INDEX

INDEX, cont.

Definition- Surveillance

Surveillance is the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

Reviewing the vast surveillance studies literature, Professor David Lyon concludes that surveillance is primarily about power, but it is also about personhood. n8 Lyon offers a definition of surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction." n9 Four aspects of this definition are noteworthy, as they expand our understanding of what surveillance is and what its purposes are. First, it is focused on learning information about individuals. Second, surveillance is systematic; it is intentional rather than random or arbitrary. Third, surveillance is routine - a part of the ordinary administrative apparatus that characterizes modern societies. n10 Fourth, surveillance can have a wide variety of purposes - rarely totalitarian domination, but more typically subtler forms of influence or control. n11

Pro- Organized Crime

Criminal drug networks rely on telecommunications for organization, coordination, communication, and economic efficiency.

Christopher A. Nolin, JD Catholic University America; Fall 2006 (CommLaw Conspectus; 15 CommLaw Conspectus 231; "Telecommunications as a weapon in the war or modern organized crime")

Managing an international empire of narcotics manufacturing and distribution is a monumental task for the drug kingpin or cartel manager. Like the Italian crime bosses that came before him, the drug kingpin is responsible for making strategic decisions and issuing direction to his virtual army of agents. The most significant difference from his Mafia predecessors is that the kingpin always directs operations from foreign soil. n30 Numerous transactions are carried out simultaneously and the kingpin must have seamless communications with his cells. n31 Effective coordination of the enterprise requires accurate transmission of information to international cells regarding warehousing locations for loads of narcotics, contacts for providing transportation once the narcotics arrive at a destination, and locations for delivering the profits. n32
The benefits of a widespread infrastructure for cells to effectively communicate information with each other is compounded by the United States' combative approach in recent decades towards South American drug trafficking. President Richard Nixon first launched the "War on Drugs" n33 in [*238] 1971, targeting the spread of narcotics on a domestic level, while aiming to reduce the influx and supply of narcotics from drug-producing countries. n34 President George H.W. Bush advanced this policy by invading Panama with American troops to capture kingpin and Army General Manuel Noriega, who surrendered to the DEA in January of 1990. n35 Never considered victorious, n36 the War on Drugs continues. n37 Despite American efforts [*239] to stem the domestic manufacture and distribution of narcotics, the Colombian drug cartels will persist so long as their nation's economy heavily relies on its drug trafficking industry, which will continue as long as cartels are permitted to pursue all avenues to perpetuate this lucrative business. n38
B. Use of Advanced Communications in Evading Scrutiny by American Law Enforcement
The economic efficiency of drug trafficking organizations stems largely from the historical success that Colombian kingpins have had in identifying and implementing advanced technologies for effective communication within the cartel. n39 The attention and scrutiny that leaders of the War on Drugs have invested in crippling the efforts of drug trafficking organizations in recent decades have forced the cartels and other drug smuggling organizations to rely heavily on telecommunications to coordinate their illicit operations in order to avoid law enforcement detection and prosecution. n40 For example, from the 1980s to early 1990s, Colombian cartels used pagers, creating codeword systems to convey times and locations for transactions. n41 Pay phones provided a virtually untraceable medium when live voice communication was required. n42 In the mid- to late-1990s, phone arcades, pre-paid phone cards, and faxes became popular methods of message transmission. n43 As the technology emerged, drug lords gradually incorporated [*240] cellular phones into their operations; they bought the phones in lots and discarded them periodically to insulate themselves from surveillance. n44

Pro- Organized Crime

Electronic surveillance is the most important and sophisticated tool in the fight against criminal drug cartels. It is often the only method available and leads to prevention, investigation, and prosecution. Christopher A. Nolin, JD Catholic University America; Fall 2006 (CommLaw Conspectus; 15 CommLaw Conspectus 231; "Telecommunications as a weapon in the war or modern organized crime")

Globally, the drug trade ranks among the most serious outgrowths of organized crime. n45 In addition to those it directly affects, drug trafficking indirectly inflicts harm on society through violent acts such as kidnappings, public turf battles, and robberies committed by drug dealers. n46 Drug trafficking generates exorbitant health care expenses and devastating effects on productivity, industry, and public safety, particularly with regard to inner-city children and the unborn children of addicted mothers. n47 Given the nation's efforts in combating the War on Drugs, however, United States law enforcement remains optimistic that progressive, efficient electronic surveillance of major narcotics organizations and cartels will lead to a decline in the debilitating effects of drug trafficking and organized crime. n48 United States law enforcement agencies generally agree that electronic surveillance may be the most important and sophisticated investigative device available in the prevention, investigation, and prosecution of organized crime. n49 In the world of drug trafficking, electronic surveillance is often the only method available to intercept communications between the drug kingpin and his highest officers within the crime enterprise. n50

Pro- Organized Crime- AT: NSA Only Terrorism/Not law enforcement

Your argument is based on a misreading of FISA that creates a false dichotomy between foreign intelligence and law enforcement.

David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

The second question is definitional: what is "foreign intelligence [*495] information?" Since 1978, FISA has defined that term to include "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against" attack, sabotage, international terrorism, or espionage committed by a foreign power or an agent of a foreign power. n57 As this language makes clear, "foreign intelligence information" must be relevant or necessary to "protect" against foreign threats to national security. But FISA does not prescribe how the information may or must be used to achieve that protection. In other words, FISA does not discriminate between protection through intelligence, diplomatic, economic, military, or law enforcement efforts, other than to require that those efforts be "lawful." n58

The legislative history of FISA confirms the statute's plain language. The House Report on the 1978 version of FISA provides:

How this [foreign intelligence] information may be used to "protect' against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information ... . Obviously, use of "foreign intelligence information' as evidence in a criminal trial is one way the government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. n59

The Senate Intelligence Committee's report on the 1978 version of FISA contains similar language:

Electronic surveillance for foreign counterintelligence and counterterrorism [*496] purposes ... is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnapping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area. n60 Nonetheless, beginning in the 1980s, the federal courts generally either implicitly assumed or actually concluded that "foreign intelligence information" excludes information relevant or necessary to protect national security using law enforcement methods. n61 Under this approach, information needed to recruit an international terrorist as a double agent was foreign intelligence information because recruitment is a method of protecting against terrorism that does not involve law enforcement. However, information needed to indict and prosecute an international terrorist was not foreign intelligence information. Although prosecution clearly can protect against terrorism - by deterring, incapacitating, or encouraging cooperation from terrorists in exchange for leniency - prosecution is a law enforcement method. By drawing this distinction, courts created a dichotomy between law enforcement methods and all other methods (including intelligence methods) of protecting national security. n62

[*497] In keeping with these judicial interpretations of FISA, prosecution of an international terrorist could be a secondary purpose of FISA surveillance, but not the primary purpose. If prosecution became - or was perceived to have become - the primary purpose of FISA surveillance, then the surveillance would have to stop, and any evidence thereafter obtained or derived from FISA would be suppressed. n63

Pro- Organized Crime- AT: NSA Only Terrorism/Not law enforcement

Narcoterror is a real threat. Drug crime and terror go hand-in-hand.
Walser, Senior Policy Analyst @ Heritage Foundation; 2009 (Ray; "U.S. drug policy in Latin America"; Testimony before the Committee on the Foreign Affairs, Subcommittee on Western Hemisphere, of the United States House of Representatives; December 7; http://www.heritage.org/research/testimony/us-drug-policy-in-latin-america)

The enrichment drugs provide for criminal organizations is enormous. Given the availability of vast quantities of cash, organizations possess the capacity to finance corruption, illicit activities, and hire killers ready to commit the unspeakable. Crime and terror, of the ordinary criminal type and of the international variety, go hand-in-hand. Terrorist organizations claiming political agendas likewise see ample opportunities to exploit the lucrative drug trade for their benefit. The narcoterrorists of the FARC have become the classic standard of a militarized political force that has discovered new life by becoming an active participant in the cocaine business serving as gatekeepers, enforcers, and agents in the cultivation, processing and transshipment of Colombian cocaine. Coupled with extortion and kidnapping, the FARC furthers the climate of lawlessness and fear in which the drug trade flourishes.
Evidence has emerged that Islamist extremist groups such as Hezbollah are also setting up shop and see the Western Hemisphere's drug trade as a profitable means of support. We must remain vigilant regarding the connections especially at a time when non-Hemispheric players are seeking wider roles, stronger ties, and greater political and economic leverage in the Americas.

Pro- Terrorism- Domestic Surveillance

Warrantless domestic surveillance effectively prevented terrorist attacks on the U.S. that would not have been possible under FISA.
Michael Hayden, Retired Air Force 4-star general, and former director of National Intelligence, CIA & NSA; December 19, 2005 (White House Archives; "Press briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence"; http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html)

Q Have you identified armed enemy combatants, through this program, in the United States?
GENERAL HAYDEN: This program has been successful in detecting and preventing attacks inside the United States.
Q General Hayden, I know you're not going to talk about specifics about that, and you say it's been successful. But would it have been as successful -- can you unequivocally say that something has been stopped or there was an imminent attack or you got information through this that you could not have gotten through going to the court?
GENERAL HAYDEN: I can say unequivocally, all right, that we have got information through this program that would not otherwise have been available.
Q Through the court? Because of the speed that you got it?
GENERAL HAYDEN: Yes, because of the speed, because of the procedures, because of the processes and requirements set up in the FISA process, I can say unequivocally that we have used this program in lieu of that and this program has been successful.

