecting the rule of law and the privacy and civil liberties of the American people." He accused the Bush Administration—with the cooperation of major telecommunications companies—of abusing authority and undermining the constitution by intercepting American citizens' communications without knowledge or warrants. Obama went on to explain he was voting for the "compromise legislation" because it would end President Bush's illegal warrantless surveillance program, restore FISA, re-establish judicial oversight and protect civil liberties. For Obama, the tradeoff was the Act's provision to grant retroactive immunity to the telecommunications companies involved in wiretapping under the Terrorist Surveillance Program. He rationalized this by saying the bill was "far better than the Protect America Act," and that providing "effective intelligence collection tools with appropriate safeguards is too important to delay."

As James Risen reported in the New York Times, the endorsement was immediately met with criticism from Obama supporters (Risen, 2008). Over 7,000 supporters called for him to reverse his decision to support immunity for telecommunications companies involved in the TSP. In the article, Risen interviewed Obama campaign advisor and Washington lawyer Greg Craig, who is quoted as saying that the compromise legislation was "the best deal possible," given the looming expiration date of certain surveillance provisions allowed by the law.

In early July 2008, the Obama campaign issued a statement on the FISA bills through its website (Rospars, 2008).

> "I want to take this opportunity to speak directly to those of you who oppose my decision to support the FISA compromise. This was not an easy call for me. I know that the FISA bill that passed the House is far from perfect. I wouldn't have drafted the legislation like this, and it does not resolve all of the concerns that we have about President Bush's abuse of executive power. It grants retroactive immunity to telecommunications companies that may have violated the law by cooperating with the Bush Administration's program of warrantless wiretapping. This potentially weakens the deterrent effect of the law and removes an important tool for the American people to demand accountability for past abuses."

Obama went on to say that he was working with Senate leaders to strike the immunity provisions from the bill, but that the compromise firmly reassured the FISA court's role as a monitor of the "watchers". Obama said, "In a dangerous world, government must have the authority to collect the intelligence we need to protect the American people. But in a free society, that authority cannot be unlimited." Obama, in explaining his decision to vote for what he called an "improved yet imperfect bill" said he did not want to lose "important surveillance tools." He also pledged, once he was sworn in as president, to have his "Attorney General conduct a comprehensive review of all our surveillance programs and to make further recommendations on any steps needed to preserve civil liberties and to prevent executive branch abuse in the future." Although Obama's promise for future review provided a necessary check on government and honored the need for civilian supremacy, his acceptance of government reliance on private parties in intelligence gathering triggers Balkin's National Security State danger.

Obama as President
State Secrets

In April of 2009, the Obama Administration filed a motion to dismiss in the case of *Jewel v. NSA*, upholding the former Bush administration's policy that courts could not evaluate the legality of the Terrorist Surveillance Program. In *Jewel*, a Bush-era class action lawsuit filed by the Electronic Frontier Foundation, the plaintiffs asked the court to "stop the illegal, unconstitutional, and ongoing dragnet surveillance of their communications and communications records." The Justice Department, in its motion to dismiss, said that disclosing information about the surveillance program would disclose "state secrets," parroting the language used by the Bush administration in response to lawsuits filed in 2006 against the program. Claiming state secrets privilege, the motion suggested the classified documents pertaining to the program were available for *in camera* review. The EFF response from Senior Staff Attorney Kevin Bankston said, "President Obama promised the American people a new era of transparency, accountability, and respect for civil liberties, but with the Obama Justice Department continuing the Bush administration's cover-up of the National Security Agency's dragnet surveillance of millions of Americans, and insisting that the much-publicized warrantless wiretapping program is still a 'secret' that cannot be reviewed by the courts, it feels like deja vu all over again." The use of "state secret" privilege as a reason to quash the lawsuit could be seen as the kind of act Balkin identified as an authoritarian state trying to hide information from the public. Whether the "secret" claim is meant to hide embarrassing information or protect existing policy failures, the government's claim that the continuance of the trial and the introduction of evidence about the spying program would jeopardize national security works against Lasswell's principle of open disclosure of government activity.