Operational intelligence has prevented the majority of the 60 attacks planned against the U.S. since 9/11.
James Jay Carafano, Vice President Defense & Foreign Policy Studies @ Heritage Foundation; August 6, 2013 (Heritage Foundation; "PRISM is essential to U.S. security in war against terrorism"; http://www.heritage.org/research/commentary/2013/8/prism-is-essential-to-us-security-in-war-against-terrorism)

At least 60 Islamist-inspired terrorist plots have been aimed at the U.S. since the 9/11 attacks. The overwhelming majority have been thwarted thanks to timely, operational intelligence about the threats. Congress should not go back to a pre-/11 set of rules just to appeal to populist sentiment.

Pro- Terrorism- Domestic Surveillance

The War on Terror necessitates different standards and limits on surveillance than normal criminal prosecutions.

William Funk, Robert E. Jones Prof Law @ Lewis & Clark; Summer 2011 (Mississippi Law Journal; 80 Miss. L. J. 1491; "Electronic surveillance of terrorism in the United States")

Second, the acceptance of the "war on terror" as more than a mere sobriquet, but as a legal concept in the United States, further supports approval of "war-time" measures. Unlike the "war on drugs" or the "war on crime," the war on terror, or at least the use of force pursuant to the Authorization for the Use of Military Force (AUMF), n49 has been accorded the status of "war" for many legal purposes. n50 Persons apprehended abroad, at least, may be treated as enemy combatants, and those alleged to have violated the laws of war (as today's terrorists routinely do) may be prosecuted by military commission for violation of those laws, rather than prosecuted as simple criminals, although their acts may well constitute federal crimes. Whether persons apprehended in the United States, and especially United States citizens, may also be tried by military commissions as unlawful enemy combatants, as were the saboteurs in *Ex Parte Quirin*, n51 is yet to be determined, although the government apparently maintains that it can. n52 Thus, limits on surveillance that might be appropriate if the purpose were ordinary law enforcement may not be appropriate if the prosecution is to occur in military tribunals under the laws of war. At the same time, despite the claims by the government of the ability to use military tribunals, so far none have been used, and it seems unlikely that they will be used for anyone apprehended in the United States. This accords with the practice in European nations, even those that have suffered serious terrorist acts on their soil, although the "Diplock courts" in Northern Ireland were extensively used in lieu of [*1505] normal jury trials to try IRA activists, and at least in one case against a supporter of Al-Qaeda. n53

Pro- Terrorism- Domestic Surveillance

Given the difficulty of gaining intelligence abroad, more flexibility at home is necessary with regards to surveillance.
William Funk, Robert E. Jones Prof Law @ Lewis & Clark; Summer 2011 (Mississippi Law Journal; 80 Miss. L. J. 1491; "Electronic surveillance of terrorism in the United States")

Third, perhaps FISA's limitation to intelligence regarding *international* terrorism (and foreign powers and their agents) justifies a different basis for engaging in surveillance of citizens. Allowing border searches without any suspicion and intrusive border searches on a reasonable suspicion basis, rather than probable cause, are examples of how cross-border concerns can justify searches that otherwise would not be justified. While FISA is not limited to (or even primarily aimed) at cross-border communications, the interest justifying the search technique is one that necessarily involves foreign actors or governments. Given the reduced capability of the government to obtain information abroad short of surveillance, compared to the capabilities to obtain information through less intrusive techniques in the United States, more flexibility regarding surveillance regarding such information might be justified.

The U.S. government is entitled to data that may contain bits of information about impending acts of terrorism. The goal should not just be punishment after an attack occurs but instead prevention.
Richard Posner, U.S. 7th Circuit Court Appeals & Senior Lecturer Law @ Univ Chicago; December 21, 2005 (Washington Post; "Our domestic intelligence crisis"; http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html)

The goal of national security intelligence is to prevent a terrorist attack, not just punish the attacker after it occurs, and the information that enables the detection of an impending attack may be scattered around the world in tiny bits. A much wider, finer-meshed net must be cast than when investigating a specific crime. Many of the relevant bits may be in the e-mails, phone conversations or banking records of U.S. citizens, some innocent, some not so innocent. The government is entitled to those data, but just for the limited purpose of protecting national security.
The Pentagon's rush to fill gaps in domestic intelligence reflects the disarray in this vital yet neglected area of national security. The principal domestic intelligence agency is the FBI, but it is primarily a criminal investigation agency that has been struggling, so far with limited success, to transform itself. It is having trouble keeping its eye on the ball; an FBI official is quoted as having told the Senate that environmental and animal rights militants pose the biggest terrorist threats in the United States. If only that were so.

Pro- Terrorism- FISA Amendments

FISA needed updating because of the difficulty in identifying the origin of digital communications.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

In thinking about these past amendments, and the critical issues at stake in the recent round of changes to FISA, one must also keep in mind two technological issues that prompted the need for FISA modernization after 9/11. One poses a difficulty for government surveillance; the other offers new promise to heighten its effectiveness. The first technological issue is the increasing challenge of determining the source of an electronic communication. FISA was based on a paradigm in which land-line telephones were associated with area codes and country codes, which made it possible to know if someone was located in the United States or not. In contrast, e-mails, Voice Over Internet Protocol (VOIP), and other kinds of digital telecommunications are not necessarily linked to a physical location. As David Kris explains, "The central operational problem in foreign intelligence surveillance is the difficulty of determining, at least in real time, the location of communicating parties who do not wish to be found." n71

FISA needed revising- it was person-focused instead of data-focused.
Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

Today's statute adopts what I will call a "person-focused" approach; its standards depend heavily on the identity and location of who is being monitored. The statute generally assumes that the subject of monitoring is a known person, and it then articulates standards for when that person's communications can be collected. This made sense in the era of the old-fashioned telephone network, when the government needed to identify a person before knowing what communications line to tap. But modern communications networks work very differently, and modern Fourth Amendment law accommodates the shift. Surveillance over modern packet-switched networks is often "data-focused"; the identity of who sent data or where that person is located often will be unknown or unknowable. Whereas traditional investigations were person-focused, tracing from people to their data, many of today's investigations are data-focused, tracing from data to the people who sent and received them.

FISA is irrelevant because it cannot keep up with technological advances.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

This Note does not seek to argue that the type and degree of foreign intelligence surveillance currently being undertaken by the federal government is illegal, oppressive, or unwise. Rather, it seeks to point out how technological advancements have rendered America's foreign intelligence legal regime irrelevant by causing a massive disconnect between its goals and its real world impact.

Pro- Terrorism- FISA Amendments

Modern surveillance must be data-focused. Digital communications make finding the location of a person and identifying characteristics of them next to impossible.
Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

Why do these details matter? They matter because they mean that modern network surveillance often works very differently than traditional telephone wiretapping or bugging. In particular, today's surveillance tends to be divorced from the identity and location of the parties to the communication. There is no known wire linked to a known person with known characteristics. Instead, a surveillance device must be inserted into a stream of packet traffic that either is configured to copy all the traffic for subsequent analysis or else to filter in real time based on known characteristics of the traffic. n47 Whether the filter is done in real time or later on, the data stream must be screened for known traffic characteristics rather than known identities. The focus must be on the data, not known persons who sent or received that data.
In this new world, the location of the surveillance no longer correlates to the location of the individuals surveilled. In particular, any point on the network will include a great deal of what James Risen has called "transit traffic" -- communications traffic that just happens to be passing through. n48 Given the dominant role of the United States in modern communications technology, much of that transit traffic is directed through communications switches in the United States. [*235] Communications service providers in the United States end up playing host to a great deal of traffic sent and received from individuals located abroad. n49 Monitoring a particular river of packet-based traffic in the United States will pick up an incredible diversity of traffic, ranging from your mom's family email to parts of an encrypted phone call sent from Afghanistan to Iraq. n50
Further, the kind of characteristics that the government might use to identify foreign intelligence information usually no longer includes a link to known individuals or places. Imagine the military seizes an al Qaeda computer in Iraq and sends it for analysis. That analysis might reveal the use of particular service providers, particular programs, particular encryption methods, or other information about traffic characteristics. However, it is unlikely to reveal anyone's identity: terrorists presumably do not use identifying email addresses like osama.binladen @gmail.com. Nor is it particularly likely to reveal anyone's location with any certainty: although IP addresses can give clues to location, they are not a clear indication of it. n51 In this setting, the government's goal must be to identify traffic that might provide sources of information rather than particular individuals likely to have it. n52

Pro- Terrorism- FISA Amendments

FISA originally person focused.
Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

When Congress began drafting foreign intelligence surveillance bills in the mid-1970s, it naturally adopted the person-focused approach reflected in then-existing technology and constitutional law. FISA's standards focused heavily on the identity and location of the person monitored. The basic structure of the statute assumes that the [*230] government starts with a suspect and then seeks authorization to collect that person's communications. Although amendments to FISA have made slight progress away from that 1970s ideal, the assumption remains a basic principle of FISA.

FISA becoming more date focused which is less intrusive.
Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

In contrast, the less invasive FISA authorities added after 1978 are more data-focused. Congress added subpoena-like authority to compel evidence from third parties in the form of National Security Letters (NSLs) and § 215 orders, n35 and a pen register and trap and trace section analogous to the pen/trap provisions used in criminal investigations. n36 These sections are keyed to whether the information collected is relevant. The law permits data collection when "the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities." n37 Why the focus on information instead of people for these particular powers? The likely reason is that pen/trap and NSL authorities are preliminary powers. They regulate less intrusive measures designed to reveal agents of foreign powers rather than monitor known ones.
But should the data-focused approach of the less invasive FISA authorities be replicated throughout the statute? In the remainder of this essay, I make the case that it should.