Overcollection

> Later the same month, the *New York Times* revealed that the National Security Agency had recently intercepted American citizens' e-mails and phone calls in violation of the terms outlined in the 2008 FISA Amendments Act (Lichtblau and Risen, 2009). Quoting "several anonymous intelligence officials," and lawyers, the article claimed that the NSA "engaged in 'overcollection' of domestic communications of Americans. The Congressional Intelligence Committees were notified of the problem—believed to involve the NSA's occasional inability to "distinguish between communications inside the United States and those overseas as it uses its access to American telecommunications companies' fiber-optic lines and its own spy satellites to intercept millions of calls and e-mail messages." The article cited an official who says this caused the NSA to "target" groups of American without warrant.

The surveillance was described as "significant and systematic," but "unintentional." The *New York Times* made inquiries to the Justice Department, who acknowledged "resolved" problems with NSA surveillance that were identified during a periodic review of agency activities—most likely the twice annual certification that the DOJ and DNI make to the FISA Court. The Justice Department also told the *New York Times* that Attorney General Eric H. Holder Jr. renewed the updated surveillance program with the National Security Court. The *Times* article quoted intelligence officials who said the "problems had grown out of changes enacted by Congress last July… enacting a new framework for collecting intelligence on terrorism and spying suspects." The article also mentions other NSA surveillance problems such as the agency's "attempt" to warrantlessly wiretap a member of Congress who was traveling oversees.

In late September 2009, Deputy Assistant Attorney General Todd Hinnen told the House Judiciary Committee that the Administration was "ready and willing" to work with Congress on specific proposals that would allow for "effective investigative authorities," while protecting privacy and civil

liberties," (Margasak, 2009). The Committee Chairman John Conyers (D-Mich) told Hinnen that he sounded like "a lot of people who came over from the DOJ before," referring to the Bush Administration. One provision required businesses to produce "any tangible things" at the FBI's request—although law enforcement must still seek the approval of the FISA Court. During the hearing, committee members referenced a Department of Justice Report, prepared by the Office of the Inspector General that showed the FBI had on three occasions, when the Court refused to grant authorization, used National Security Letters to acquire information from private businesses. Hinnen assured the committee that these policies had been corrected under the Obama Administration, but they still show a move towards a parallel track of government operating outside of the bounds of civilian authority.

Growth of the Security Elite

Nothing seems to indicate a parallel track of intelligence gathering more than the 2010 FBI budget, which included $9 million dollars for what was called the "Going Dark Program." The program was described as supporting the FBI's electronic surveillance, intelligence collection and evidence gathering capabilities. This raised the program's total budget for 2010 to $233.9 million dollars, including 133 positions. The budget also called for $23.5 million to "enhance and support the surveillance capabilities of the Special Operations Group, the Special Surveillance Group and the Aviation Program. This raised the current program funding to $161 million, with 1,108 positions (FBI Budget FY 2010).
In the January 21, 2010 Memorandum on Transparency and Open Government, President Barack Obama pledged to create "an unprecedented level of openness in Government." A reversal of the memo by former Attorney General John Ashcroft, Obama called for federal agencies to operate under a "presumption in favor of disclosure." Since each Administration's FOIA memo is seen as a working policy distributed to all agencies, this indicates a move away from Lassewell's garrison state since the President was openly promoting disclosure of information in government departments.

Also in January, the Justice Department's Office of the Inspector General released an Internal Audit criticizing the FBI for using exigent letters and other informal requests to get the phone companies to turn over telephone toll billing records, in violation of the Electronic Communications Privacy Act (Singel, 2010). The report said that the FBI gave phone carriers multimillion dollar contracts to keep phone records longer and prioritize responses to FBI inquiries. The report also said that the companies set up remote terminals inside FBI offices. The report said this practice had been going on for the last four years, however the greater revelation was that the Obama Administration issued a secret rule in early January saying that the practice was legal.

The report said that the FBI allowed remote terminals inside Agency offices, staffed with telecommunication provider employees (from MCI, AT&T and Sprint) responding to National Security Letters. The audit suggested that AT&T employees began using exigent letters in a "casual, routine and unsupervised" manner. In fact, one revealed that they would give agents "sneak peaks" of information before agents decided if it was worthwhile to apply for official authorization. The audit estimated that there were more than 3,500 off the book requests between 2003 and 2007, when the FBI removed the telecom employees from the offices. The FBI denies that its employees obtained phone records in an illegal manner.