Technology and 4th Amendment increasingly data-focused.
Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

Specifically, this Part explains how the person-focused FISA of 1978 rests on assumptions about technology and constitutional law that are often no longer valid today. The technology and constitutional law of intelligence investigations has become heavily data-focused [*233] rather than person-focused. Both internet technologies and modern Fourth Amendment law key more to information collected and less to who sent or received it. Many investigations will unfold just as they did in the 1970s. However, in many cases the government will not know who sent or received particular communications or where that person was located. Nor will it necessarily need to know that information, because location and identity are much less important than relevance. What matters is the information rather than the individual who served as its source.

Pro- Terrorism- PATRIOT Act

PATRIOT Act helps prevent terrorism in a number of ways: 1) one search warrant for downstream communication providers 2) warranted search of voice emails 3) pen register and trap and trace liberalization

Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

While the ACLU's concerns are valid, they do not accurately reflect the intent of the legislative provisions or their operation. The USA Patriot Act enhances the ability of our intelligence and law enforcement communities to detect and prevent terrorist attacks.

Before the USA Patriot Act was adopted, local courts could only authorize wiretaps within the jurisdiction of the court. n414 Search warrants issued for email communications could not extend beyond the jurisdiction of the court issuing it. n415 For example, if a court in Tampa ordered a search warrant on Wile E. [*233] Hacker, and during the course of the investigation a new email account is discovered on an internet service provider in San Francisco, law enforcement had no right to search that email account without obtaining an additional search warrant for that jurisdiction. n416 The USA Patriot Act changed these limitations by giving the courts permission to compel assistance from any communications provider in the U.S whose assistance is appropriate to further an investigation. n417 This allows federal investigators authority to execute the same search warrant on any downstream communication provider, regardless of the state in which it is operating.

Before the USA Patriot Act, the use of voice communications in email created a quandary for law enforcement because voice communications were protected by much more restrictive wiretap orders. n418 Law enforcement officers, even with a subpoena, could acquire a limited amount of information from an internet service provider. n419 Moreover, the Cable Act n420 set out an extremely restrictive set of rules governing law enforcement access to records held by local cable companies. n421 After adoption of the USA Patriot Act, law enforcement can obtain voice mail and other stored voice communications once a search warrant has been authorized. n422 The Act significantly expands the data that can be obtained from an internet service provider. n423 The Cable Act has also been amended to allow law enforcement to subpoena customer records without notification to the customer. n424

Moreover, Sections 214 and 215 of the USA Patriot Act had the impact of liberalizing the use of pen register and trap and trace devices in addition to allowing law enforcement to require [*234] the production of any tangible things relevant to an international terrorism investigation. n425

Pro- Terrorism- PATRIOT Act

Pre-PATRIOT Act surveillance maintained a wall between intelligence gathering and law enforcement, which made task of preventing terrorism more difficult. The PATRIOT Act amended FISA to allow for greater coordination during surveillance operations.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

[*222] Thus, the wall was effective in preventing cooperation and coordination between intelligence and law enforcement, precisely the opposite of what is necessary in order to respond to quickly developing events involving terrorist activities within and outside of the U.S. Before the USA Patriot Act, the wall "often precluded effective and vital information sharing between the intelligence community and law enforcement." n336 The wall was the result of a judicial belief that it could approve applications for electronic surveillance as long as the government's objective was not "primarily" directed toward criminal prosecution of foreign agents. n337
The Attorney General addressed this "wall" problem and others through provisions of the USA Patriot Act. n338 The Act made two significant changes to FISA. First, Section 218 removed the "primary purpose" language and replaced it with "a significant purpose" standard, permitting the use of FISA when "a significant purpose of the search or surveillance was foreign intelligence." n339 Second, the USA Patriot Act made it clear in Section 504(a) that "coordination between intelligence and criminal [*223] personnel was not the grounds for denying a FISA application." n340 Moreover, after the "enactment of the USA Patriot Act, the [Justice] Department promulgated new procedures ... that expressly authorized -- and indeed required -- coordination between intelligence and law enforcement." n341 The legality of these new procedures became the subject of a FISA Court opinion which rejected them in part on May 17, 2002. n342 However, the new procedures were later approved by the FISA Review Court on November 18, 2002. n343
The FISA Review Court held that the wall imposed by the various agencies as a result of judicial interpretation was not legally required, thus clearing the way for more information sharing between law enforcement and intelligence authorities. n344

Pro- Terrorism- Public/Private Partnership

Information is the new battlefield in the War on Terror. Any new data point could be the new clue that stops another 9/11 style attack. Public-private partnerships are critical in this regard since private industries have unparalleled access and can obtain and share the information more easily with fewer legal restrictions.

Jon D. Michaels, Prof Law @ UCLA; August 2008 (California Law Review; 96 Calif. L. Rev. 901; "All the president's spies: Private-public intelligence partnerships in the War on Terror")

Unable to target or repel terrorists using conventional military tactics and munitions alone, the United States is acutely aware that today's pivotal battlefield is an informational one. Teams of U.S. intelligence agents, acting as eavesdroppers, infiltrators, interrogators, and data-miners, must race against the clock to anticipate terrorists' actions, frustrate their missions, and dismantle their infrastructure. n1 Because the U.S. government does not know the who, [*902] what, where, and when of the next terrorist strike, but recognizes that the plot might be hatched on domestic soil, its first step must be to cast a wide net to gather all sorts of data points, n2 any one of which might be the clue that leads intelligence agents to prevent another September 11-like catastrophe. n3 In this regard, there is no better ally than the private sector. Its comparative advantage over the government in acquiring vast amounts of potentially useful data is a function both of industry's unparalleled access to the American public's intimate affairs - access given by all those who rely on businesses to facilitate their personal, social, and economic transactions - and of regulatory asymmetries insofar as private organizations can at times obtain and share information more easily and under fewer legal restrictions than the government can when it collects similar information on its own. n4

The government is dependent on private data from businesses in the War on Terror.

Jon D. Michaels, Prof Law @ UCLA; August 2008 (California Law Review; 96 Calif. L. Rev. 901; "All the president's spies: Private-public intelligence partnerships in the War on Terror")

Technological advances and the concomitant universal reliance on such innovations to communicate and to conduct personal and business transactions electronically have generated an unprecedented number of data points about individuals who use email, surf the web, speak via telephone, wire money, bank, travel commercially, and transact business via the Internet. n18 All of the information about particular electronic transactions (and all of the background details people supply to subscribe to shopping or frequent-traveler membership clubs or to gain access to websites' content) is possessed in large measure by private firms involved in commerce, finance, and telecommunications. n19 With high-powered computers and increasingly sophisticated software, n20 analysts can mine these stores of data and detect particularly significant patterns of behavior, including activities ostensibly indicative of terrorist planning. n21 People simply do not interface with the government in the same ways or with the same frequency as they do with the private sector, and thus the intelligence agencies find themselves particularly drawn to, and in some respects dependent upon, private data resources. n22

Pro- Leaks bad- National Security

Leaks of classified information undermine national security.
Geoffrey Stone, Prof Law @ U Chicago; June 12, 2013 (DemocracyNow.Org; "Is Edward Snowden a hero? A debate with journalist Chris Hedges & law scholar Geoffrey Stone";
http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a)

The question, why I think he deserves punishment, is—he said it actually himself in the clip that you played earlier: He said, "I'm just an ordinary guy." Well, the fact is, he's just an ordinary guy with absolutely no expertise in public policy, in the law, in national security. He's a techie. He made the decision on his own, without any authorization, without any approval by the American people, to reveal classified information about which he had absolutely no expertise in terms of the danger to the nation, the value of the information to national security. That was a completely irresponsible and dangerous thing to do. Whether we think it was a positive thing in the long run or not is a separate question, but it was clearly criminal.

Pro- Terrorism Bad- Civil Liberties

Another terrorist attack in the style of 9/11 would destroy civil liberties more effectively than anything else, including domestic surveillance. Prefer this evidence- it is comparative of civil liberties violations between terrorism and surveillance.

Geoffrey Stone, Prof Law @ U Chicago; June 12, 2013 (DemocracyNow.Org; "Is Edward Snowden a hero? A debate with journalist Chris Hedges & law scholar Geoffrey Stone"; http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a)

Let me make another point about civil liberties here, by the way, that it's extremely important to understand that if you want to protect civil liberties in this country, you not only have to protect civil liberties, you also have to protect against terrorism, because what will destroy civil liberties in this country more effectively than anything else is another 9/11 attack. And if the government is not careful about that, and if we have more attacks like that, you can be sure that the kind of things the government is doing now are going to be regarded as small potatoes compared to what would happen in the future. So it's very complicated, asking what's the best way to protect civil liberties in the United States.

Pro- National Security Outweighs Civil Liberties

National security is a precedent toward securing civil liberties. The appropriate balance between security and liberty is removing internal and external threats. National security is the priority.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

This Article will conclude by suggesting that the appropriate balance between civil liberties and national security is achieved only when a nation is free from internal and external threats. However, the nation's security ultimately must be a priority, and a condition precedent toward securing civil liberties. When the nation is secure, its people are secure and when a nation is under attack, civil liberties become secondary to national security.

National security is a precondition for civil liberties and freedom. Prefer this evidence- it is comparative and specific to the impact of domestic surveillance on civil liberties versus terrorism.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

Thus, we have perhaps come full circle. This Article began with a review of the report of the Church Committee investigation and concerns of executive branch and intelligence agency abuse that led to the passage of FISA and implementation of Executive Order 12,333. These legislative and executive measures were meant to constrain the activities of the intelligence agencies and provide clear guidance on the constitutional limits of foreign and domestic surveillance. Today, because of the terrorist attacks the intelligence agencies will once again become a focal point as the U.S. searches for answers to the questions of why the intelligence community was not able to prevent attacks. It is possible, indeed likely that legislative solutions will be proposed to now untie the hands of the intelligence community in ways that may make it better able to combat terrorism. [*238] These are precisely the questions that were debated as the USA Patriot Act was considered and ultimately passed into law. Some suggest that the USA Patriot Act is the most dangerous kind of law, a law that was passed in the heat of emotion and in reaction to a terrible tragedy. Once again, the question of striking the balance between national security and the Fourth Amendment will be center stage. However, now the context is not domestic surveillance of individuals, organizations and watch lists, but rather terrorism.
The appropriate balance between protecting the nation and civil liberties has been reached through the Congressional legislative efforts in its attempt to make it easier to combat terrorism. The genius of democratic society is that, though the system is not perfect, it does work. The constitutional checks and balances operate well to curtail overzealous executive, legislative or judicial activity regardless of the catalyst for overzealousness. As the Fourth Amendment cases have held, the purpose of the criminal law is to punish and deter crime. However, the purpose of intelligence collection is "stop or frustrate the immediate criminal activity." n442 The cases reviewed in this Article have found that the Congress struck an appropriate balance between national security and Fourth Amendment privacy concerns.
In the final analysis, it becomes very difficult to preserve civil liberties if the survival of the nation is in the balance. Without a secure nation, civil liberty becomes a function of those in control of the government. Thus, by preserving the nation we are better able to preserve freedom.

Pro- National Security Outweighs Civil Liberties

Multiple historical examples of wartime suspension of civil liberties- national security and civil liberties are not mutually exclusive.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

National security and civil liberty interests are not mutually exclusive. We can and must balance both interests appropriately because, in the final analysis, if we cannot secure our nation, civil liberties will mean very little. History demonstrates that when the nation is *in extremis*, laws bend. Several examples prove this point. President Lincoln ordered a blockade of the southern ports and suspended the right of *habeas corpus* during the Civil War. n21 During World War II, the U.S. ordered the internment of Japanese Americans on the West Coast. n22 Most recently, during the war on terrorism, several American citizens were indefinitely detained by the military as "enemy combatants." n23 Precedent supports the government. During World War II, the federal courts upheld the government's right to hold captured Nazi spies as unlawful enemy combatants. n24 The Latin maxim, *inter arma silent leges* is often invoked to explain the government's tendency toward self-preservation during national emergency. The phrase means "in times of war, the laws are silent." n25 Yet, the laws are not silent, nor should they be. The laws will probably be interpreted to support the government's tendency toward self-preservation when a "threat to the nation's security is real," but they should never be silent altogether. n26

Pro- Authorization of the Use of Military Force

AUMF gives the president powers for warrantless domestic surveillance.
Former Attorney General Alberto Gonzales; December 19, 2005 (White House Archives; "Press briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence"; http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051219-1.html)

Now, in terms of legal authorities, the Foreign Intelligence Surveillance Act provides -- requires a court order before engaging in this kind of surveillance that I've just discussed and the President announced on Saturday, unless there is somehow -- there is -- unless otherwise authorized by statute or by Congress. That's what the law requires. Our position is, is that the authorization to use force, which was passed by the Congress in the days following September 11th, constitutes that other authorization, that other statute by Congress, to engage in this kind of signals intelligence.
Now, that -- one might argue, now, wait a minute, there's nothing in the authorization to use force that specifically mentions electronic surveillance. Let me take you back to a case that the Supreme Court reviewed this past -- in 2004, the Hamdi decision. As you remember, in that case, Mr. Hamdi was a U.S. citizen who was contesting his detention by the United States government. What he said was that there is a statute, he said, that specifically prohibits the detention of American citizens without permission, an act by Congress -- and he's right, 18 USC 4001a requires that the United States government cannot detain an American citizen except by an act of Congress.
We took the position -- the United States government took the position that Congress had authorized that detention in the authorization to use force, even though the authorization to use force never mentions the word "detention." And the Supreme Court, a plurality written by Justice O'Connor agreed. She said, it was clear and unmistakable that the Congress had authorized the detention of an American citizen captured on the battlefield as an enemy combatant for the remainder -- the duration of the hostilities. So even though the authorization to use force did not mention the word, "detention," she felt that detention of enemy soldiers captured on the battlefield was a fundamental incident of waging war, and therefore, had been authorized by Congress when they used the words, "authorize the President to use all necessary and appropriate force."
For the same reason, we believe signals intelligence is even more a fundamental incident of war, and we believe has been authorized by the Congress. And even though signals intelligence is not mentioned in the authorization to use force, we believe that the Court would apply the same reasoning to recognize the authorization by Congress to engage in this kind of electronic surveillance.

Pro- PATRIOT Act

PATRIOT Act is a balance between security and liberty.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

[*228] Congress was well aware that the USA Patriot Act would break down barriers between intelligence collection and law enforcement. n373 Senator Feingold expressed concern that the "significant purpose" amendment may be used to abuse Fourth Amendment protections. n374 However, the balance between national security and civil liberties was struck by Congress in the amendments to FISA. For those who were concerned that the amendments gave the government too much power, Senator Leahy suggested that "it will be up to the courts to determine how far law enforcement agencies may use FISA for criminal investigation and prosecution beyond the scope of the statutory definition of foreign intelligence information." n375

PATRIOT Act unlikely to be rule unconstitutional on 4th Amendment grounds since the courts will defer to political branches. Especially true in light of concern for civil liberties and national security in PATRIOT Act.
William Funk, Robert E. Jones Prof Law @ Lewis & Clark; Summer 2011 (Mississippi Law Journal; 80 Miss. L. J. 1491; "Electronic surveillance of terrorism in the United States")

The issue here is less whether FISA as amended is constitutional according to established constitutional doctrine massaged in the inimitable American way, but rather the questions it raises about the nature of the struggle against international terrorism and the appropriate means to combat that terrorism consistent with retaining the individual freedoms citizens of developed nations have come to expect. First, we should not expect bi-partisan determinations agreed to by both political branches in an area of national security, in an apparent attempt to balance the needs of national security with individual liberties, to be likely overturned by courts on the basis of the Fourth Amendment." Here, the USA-PATRIOT Act amendment was made in the immediate aftermath of the 9/11, but it originally had a sunset provision that required it to be reconsidered in the future, under calmer conditions. It was, and the "significant purpose" change was retained. In other words, despite our general reliance on courts to protect individual liberties, history suggests that when national security is threatened from foreign aggressors, courts are likely to defer to the political branches. Here, moreover, that deference seems especially deserved, given the expression of [*1504] concern for protecting both civil liberties and national security contained in the congressional materials.

Pro- Protect America Act

Protect America Act expands privacy protections- approval required for foreign surveillance of U.S. citizens, reverse targeting prohibited, and new mechanisms for oversight and audit.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

We have thus far considered Congress's crafting of new rules for some of the contested NSA behavior through the FAA. This statute also expands FISA's existing privacy protections. Until this new enactment, FISA had not regulated surveillance of targets, whether U.S. citizens or not, when they were located outside the United States. The FAA now requires that a FISC approve surveillance of a U.S. citizen abroad based on a finding that the person is "an agent of a foreign power, or an officer or employee of a foreign power." n56
The statute also contains a prohibition on "reverse targeting." As discussed, the FAA permits surveillance of foreign-to-domestic communications that have a nexus to "foreign intelligence." Reverse targeting would involve the government using this link as a pretext to gather intelligence about the domestic party to the communication. The FAA states that the government cannot target "a person reasonably believed to be outside the [*417] United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States." n57 As a final privacy safeguard, the FAA also contains new mechanisms for congressional oversight and crafts new audit functions for the Inspectors General of the DOJ and intelligence community. I will return to these safeguards in Part III.

Pro- Protect America Act

Permanent FISA amendments eliminated the constitutionally suspect language from the Protect America Act and give immunity to companies aiding in the collection process.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The Protect America Act of 2007 expired on February 1, 2008. Congress and the President extended the Act for six months, and on July 9, 2008 President Bush signed into law new amendments to FISA. n174 The permanent FISA amendments include different and potentially less constitutionally suspect language than does the Protect America Act. n175 Although the new language appears to be less constitutionally suspect, these new amendments provide immunity to companies which aid the government in collections procedures. n176 Once again, United States citizens are left without a remedy for constitutional violations. Additionally, these amendments do nothing to remedy Fourth Amendment violations which potentially occurred between August 5, 2007, and February 1, 2008. Nor does amending the Act reveal how many Americans' conversations and/or emails were warrantlessly searched and seized by the government. Thus, this Act's history and implications remain important.

Protect America Act definition of foreign allows domestic surveillance.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The definition of "foreign intelligence" is critical to the constitutional analysis of the Protect America Act. The Act does not provide a different definition of "foreign intelligence" from the one provided in FISA; thus in interpreting the Protect America Act, FISA's definition of "foreign intelligence" applies. n84 In FISA's definition, "foreign" applies to the content of the information gathered, and not to the location in (or from) which the information is gathered, or the nationality of the sources from which it is gathered. n85 Instead, "foreign intelligence" means "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against ... " harms or clandestine operations against the United States. n86 The definition [*184] does not contain any language limiting the country from which the information may be collected. n87 Thus, while the Act's asserted purpose is to collect foreign intelligence, the Act's definition of foreign intelligence does not provide inherent protection against domestic surveillance - domestic surveillance is not precluded from the definition of foreign surveillance. How an act defines its terms, rather than the terms themselves out of context, dictates the Act's application; this is a critical point in understanding the Protect America Act's far-reaching implications.