The Obama administration retroactively legalized the FBI-telecomm arrangement in January of 2010, solidifying and legally protecting the government's reliance on private parties in intelligence gathering. The Oversight and Review Division of the Office of the Inspector General released a report detailing the FBI's use of informal requests for telephone records (Ackerman, 2010). In response, Senators Russell Feingold, Richard Durbin and Ron Wyden wrote a letter to Attorney General Eric Holder expressing great concern over the report's revelation of "rampantly" illegal methods employed by the

FBI in obtaining phone records. The letter officially requested a copy of the "January 28, 2010 Office of Legal Counsel opinion referenced in the report," as it was believed to establish the legal authority that the FBI claimed to obtain the "phone records on a voluntary basis from providers, without legal process or qualifying emergency."

Executive Support for Congressional Actions

On February 27, 2010, President Obama signed H.R. 3961, a one-year extension to certain provisions in the USA PATRIOT Act and the Intelligence Reform and Prevention Act of 2004. The extended provisions included 1) authorizing court-approved roving wiretaps on multiple phone lines; 2) allowing court-approved seizure of records and property in anti-terrorism operations; and 3) permitting surveillance of non-U.S. lone wolf terrorists. The extensions were passed as part of the Medicare Physician Payment Reform Act.

In July of 2010, the *Washington Post* reported that the Obama Administration was trying to "make it easier" for the FBI to get individual's Internet activity records from telecommunication companies when the records are relevant to intelligence investigations (Nakashima, 2010). The *Post* reported that the Administration wanted to include "electronic communication transactional records" in the list of records that the FBI could request without the approval of the FISA Court. Electronic communication transaction records would include e-mail addresses of correspondents, and possible the browsing history, but not e-mail content. These provisions post a threat to civil liberties—in particular First Amendment rights to freedom of speech and association. The FBI would use National Security Letters to compel carriers to turn over the records, and as one former Homeland Security official added, it would make it "faster and easier" for the FBI to get the data. The article quoted a "senior administration government official" who said "most" providers already turn over such data. The Administration has asked Congress to amend the statute, the Electronic Communications Privacy Act, in the fiscal year that begins in October.

In the fall of 2010, the *New York Times* reported that The Obama Administration wanted to make it easier for companies to comply with FBI wiretap orders to intercept and "unscramble" encrypted messages (Savage, 2010). The *Times* reported that the Obama administration had plans to submit a bill to Congress in 2011. The article quoted Center for Democracy and Technology Vice President James X. Dempsey as saying the proposal would challenge the decentralized design of the Internet, "They basically want to turn back the clock and make Internet services function the way that the telephone system used to function." The Communications Assistance to Law Enforcement Act mandated that phone and broadband networks have intercept-ready switches at carrier offices, but when targets use encrypted messages, the FBI must seek service provider assistance in unscrambling the messages. The communication service providers are not subject to CALEA, although some already have intercept capabilities. In the *Times* article, several of the proposal's anticipated requirements are identified: Communications services that encrypt messages must have a way to unscramble them.

Foreign-based providers that do business inside the United States must install a domestic office capable of performing intercepts. Developers of software that enables peer-to-peer communication must redesign their service to allow interception. To date, there has been no legislation introduced that relates to these anticipated revisions.

On February 24, 2011, President Obama signed the FISA Sunsets Extension Act (H.R. 514) extending three provisions of the USA PATRIOT Act and the Intelligence Reform and Terrorism Prevention Act of 2004, including: 1) authorization for court approved roving wiretaps on multiple phone lines; 2) authorization for court-approved seizure of records and property in anti-terrorism operations; and 3)

authorization for lone-wolf surveillance of non-U.S. citizens (Pub. L. 112-3, became law on Feb. 25, 2011). This provides the U.S. government the ability to access business records, conduct roving wiretaps and monitor terrorism suspects until May 27, 2011. The extensions were originally scheduled to expire on February 28, 2011.

As the United States Congress returns to session in May 2011, it will need to revisit the 90-day extension it granted in February for expiring PATRIOT Act provisions, extending expiration to May 27. Given the bipartisan support for the February passage of the extensions, it could be a speedy process. Senate Majority Leader Harry Reid, after the passage of the 90-day extension, pledged to devote a week of Senate time to the PATRIOT Act legislation. The House Judiciary Committee held two hearings on the Patriot Act in March 2011. There are, as of yet, no committee reports on the legislation. The Senate's Judiciary Committee considered the PATRIOT Act bill (S.), sponsored by Patrick Leahy, voting 11-7 in favor of the bill. The bill would extend the three provisions until December of 2013, but it would also sunset the authorization for the FBI's use of national security letters on that date. Leahy has been a vocal critic of past PATRIOT legislation, saying the administration's proposals raise "serious privacy and civil liberties concerns," (Leahy Statement on Thursday, before August 2, 2010). In the same statement, Leahy said, "While the government should have the tools that it needs to keep us safe, American citizens should also have protections against improper intrusions into their private electronic communications and online transactions."