Pro- Protect America Act

Protect America Act allows surveillance directed at a person reasonably believed to be outside the U.S.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The Protect America Act redefines electronic surveillance, despite the fact that FISA's definition of foreign surveillance continues to apply. Section 2 of the Protect America Act provides the law's "first substantive provisions." n88 First, Section 2 establishes that the FISA definition for electronic surveillance, section 101(f), n89 does not apply to the activities described in the Protect America Act. n90 FISA's definition of electronic surveillance contains clauses relating to the target and the collection procedures defined as "acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication." n91 In rejecting this definition, the Protect America Act states that "nothing in the definition of electronic surveillance under section 101(f) [of FISA] shall be construed to encompass surveillance directed at a [*185] person reasonably believed to be located outside of the United States." n92 Therefore, if surveillance is directed at a person "reasonably believed to be outside the United States," FISA's definition of electronic surveillance does not apply to that intelligence gathering, because it is a Protect America Act collection, not a standard FISA collection. Such person does not benefit from FISA's protections or the limitations FISA places on intelligence collection; instead the Protect America Act governs the activities directed at that person.
Additionally, section 2 does not explicitly state that this exception to FISA's electronic surveillance definition applies only to surveillance of a foreign person. n93 It also does not "explicitly address the location of the parties to the communication or the location of the acquisition of the information involved." n94 The meaning of "directed at" could therefore permit surveillance of individuals other than the target n95 in order to gain information about that foreign target. Because FISA section 101(f) does not limit the Protect America Act, the people from whom the intelligence community gathers information about the target could include people inside the United States and/or United States citizens. n96 Congress defined the activities in the Protect America Act as outside FISA's meaning of "electronic surveillance," n97 thereby excluding those activities from the limitations placed on "electronic surveillance" by FISA, such as warrants or court approval. n98

Protect America Act does not place limitations on warrantless information acquisition of U.S. citizens.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

Unlike FISA's Section 102, which provides limitations on warrantless electronic surveillance, the Protect America Act's section 2(a) does not limit warrantless information acquisition, even if there is a substantial likelihood that a party to the surveyed communication is either a United States citizen, or an individual located within the United States. n105 Instead, section 2(a) allows the President to authorize warrantless collection of foreign intelligence for up to one year, provided that: n106

1. "there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States;" n107
2. "the acquisition does not constitute electronic surveillance;" n108
3. "the acquisition involves obtaining the foreign intelligence information from or with the assistance of communications service provider, custodian, or other person...who has access to communications;" n109
4. "a significant purpose of the acquisition is to obtain foreign intelligence information;" n110 and [*187] 5. FISA Section 101(h) minimization procedures are followed. n111

Pro- Examples- Highlander

NSA whistleblowers concede that Highlander saved many lives in Iraq and led to the assassination of Al Qaeda operatives.

Jonathan D. Forgang, JD Fordham Univ Law; October 2009 (Fordham Law Review; 78 Fordham L. Rev. 217; " 'The right of the people': The NSA, the FISA amendments act of 2008, and foreign intelligence surveillance of Americans overseas")

National security surveillance like the Highlander program inevitably invades the privacy of its monitored targets. This invasion is often justified when it is necessary to protect American interests. There is little doubt that the Highlander surveillance has greatly enhanced the safety of Americans. Kinne and Faulk both claim that the surveillance helped the military disarm improvised explosive devices (IEDs) and preemptively capture dangerous persons intending to harm U.S. servicemen in Iraq. n12 The United States also used the surveillance to help assassinate one of the al Qaeda operatives responsible for the USS Cole bombing. n13

Pro- AT: 1st Amendment/Unconstitutional

No 1st Amendment violations.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

More recent surveillance cases have followed the lead of the Laird Court. Challenges to the NSA's wiretapping program have foundered because plaintiffs have failed to convince federal courts that secret surveillance has caused them any legally cognizable injury. In ACLU v. NSA**,** n54 the Sixth Circuit dismissed any suggestion that First Amendment values were threatened when the government listened to private conversations. As that court put it: "The First Amendment protects public speech and the free exchange of ideas, while the Fourth Amendment protects citizens from unwanted intrusion into their personal lives and effects." n55 The court concluded that the plaintiffs had [*1944] no standing to assert First or Fourth Amendment violations, as they could not prove that the secret government surveillance program had targeted them. n56 Similarly, in Al-Haramain Islamic Foundation, Inc. v. Bush, n57 the government successfully invoked the state-secrets doctrine to stop the plaintiffs from finding out whether they were the subjects of secret surveillance under the program. n58 This ruling created a brutal paradox for the plaintiffs: they could not prove whether their telephone calls had been listened to, and thus they could not establish standing to sue for the violation of their civil liberties. n59 Despite the fact that the judges in the case knew whether surveillance had taken place, they believed that the state-secrets doctrine barred them from ruling on that fact. n60 And the Court's most recent decision in Clapper affirmed this approach to standing to challenge surveillance. Plaintiffs can only challenge secret government surveillance they can prove, but the government isn't telling. Plaintiffs (and perhaps civil liberties) are out of luck.

Pro- AT: 1st Amendment/Unconstitutional

The thesis that there is no such thing as free speech proves that no class of expression is separable from consequences and the decision to allow or deny speech is always already political. State intervention in speech is inevitable and desirable! Take responsibility for your speech act. The impact of hate speech outweighs the potential slippery slope towards tyranny.

Fish, Prof Law @ Florida International Univ; 94 (Stanley; There's No Such Thing As Free Speech, And It's A Good Thing Too; P. 114- 115)

It is a counsel that follows from the thesis that there is no such thing as free speech, which is not, after all, a thesis as startling or corrosive as may first have seemed. It merely says that there is no class of utterances separable from the world of conduct and that therefore the identification of some utterances as members of that nonexistent class will always be evidence that a political line has been drawn rather than a line that denies politics entry into the forum of public discourse. It is the job of the First Amendment to mark out an area in which competing views can be considered without state interference; but if the very marking out of that area is itself an interference (as it always will be), First Amendment jurisprudence is inevitably self-defeating and subversive of its own aspirations. That's the bad news. The good news is that precisely because speech is never "free" in the two senses required—free of consequences and free from state pressure—speech always matters, is always doing work; because everything we say impinges on the world in ways indistinguishable from the effects of physical action, we must take responsibility for our verbal performances—all of them—and not assume that they are being taken cares of by a clause in the Constitution. Of course, with responsibility comes risks, but they have always been our risks, and no doctrine of free speech has ever insulated us from them. They are the risks, respectively, of permitting speech that does obvious harm and of shutting off speech in ways that might deny us the benefit of Joyce's Ulysses or Lawrence's Lady Chatterly's Lover or Titian's paintings. Nothing, I repeat, can insulate us from those risks. (If there is no normative guidance in determining when and what speech to protect, there is no normative guidance in determining what is art—like free speech a category that includes everything and nothing—and what is obscenity.) Moreover, nothing can provide us with a principle for deciding which risk in the long run is the best to take. I am persuaded that at the present moment, right now, the risk of not attending to hate speech is greater than the risk that by regulating it we will deprive ourselves of valuable voices and insights or slide down the slippery slope toward tyranny. This is a judgment for which I can offer reasons but no guarantees. All I am saying is that the judgments of those who would come down on the other side carry no guarantees either. They urge us to put our faith in apolitical abstractions, but the abstractions they invoke—the marketplace of ideas, speech alone, speech itself—only come in political guises, and therefore in trusting to them we fall (unwittingly) under the sway of the very forces we wish to keep at bay. It is not that there are no choices to make or means of making them; it is just that the choices as well as the means are inextricable from the din and confusion of partisan struggle. There is no safe place.

Pro- AT: 4th Amendment/Unconstitutional

Obama's surveillance is different from Bush's- he has Congressional approval and does not use wiretapping.
Geoffrey Stone, Prof Law @ U Chicago; June 12, 2013 (DemocracyNow.Org; "Is Edward Snowden a hero? A debate with journalist Chris Hedges & law scholar Geoffrey Stone"; http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a)

GEOFFREY STONE: They're two completely different programs. The Bush NSA surveillance program was enacted in direct defiance of the Foreign Intelligence Surveillance Act. The Obama program, if we want to call it that, was approved by Congress. That's number one. Number two is, the Bush program involved wiretapping of the contents of phone conversations. The Supreme Court has long held that that is a violation of the Fourth Amendment, if there's not an individualized determination of probable cause. The Obama program, if we want to call it that, does not involve wiretapping; it involves phone numbers. And the Supreme Court has long held that the government is allowed to obtain phone records, bank records, library records, purchase records, once you disclose that information to a third party. And there is no Fourth Amendment violation. So they're two completely different programs.

NSA domestic surveillance is legal- does not violate constitution.
Geoffrey Stone, Prof Law @ U Chicago; June 12, 2013 (DemocracyNow.Org; "Is Edward Snowden a hero? A debate with journalist Chris Hedges & law scholar Geoffrey Stone"; http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a)

GEOFFREY STONE: Well, first of all, there is, so far as I can tell from everything that's been revealed, absolutely nothing illegal or criminal about these programs. They may be terrible public policy—I'm not sure I approve of it at all—but the fact is the claim that they're unconstitutional and illegal is wildly premature. Certainly from the standpoint of what's been released so far, whether Mr. Hedges likes it or not, or whether Mr. Snowdon likes it or not, these are not unconstitutional or illegal programs.

PATRIOT Act made it easier to obtain FISA warrants.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

Although the NSA is not generally permitted to conduct domestic surveillance for law enforcement purposes, information about U.S. citizens obtained under a FISA warrant may be used in criminal proceedings against them. n88 The information sought to be used need not be evidence of a crime related to espionage. The only limitation is that the collection of foreign intelligence information must have been a "significant" purpose of the FISA surveillance. n89 Prior to the passage of the USA PATRIOT Act in 2001, n90 the collection of foreign intelligence [*520] information needed to be the "primary purpose" of FISA surveillance. Now, it need only be a "significant purpose" of the surveillance in order for a FISA warrant to be issued. n91 This change drastically increased the ease with which government agents can obtain domestic surveillance warrants under FISA.

Pro- AT: 4th Amendment/Unconstitutional

The impact is inevitable since warrantless surveillance of foreigners' communication with U.S. citizens was legal before 9/11.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

With respect to ECHELON, the restrictions imposed by Executive Order No. 12,333 and FISA apply only to situations where the NSA seeks to conduct surveillance within the United States or against U.S. persons abroad. n114 Virtually no restrictions are placed on the ability of the agency to conduct such surveillance on non-U.S. persons located outside the territorial limits of the United States. n115 Because the NSA is allowed to conduct virtually unfettered surveillance of foreign persons outside the United States, American citizens may be inadvertently surveilled by the NSA without a warrant whenever they communicate with foreign persons located in other countries. n116 Even assuming that the NSA does not routinely engage in the interception of domestic U.S. signals, the capture of so many foreign communications still results in the collection, without a warrant, of a significant number of phone calls made to and from U.S. persons each year. n117 Presumably, such situations occurred even prior to President Bush's issuance of the secret executive order allowing warrantless domestic surveillance in apparent violation of FISA. n118

Unintentional and inadvertent surveillance of domestic electronic communications involving U.S. citizens is legal under U.S. Signals Intelligence Directive 18 (USSID 18).
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

It is the stated policy of the NSA "to target or collect only foreign communications." n126 USSID 18 makes clear that the NSA "will not intentionally collect communications to, from or about U.S. persons or persons or entities in the United States," except as allowed under its provisions. n127 Although the NSA generally may not intentionally collect the communications of U.S. persons without a FISA warrant, USSID 18 specifically states that the agency may collect such communications unintentionally. n128 More specifically, section 3.1 of USSID 18 states that if the NSA "inadvertently" collects communications made to or from U.S. persons who were not the lawful target of the surveillance efforts, the [*526] agency may still retain, analyze, and disseminate such information under certain circumstances. n129

Miller and Smith decisions prove NSA data mining does not violate the 4th Amendment because there is not a reasonable expectation of privacy from third parties.
Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

Both United States v. Miller n109 and Smith v. Maryland, n110 decided in a span of three years, indicate that a person does not have a legitimate expectation of privacy in records that are voluntarily conveyed to a third-party. In Miller, the issue was whether the government violated the Fourth Amendment by requiring a bank to copy and inspect a person's records. n111 The Court held that a person had no reasonable expectation of privacy in information held by the third-party bank. n112 Similarly, in Smith, the issue was whether the government had performed a search under the Fourth Amendment n113 when a phone company, at the government's request, installed a pen register to record the numbers dialed. n114 The Court held that the person had no privacy expectation in the dialed numbers because those numbers are necessarily conveyed to the phone providers. n115

Pro- AT: 4th Amendment/Unconstitutional

4th Amendment is more focused on methods of surveillance and the information collected rather than protecting persons.

Orin S. Kerr, Prof Law @ George Washington Univ; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 225; "Surveillance: Updating the Foreign Intelligence Surveillance Act")

Consider the evolution of the Fourth Amendment "search" doctrine. In 1967, Katz proclaimed that "the Fourth Amendment protects people, not places," n53 which suggested that the law would make individualized determinations into how much the government invaded a person's privacy. But the law evolved differently. Instead of making individualized determinations, surveillance law has tended to focus on the methods of surveillance and the information the government collects. [*236] Although much of the law remains uncertain, n54 existing law has hardened into rules that pay little attention to identity or context. Some techniques never amount to Fourth Amendment searches, including undercover operations, n55 the installation of pen registers, n56 intercepting cordless phone calls, n57 surveillance in public, n58 and acquiring noncontent account records. n59 Other techniques are always or virtually always searches, such as wiretapping the contents of landline phone calls. n60 The rule-like nature of the Fourth Amendment "search" doctrine means that how the Fourth Amendment applies often does not depend on who is monitored or where. n61
The law governing the reasonableness of searches has changed as well. With the benefit of hindsight, we can now see that Keith was an early application of the Fourth Amendment's "special needs" doctrine, n62 which permits relaxed Fourth Amendment standards when government actors conduct searches and seizures for reasons beyond [*237] traditional law enforcement. Since Keith, the Supreme Court has refined and generalized the special needs doctrine; over time its emphasis has changed. Whereas Keith focused on identity, modern special needs cases focus on the "programmatic purpose" of governmental conduct. n63 The initial inquiry identifies the overarching purpose of the government's surveillance scheme rather than the identity of who is searched or seized. n64 The non-law enforcement interests involved are then balanced against the intrusiveness of the government's conduct. n65 Like the Fourth Amendment's search inquiry, reasonableness looks less to identity and context of the person monitored and more at the nature of the government's conduct. n66

Evidence of NSA domestic surveillance would be inadmissible because of state secrets privilege.

Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

In contrast to the Totten categorical bar, the government can likely assert the state secrets privilege under the second ground, as both conditions are likely met. It likely has asserted the privilege correctly, n152 and there have been no public disclosures meaning that any future disclosures could potentially be dangerous to national security. n153 The court in Hepting v. AT&T Corp. n154 agreed that both conditions were met, and the privilege applies. However, the court reluctantly reached this conclusion because NSA public disclosures about other security programs may have alerted any potential terrorists to the call database. n155 In fact, the court even warned that if any public disclosures occurred accidentally or deliberately later on, then those disclosures might preclude the government from asserting the state secrets privilege. n156

Pro- AT: 4th Amendment/Unconstitutional

Foreign intelligence sharing makes the impact inevitable.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

Another issue arises from the fact that Executive Order 12,333 allows U.S. government agencies to accept intelligence about U.S. citizens acquired by foreign governments, regardless of how the information was obtained. Given the secrecy and collaboration that takes place in the UKUSA security agreement, the concern is that the NSA is side-stepping FISA by simply allowing a foreign government to spy on U.S. citizens and then freely sharing in the resulting intelligence. Although Executive Order 12,333 forbids the NSA from actively soliciting a foreign agency to conduct surveillance that the NSA could not conduct on its own, n87 there is evidence that the rule enjoys very little fidelity. Even assuming that the NSA strictly adheres to Executive Order 12,333 and accepts and shares intelligence only in good faith, the synergistic nature of the UKUSA pact may make the practice of intelligence sharing within the pact unconstitutional. A more detailed analysis of this idea is provided in the next section.

Pro- AT: Accountability/National Security Secrecy Bad

Department of Justice and Attorney General review and authorization of warrantless domestic surveillance under Bush led to accountability and revision of questionable actions.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

The end of the forty-five day period occurred at a time when Attorney General Ashcroft was hospitalized and had transferred his responsibilities to Deputy Attorney General Comey, who became the Acting Attorney General. When the White House learned that the Justice Department was withdrawing its imprimatur for the surveillance program, White House Counsel Alberto Gonzales went to Ashcroft's hospital room, apparently to ask him to overrule Comey. In dramatic testimony before the Senate Judiciary Committee in 2007, Comey testified about the March 2004 confrontation between Gonzales and the Justice Department lawyers in Ashcroft's hospital room. n167 Ashcroft refused to re-approve the program, and the Bush Administration reauthorized the program without the Attorney General's certification. n168 In response, Comey and other high level Justice Department officials, including FBI director Robert Mueller, prepared to resign. n169 President Bush's Chief-of-Staff Andrew Card expressed concern "that there were to be a large number of resignations at the Department of Justice." n170 Later, Comey and Mueller each met privately with President Bush, and after those meetings, the President indicated that the program would be modified so that it could receive the Justice Department's approval. n171

Foreign intelligence surveillance court and Justice Department review provided additional accountability mechanisms for domestic electronic surveillance.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

The Justice Department informed the Chief Judge of the Foreign Intelligence Surveillance Court (FISC) about the program, and that judge expressed concern about the program's possible illegality. n176 The judge did not believe that she had the power to rule on the legality of the program, but did insist that the government not use any information derived from the program in its warrant applications with the FISC. n177 When a senior Justice Department lawyer discovered that such information had been used in FISA warrant applications and informed the FISC Chief Judge, the judge complained to the Attorney General and insisted "that high-level Justice officials certify the [warrant application] information was complete" in order to prevent future lapses. n178 The Justice [*396] Department temporarily suspended part of the program and instituted tighter controls. n179

Pro- AT: Accountability/National Security Secrecy Bad

President Bush modified domestic surveillance to allow judicial review.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

In January 2007, the Bush Administration apparently modified the surveillance program and brought it under the supervision of the Foreign Intelligence Surveillance Court (FISC). n228 While the Bush Administration officials initially described the program as broad enough to target communications where there is "a reasonable basis to conclude that one party to the communication is ... a member of an organization affiliated with al Qaeda," n229 this new iteration of the program called for targeting "communications into or out of the United States where there is probable cause to believe that one of the communicants is a member or agent of al Qaeda or an associated terrorist organization." n230 This decision constitutes partial rectification by ceasing the most controversial aspect of the program: the lack of any judicial supervision. The decision to bring the program under court supervision may have been caused by pressure from the cooperating telecommunications companies or by the prospect of a less friendly 110th Congress controlled by the Democratic Party.

FAA was a step in the right direction regarding national security secrecy.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

In this light, the FAA takes modest steps in the right direction. We can consider, for example, its new requirements regarding reporting to Congress and inspector general audits. Every six months, the attorney general and the director of national intelligence (DNI) are to assess compliance with targeting and minimization procedures and to submit their report to the congressional committees with oversight responsibilities. In addition, the inspectors general of the DOJ and each relevant element of the intelligence community are to review: (1) the compliance with the adopted targeting and minimization procedures; (2) the number of disseminated intelligence reports that involved U.S. persons; and (3) the number of targets that were later determined to be located in the United States.