Latest Actions

At the end of April 2011, the attorney representing whistleblower Thomas Tamm, the former Justice Department official who claimed credit for leaking information about the Terrorist Surveillance Program to the *New York Times* for their groundbreaking 2005 article would not be prosecuted for leaking secret information (Savage). Tamm discovered the illegal NSA wiretapping program while he held Top Secret/SCI clearance at the DOJ Office of Intelligence Policy and Review (Poulsen). Attorney General Eric Holder did not confirm or deny the report, but if it is true, the move can be seen as in line with the Lasswellian principals of civilian supremacy and disclosure.
Finally, the move towards a security state can be seen in the rise of a "security elite" that manage war and security through intelligence and military officers without the consent of state sovereigns. On April 27, 2011, Obama announced he was nominating General David Patraeus as the head of the historically civilian-led Central Intelligence Agency (Greenwald). Patraeus, a military officer like his predecessor Michael Hayden, has a limited background in intelligence, but is better known for serving as commander in two post 9/11 wars. This appointment has been criticized by some in Washington as a move towards militarizing the CIA. Senate Intelligence Committee Chairwoman Dianne Feinstein said, "You can't have the military control most of the major aspects of intelligence," (Greenwald). Another member of the Senate Intelligence Committee, Jane Harman, said she has heard concerns that the military is taking over intelligence operations. Echoing her concern, House Intelligence Committee Chairman Pete Hoekstra, said, "We should not have a military person leading a civilian agency at this time." Incidentally, the first four Directors of the CIA were military officers (1947-1953).

Another example of the militarization of intelligence through the use of a security elite is The Department of Homeland Security, a cabinet department created in response to the September 11th attacks. The DHS was established on November 25, 2002 by the Homeland Security Act. The mission of the office was to "develop and coordinate the implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks." The office coordinates the "implementation of a comprehensive national strategy to secure the United States from terrorist threats or attacks," through the coordination of executive branch efforts to "detect, prepare for, prevent, protect against, respond to, and recover from terrorist attacks within the United States," (National Security

Strategy, 2007). Twenty-two agencies were absorbed into the department, which in 2012 has funding of $57 billion and over 200,000 employees. The DHS is an integrated agency with more than 87,000 jurisdictions at the federal, state and local level. The DHS celebrated its 8th anniversary under the Obama Administration in March of 2011, with Obama appointee Secretary Janet Napolitano at the head.

In a May 2011 interview with San Francisco Gate Editorial Board, Department of Homeland Security Secretary Janet Napolitano, when asked about restoring the balance between liberty and security, said, "I would suggest that there is a change that is perhaps imperceptible to the public eye, but is there nonetheless," (Diaz). As an example, she cited the new chief privacy officer in the DHS, as well as "an entire group" of employees that review civil liberties.

Conclusion

This paper sought out to provide a review of Barack Obama's surveillance policies through the lens of a national security state developed through the theories of Lasswell, Nagan, Hammer and Balkin. Although this analysis is unconventional, it was designed to provide new perspective on United States surveillance policies. In reviewing Obama's actions from 2004-present, there is a clear shift in the policies of "Obama the Candidate" versus "Obama the President." This is hardly surprising. As foreshadowed by Lasswell's communist-era warnings about a Garrison state, the United States intelligence gathering community has grown exponentially in the latter half of the 20th and beginning of the 21st century. Spurred by terrorist attacks and general fear of threats from abroad, Americans have been willing to sacrifice civil liberties in exchange for security. This has created a national culture of crisis where we are always at risk and always at war. While it is easy for presidential candidates or members of Congress to fight against expanding surveillance capabilities, the president is tasked with protecting the country. During the continuing War on Terror, this responsibility includes maintaining and expanding the security state created by one's predecessors.

Lasswell's solution to balancing national security and individual freedom called for the government to endure the national defense crisis by limiting the loss of fundamental freedoms. The central nervous system of intelligence gathering introduced by Nagan and Hammer relied upon a security elite operating outside of the bounds of constitutionally-bound state sovereignty. Balkin's theory of a ubiquitous National Security State formalized these theories by offering the model of a parallel track of government that relied on private parties to collect intelligence outside of traditional state-sponsored law enforcement intelligence gathering. The state of surveillance in the United States in 2011 aligns with these theories but it is also a continuation of 20th century intelligence practices. For example, the cooperation between the government and telecommunication companies and law enforcement's reliance on these private parties to provide communications information is nothing new. In the 1920's government agents operating in the "Black Chamber" visited major telecommunication companies and asked for copies of transmitted telegraphs. The National Security Agency, established in 1952, has long operated outside of the realm of traditional checks and balances for government oversight—the National Security Act of 1959 protected the agency from forced disclosure of classified or unclassified information on organizational structures or policies. Although the 1970's era FISA law created stricter constitutional protections for intelligence gathering, the decades of lawmaking and revisions to FISA since that time have returned the country to the early days of intelligence gathering where agents can operate outside of the law as long as they are acting in the interest of protecting national security. The bigger picture reveals an America where the balance between civil liberties and national security are continually eroded by external foreign threats to the well being of the nation. The Bill of Rights and the Constitution are intact, but the protections they provide are often willingly set aside in the name of national defense. Although this is a common practice during wartime, the War on Terror formalizes

this threat into an indefinite period of national crisis. Although Lasswell saw this crisis of insecurity as a period that might last a decade, modern citizens know that the insecurity might now be a permanent justification for the erosion of liberty… the "new normal."

References

Address Before a Joint Session of the Congress on the United States Response to the Terrorist Attacks of September 11, 2 Pub. Papers 1140 (Sept. 20, 2001).
American Civil Liberties Union. "Establishing a New Normal, National Security, Civil Liberties and Human Rights Under the Obama Administration, An 18-Month Review." Accessed March 1, 2011. http://www.aclu.org/files/assets/EstablishingNewNormal.pdf.
Ackerman, S. 2010. "Retroactive Immunity for Illegal Surveillance (Obama Edition)." *The Washington Independent*, January 22. Accessed March 15, 2010. http://washingtonindependent.com/74588/retroactive-immunity-for-illegal-surveillance-obama-edition.
Balkin, J.M., "The Constitution in the National Surveillance State." *Minnesota Law Review*, Vol. 93, No. 1, 2008; *Yale Law School, Public Law Working Paper* No. 168. Accessed March 15, 2010. http://ssrn.com/abstract=1141524.
Department of Homeland Security. "8th Anniversary Celebration." Accessed March 15, 2010. http://www.dhs.gov/xabout/history/8th-anniversary-celebration.shtm.
Department of Homeland Security. "National Strategy For Homeland Security" (PDF). *pdf file*. Retrieved October 31, 2007.
Diaz, J. 2011. "Threats to civil liberties continuing under Obama." *San Francisco Chronicle*, May 1, 2011, F-2. Accessed May 1, 2011. http://sfgate.com/cgi-bin/article.cgi?f=/c/a/2011/05/01/INBL1J7NKF.DTL
Electronic Frontier Foundation. 2009. "Obama Administration Embraces Bush Position on Warrantless Wiretapping and Secrecy." *Electronic Frontier Foundation Press Release*, April 6, 2009. Accessed March 15, 2010. http://www.eff.org/press/archives/2009/04/05
Federal Wiretapping Statute, ch. 197, 40 Stat.1017-18 (1918).
Gallup Poll, Liberty vs. Security: Public Mixed on Patriot Act, July 19, 2005.
Government Defendants' Notice of Motion to Dismiss and For Summary Judgment and Memorandum *Jewel et al. v. National Security Agency et al.*, Case No. 08-cv-4373-VRW
Greenwald, G. "A more militarized CIA for a more militarized America." Salon.com. April 28, 2011.
Homeland Security Act of 2002
The Permanent Provisions of the PATRIOT Act., xxxth Cong. Xx-xx (2011) (subcommittee on Crime, Terrorism and Homeland Security) March 30, 2011.
The Reauthorization of the PATRIOT Act., xxth Cong. Xx-xx (2011) (subcommittee on Crime, Terrorism and Homeland Security) March 9, 2011.
Huffington Post. 2008. "Obama Backs Bill Giving Immunity To Telecoms." *The Huffington Post*, June 20. Accessed March 15, 2010. http://www.huffingtonpost.com/2008/06/20/obama-backs-bill-giving-i_n_108370.html
Interview by Eric Schmidt with Senator Barack Obama at Google (Nov. 14, 2007), http://www.youtube.com/ watch?v=m4yVlPqeZwo.
Lasswell, H. 1950. *National Security and Individual Freedom.* McGraw Hill: New York.
Lasswell, H. 1964. "The Structure and Function of Communication in Society." *The Communication of Ideas.* 37 (ed. Lyman Bryson, 1964).
Lichtblau, E. and Risen, J. 2009. "Officials Say U.S. Wiretaps Exceeded Law." *The New York Times*, April 15. Accessed March 15, 2010.
Margasak, L. 2009. "Obama: Patriot Act Surveillance Law Should Stay." *Huffington Post*, September 22. Accessed March 15, 2010. http://www.huffingtonpost.com/2009/09/22/obama-patriot-act-surveil_n_295194.html
Nagan, W.P. and Hammer, C. "Communications Theory and World Public Order: The Anthropomorphic Jurisprudential Foundations of International Human Rights." Unpublished paper attained from author.