Pro- AT: Binney & Tice

Binney and Tice left he NSA years ago- they do not know the inner workings any more.
Joel Brenner, former NSA inspector general; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

JOEL BRENNER: I think you're talking about Mr. Tice and Mr. Binney.
Mr. Binney hasn't been at the agency since 2001. Mr. Tice hasn't been at the agency since 2005. They don't know what's going on inside the agency.

Pro- AT: Blackmail

Little to no risk of blackmail from domestic surveillance in current political climate.
Richard Posner, U.S. 7th Circuit Court Appeals & Senior Lecturer Law @ Univ Chicago; December 21, 2005 (Washington Post; "Our domestic intelligence crisis"; http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html)

The data that make the cut are those that contain clues to possible threats to national security. The only valid ground for forbidding human inspection of such data is fear that they might be used to blackmail or otherwise intimidate the administration's political enemies. That danger is more remote than at any previous period of U.S. history. Because of increased political partisanship, advances in communications technology and more numerous and competitive media, American government has become a sieve. No secrets concerning matters that would interest the public can be kept for long. And the public would be far more interested to learn that public officials were using private information about American citizens for base political ends than to learn that we have been rough with terrorist suspects -- a matter that was quickly exposed despite efforts at concealment.

Pro- AT: Data Mining

Data mining on foreign intelligence has always been permitted and is too difficult to maintain today with the problem of identifying the origin of digital communication.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

[*420] It is important to note that the concept of data mining was not unknown to the Congress that enacted FISA, nor the ones that subsequently amended it on several occasions. Here, we see that identifying a legal codification of wisdom, as Holmes wishes, can be a complex task - especially when technology is involved. Holmes speaks of rules embodied in law "as steadying guidelines, focusing our aim, and reminding us of long-term objectives and collateral dangers that might otherwise slip from view in the flurry of an unfolding crisis." n73 But what past wisdom does FISA embody? FISA had permitted data mining so long as it was carried out on telecommunications captured outside of the United States. The difficulty of determining the source of an electronic communication, as noted above, makes this an increasingly unstable compromise in the twenty-first century.

Data mining is good- led to apprehension of numerous criminals and prevented other crimes. Helped recover millions of dollars in fraudulent Medicare payments, detect money laundering and smuggling operations, and solve identity theft cases.

Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

The potential benefits of data mining are clear. Target-based programs such as REVEAL and MATRIX have helped apprehend or [*324] develop cases against numerous criminals. n29 Match-based programs like CAPPS II have undoubtedly kept some dangerous individuals off planes and probably deterred others from trying to get on. n30 Event-based data mining has helped the government recover millions of dollars in fraudulent Medicare payments, detect money laundering and immigrant smuggling operations, and solve identity theft cases. n31

Costs of data mining do not necessarily outweigh the benefits. Only prove there should be some regulation.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

These potential costs of data mining do not necessarily outweigh its benefits. But they at least suggest that data mining by the government should be subject to some regulation. [*328]

Data mining does not violate the 4th Amendment.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

The implications of Miller and Smith for data mining are fairly clear. These cases stand for the proposition that the government can obtain information about us from third parties without worrying about the Fourth Amendment. Since virtually all information obtained through data mining comes from third party record holders -- either the government itself, commercial data brokers, or a commercial entity like a bank -- its acquisition does not implicate the Fourth Amendment.

Pro- AT: FISA Good- The Wall

The predominant interpretation of FISA created a wall between intelligence and law enforcement. The FBI and NSA could coordinate with each other but not with the Justice Department or Attorney General.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office @ Time Warner, & former Assoc Deputy Attorney General @ Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

The foundations of the FISA wall lie in the "primary purpose" test described above. As that description makes clear, the wall's principal application was in limiting coordination between FBI intelligence agents and federal prosecutors. The wall did not, by its terms, limit coordination among members of the U.S. Intelligence Community - e.g., between FBI intelligence agents and the CIA or the NSA. n70 Instead, it operated within the Department of Justice - regulating contacts between the FBI and federal prosecutors in the Criminal Division and the U.S. Attorneys' Offices, and was implemented through DOJ rules, procedures, and practices.

Maintaining the wall is a key factor in preventing coordination between executive agencies.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

In maintaining the wall during the 1990s and thereafter, DOJ was highly [*500] influenced by its belief that the courts would require the wall if presented with the question (and also by the belief that if the courts dismantled it, Congress would rebuild it through legislation). The General Accounting Office (GAO) concluded in a July 2001 report that a "key factor inhibiting ... coordination [between the FBI and the Criminal Division] is the concern over how the Foreign Intelligence Surveillance Court or another federal court might rule on the primary purpose of the surveillance or search in light of such coordination." n72 As detailed below, subsequent events showed that the department's concern was entirely justified.

Constructing and tearing the wall down demonstrates the accountability and review process and well as check and balances.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

The rise and fall of the FISA wall is a case study in our constitutional system of divided government. It took all three branches of the national government to build the wall: Congress had to express a policy preference for separating law enforcement and intelligence, courts had to issue opinions implicitly reading FISA to require such separation, and the Department of [*529] Justice had to accede to those interpretations and apply them internally. Correspondingly, it took all three branches of government to tear down the wall: Congress had to pass the Patriot Act (and the president had to sign it), the Justice Department had to take an unprecedented appeal advancing novel legal arguments, and the Court of Review had to issue its decision substantially agreeing with those arguments.

Pro- AT: FISA Good- The Wall

Coordination is critical to preventing espionage and terrorism.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

There is a strong argument that the wall makes the government less effective in protecting the country from foreign threats. To those with little experience in law enforcement or national security investigations, the harm caused by limits on coordination may not be obvious. But the harm is real. n178 To protect national security effectively, domestic intelligence and law enforcement must closely coordinate their operational activities. Properly understood, they are separate but similar tools in the president's national security toolbox - far more similar to each other than either one is to other tools like diplomacy, military strikes, covert paramilitary action, or economic initiatives. They seek much the same information about foreign spies and terrorists, particularly within the United States, and they use many of the same investigative techniques to collect and process that information - for example, judicially approved, targeted searches and wiretaps (e.g., under FISA or Title III); undercover agents and recruited informants; and lures or "honeypots" to attract would-be perpetrators (although law enforcement here is circumscribed [*522] somewhat by entrapment doctrine). n179 These similarities apply not only to investigations of espionage and terrorism themselves, but also to investigations of ordinary crimes committed to finance or otherwise facilitate espionage and terrorism. n180
The similarities between intelligence and law enforcement make coordination essential. As I testified before the Senate Judiciary Committee in September 2002 (as a government witness):

When we identify a spy or a terrorist, we have to pursue a coordinated, integrated, coherent response. We need all of our best people, intelligence and law enforcement alike, working together to neutralize the threat. In some cases, the best protection is prosecution - like the recent prosecution of Robert Hanssen for espionage. In other cases, prosecution is a bad idea, and another method - such as recruitment - is called for. Sometimes you need to use both methods. But we can't make a rational decision until everyone is allowed to sit down together and brainstorm about what to do. n181 Law enforcement officials can add value to an intelligence investigation by bringing perspective, expertise, and certain investigative tools. By and large, as a result of their training and experience, prosecutors and other law enforcement officials are able and inclined to address national security threats through law enforcement efforts. n182 By bringing that perspective to bear, law enforcement officials may identify ways to neutralize a national security threat that do not occur to counterintelligence officials. For example, an assistant United States attorney may be better than an FBI intelligence agent or an OIPR lawyer at identifying a viable prosecution for providing material support to a terrorist [*523] organization. n183 If such a prosecution puts a stop to fundraising by terrorists, it protects national security.
Law enforcement officials also have expertise in conducting complex investigations and assembling cases generally, and there is a growing cadre of federal prosecutors with extensive expertise in espionage and terrorism cases. Law enforcement officials can offer assistance to intelligence agents in formulating an interview strategy to obtain leads to additional or corroborating information. They can also help to ensure that undercover operations are designed to avoid entrapment or other legal problems. Law enforcement officials experienced in national security cases can provide valuable strategic and tactical guidance on a variety of issues that may aid in protecting sensitive sources and methods and other classified information from exposure in future litigation. Such expertise helps to ensure the success of any prosecution that may occur and also helps even if no prosecution ever occurs. Many law enforcement officials have expertise in financial review and analysis and can assist intelligence agents in reviewing complex money trails. In that respect, particularly, their expertise may assist the investigation even if no prosecution is ever brought.
Finally, prosecutors and other law enforcement officials provide certain investigative tools that are not available to counterintelligence officials. Prosecutors can use the grand jury not only to obtain documents, but also to compel testimony in furtherance of a lawful criminal investigation. n184 National security letters, which may be issued by FBI agents, and FISA tangible-things orders, which may be issued by the FISA Court, are not as powerful, primarily because they cannot compel the attendance of witnesses. n185 Prosecutors can invoke mutual legal assistance treaties with other nations. And prosecutors can offer immunity from prosecution or motions for reduction in sentence in exchange for cooperation, n186 which may in certain cases produce extraordinary foreign intelligence information.