Nakashima, E. 2010. “White House proposal would ease FBI access to records of Internet activity.” *The Washington Post*, July 29. A01. Accessed October 1, 2010.
Napolitano, J. “Marking the 8th Anniversary of the Department of Homeland Security.” *The White House Blog*. Accessed on March 1, 2011.
http://www.whitehouse.gov/blog/2011/02/28/marking-8th-anniversary-department-homeland-security
WPRESS RELEASE, "RENEWAL OF AMERICAN LEADERSHIP " JUL 12, 2004
Obama, B. Senate Floor Statement of Barack Obama. Accessed March 15, 2011.
http://obamaspeeches.com/053-Floor-Statement-S2271-PATRIOT-Act-Reauthorization-Obama-Speech.htm
Obama, B. Senate Floor Statement of Senate Barack Obama. Accessed March 15, 2011.
http://obamaspeeches.com/041-The-PATRIOT-Act-Obama-Speech.htmSource: obama.senate.gov/speech/051215-senate_floor_st/ Date: 12/15/2005
Poulsen, K. 2011. “Feds Drop Probe of NSA Wiretapping Whistle Blower.” Wired, April 26. Accessed May 1, 2011. http://www.wired.com/threatlevel/2011/04/tamm/
Risen, J. 2008. “Obama Voters Protest His Switch on Telecom Immunity.” *The New York Times*, July 2. Accessed March 15, 2010.
http://www.nytimes.com/2008/07/02/us/politics/02fisa.html?ref=foreignintelligencesurveillanceactfisa&pagewanted=all
Rospars, J. 2008. “Response from Barack on FISA and Discussion with Policy Staff.” *MyBarackObama.com*, July 3. Accessed March 15, 2010.
http://my.barackobama.com/page/community/post/rospars/gGxsZF
Sargent, G. 2007. “Obama: I Would Support Dodd's Filibuster.” *Talking Points Memo*, October 23. Accessed March 15, 2010.
http://tpmelectioncentral.talkingpointsmemo.com/2007/10/obama_i_would_support_dodds_filibuster.php
Sargent, G. 2007. “Obama Camp Says It: He’ll Support Filibuster of Any Bill Containing Telecom Immunity.” *Talking Points Memo*, October 24. Accessed March 15, 2010.
http://tpmelectioncentral.talkingpointsmemo.com/2007/10/obama_camp_says_it_hell_support_filibuster_of_any_bill_containing_telecom_immunity.php.
Savage, C. 2010. “U.S. Tries to Make It Easier to Wiretap the Internet.” *The New York Times*, September 2. Accessed October 1, 2010.
http://www.nytimes.com/2010/09/27/us/27wiretap.html?_r=2&pagewanted=1&hp
Singel, R. 2010. “FBI, Telecoms Teamed to Breach Wiretap Laws.” *The Washington Independent*, January 21. Accessed
Sonmez, F. 2011. “Patriot Act debate will ramp up again next month.” The Washington Post, April 19. Accessed May 1, 2011.
http://www.washingtonpost.com/blogs/2chambers/post/patriot-act-debate-will-ramp-up-again-next-month/2011/04/19/AF1sys6D_blog.html
Yardley, H.O. *The American Black Chamber.* Indianapolis, IN: Bobbs-Merrill, 1931.