Pro- AT: FISA Good- The Wall

Our evidence is reverse causal and accesses you rights impacts. Eliminating the wall leads to better protection of rights.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

Although conventional wisdom says otherwise, there is also an argument that keeping the wall down will enhance protections for civil liberties. That is true for two reasons. First, with the wall down, more DOJ lawyers may become more involved in national security investigations, as they are now involved in ordinary criminal investigations. More lawyers means more oversight, and lawyer oversight is how this country has protected civil liberties in intelligence [*524] matters for more than thirty years. Second, in the arsenal of remedies the executive branch now has at its disposal for neutralizing foreign threats to national security, conventional law enforcement is in fact among the most benign. The wall channels government toward more extreme measures.

Having the wall down is a gentler response to the treat of spying and terror than the alternative of detention of enemy combatants.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

Critics sometimes oppose the wall on the ground that prosecutors may push national security investigations towards law enforcement remedies. As a complaint about civil liberties (rather than operational effectiveness), however, this seems misguided. Whatever may have been the case when FISA was enacted in 1978, prosecution today is among the gentlest of available remedies. Civil libertarians therefore ought to oppose the wall because it tends to channel the government towards less gentle measures.
Different national security threats suggest various responses, but there will always be some threats that, in the government's view at least, require a person to be incarcerated. Some individuals are too dangerous to be allowed freedom of movement either in the United States or abroad. That is at least as true of national security threats from terrorists and spies as it is of ordinary criminals. If some form of detention is required, the question becomes how to achieve it. The FISA wall exerts a significant effect on the resolution of that question.
With the wall down, and prosecutors allowed a seat at the inter-agency table, civilian prosecution will tend to be available as one of several options. With the wall up, however, and prosecutors excluded from discussions, law enforcement responses lose their principal spotters and advocates, leaving other alternatives more likely to prevail. n202 Today, one obvious alternative to civilian [*528] prosecution is military detention. n203 Whatever its merits as a constitutional or policy matter, n204 military detention should be far less palatable to civil libertarians than is civilian prosecution: the Supreme Court has held that "the full protections that accompany challenges to detentions in other settings may prove unworkable and inappropriate in the enemy-combatant setting," at least when the U.S. citizen involved was captured on the battlefield abroad. n205 More extreme measures are also possible: alternatives to law enforcement reportedly under consideration in the immediate aftermath of September 11, 2001, included "shooting down a civilian airliner hijacked by terrorists; setting up military checkpoints inside an American city; employing surveillance methods more sophisticated than those available to law enforcement; or using military forces "to raid or attack dwellings where terrorists were thought to be, despite risks that third parties could be killed or injured by exchanges of fire."' n206 With September 11 now several years in the past, it may be easy once again to scoff at such possibilities. Another major attack on American soil, however, would exert enormous pressure and could easily resurrect the most extreme proposals. n207

Pro- AT: FISA Good- The Wall

Increased involvement of lawyers in the intelligence process is a positive development for civil liberties.
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

One of the main effects of the FISA wall was to keep lawyers away from intelligence investigations. With the wall up, two groups of lawyers had access to FBI intelligence investigations: OIPR, whose lawyers processed FISA applications, and the Office of the General Counsel (OGC) at the FBI. n199 Neither group was very large, neither group was dispersed in the field, where intelligence investigations take place, n200 and neither group of lawyers worked proactively with agents in conducting investigations. By and large, OIPR lawyers would learn of an investigation only in connection with preparing FISA applications as requested by the agents, and FBI-OGC lawyers would provide legal advice only as requested by the agents. This is a far cry from the cooperative model that applies in traditional criminal cases, where agents and lawyers work closely together on all aspects of an investigation. Indeed, in traditional law enforcement, no general "oversight" mechanism is needed [*527] because lawyers are intimately involved in the basic conduct of the investigations themselves.
With the wall down, dozens of prosecutors, in the Criminal Division and in U.S. Attorneys' Offices, now legally enjoy access to FBI intelligence investigations, and they increasingly work with agents, though not yet in something approaching a full cooperative model. n201 This is a positive development for civil liberties. By training and temperament, prosecutors almost always want to preserve the option of a criminal prosecution and to preserve that option they must ensure that rules are followed. As every prosecutor knows, violations can cause serious consequences when exposed through adversary testing by a defense attorney. Even in cases where litigation seems remote or impossible, most prosecutors remain fundamentally rule-bound. For this reason, civil libertarians ought to oppose the wall and encourage increased prosecutorial involvement in national security investigations.

Rebuilding the wall would be a threat to security and liberty. Even if lawyers aren't perfect, they are better than military detention, military tribunals, and Hellfire missiles!
David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

As the Court of Review concluded, however, the wall was never required as a matter of statutory or constitutional law. Nor does it advance any sound policy goal. On the contrary, rebuilding the wall would make Americans less safe from foreign threats and from possible abuses by our own security services. The wall keeps lawyers out of intelligence investigations, and whatever their other faults, lawyers tend to respect and follow the law. Moreover, it would be more than a little ironic if concerns about privacy and civil liberties were allowed to foreclose the use of civilian courts and thereby encourage the use of alternative remedies with fewer protections. A civilian prosecution - with counsel provided by the government, an Article III judge and a jury of twelve peers, the benefits of the Federal Rules of Evidence, conducted in full view of the press and public - is a far better prospect to most civil libertarians than military detention, a military tribunal, or a Hellfire missile.

Pro- AT: FISA Good- The Wall

Wall has no effect on who is under surveillance, how surveillance occurs, or what information is sought. Government would rather have information than coordination so the wall does not protect privacy. David S. Kris, Senior VP, Deputy General Counsel & Chief Ethics & Compliance Office, Time Warner, & former Assoc Deputy Attorney General for Justice Department; 2006 (Stanford Law & Policy Review; 17 Stan. L. & Pol'y Rev 487; "The rise and fall of the FISA wall")

The wall does not prevent the government from conducting any FISA search or surveillance. Its only direct impact is to restrict coordination between intelligence and law enforcement officials in the context of foreign intelligence investigations in which FISA is or may be used. The wall puts the government to a choice between eschewing internal coordination and eschewing a FISA search or surveillance. As a moment's thought would indicate, this is a Hobson's choice - the government always elects information over coordination because it would rather fight with one hand tied behind its back than blindfolded. Thus, the wall is not a fixed restriction on search or surveillance activity itself. It is, instead, a malleable requirement that the government can satisfy by keeping law enforcement officials away from intelligence investigations. Put another way, as long as intelligence officials carefully avoid [*519] contact with law enforcement officials, they may - and historically did - intrude on individuals' privacy to the same extent with the wall up as they now can with the wall down.

The wall certainly does not change who may be searched or surveilled. Today, as in 1978, FISA may be used only against foreign powers and agents of foreign powers. Those terms are defined specifically in 50 U.S.C. 1801, and the definitions do not vary according to the nature of the government's investigative purpose. As discussed in Parts I and II, supra, lowering the wall permits coordination between intelligence and law enforcement officials, but it does not allow FISA to be used against ordinary criminals under any circumstance. Corrupt corporate executives, mafia dons, street-level drug dealers, and domestic terrorists may all rest assured in the knowledge that today, as always, they are immune from searches and surveillance under FISA.

Nor does the wall change what information is sought or acquired. As discussed in Part I, even the staunchest defenders of the wall recognize that intelligence and law enforcement officials desire the same information about FISA targets and their associates. Prosecutors and intelligence officials are similarly greedy: if they suspect a target of involvement in terrorism, espionage, or some other threat to national security, they want to know everything related to that threat. Constructing a compelling case for a jury requires investigation of the same basic facts as constructing a good briefing paper for intelligence policy-makers. n171

Pro- AT: FISA Good

FISA is obsolete. Its definition of surveillance is largely not applicable to data mining and post 9/11 cell phone requirements. Miller decision proves data provide by third party has no reasonable expectation of privacy.

Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

In order to outline what seems to be a major flaw in the way FISA was drafted, it is worthwhile to begin by making what may be a self-evident observation: FISA only applies to acts of government surveillance. That is to say, a prerequisite to trigger FISA's applicability to any particular instance of government observation is that the observation must fit FISA's definition of surveillance. If it does not, FISA is not implicated and the government is free to listen as it wishes. n52 With the NSA's increased use of data-mining technology, pattern-based inquiries, and National Security Letters, FISA's definition of surveillance may be antiquated to the point that it could render the entire statute irrelevant.

The definition of surveillance, in pertinent form, is the acquisition of a communication either sent or received by a "particular, known United States person who is in the United States," if the communication was acquired by "intentionally targeting" that person, and if the circumstances are such that they have a reasonable expectation of privacy. n53 Alternatively, "surveillance" also means the acquisition of any communication to or from someone located in the United States, if the acquisition occurs within the United States. n54

It is clear from both FISA and Supreme Court precedent that an individual must have a reasonable expectation of privacy for "surveillance" to occur. In *United States v. Miller*, the Supreme Court held that individuals have no expectation of privacy in information held by a third party. n55 Through the use of National Security Letters, the FBI and the NSA routinely exploit this rule of law to acquire vast amounts of personal information on U.S. citizens from private corporations, such as phone companies and Internet service providers. n56 Because FISA's definition of surveillance fails to account for this practice, the government is not required to get a warrant or make any certification of probable cause. Considering how much the technological capacity of the private sector for gathering and retaining personal information has increased in recent years, the privacy implications of government access to this data are huge.

[*434] Recent "E-911" legislation, which requires all new cell phones in the U.S. to be fitted with devices that continuously transmit the phone's location, is an apt example. n57 In the wake of this law, those who regularly carry a cell phone now leave a digital trace everywhere they travel within a matter of feet. If cellular carriers were to share their customer's data with the NSA, CIA, or FBI, as has been widely alleged, those agencies could easily tell not only to whom those customers talk, but with whom they spend their time (assuming they have a cell phone as well), where they spend their time, how long they are there, etc. All of this can potentially be accomplished without doing any actual "surveillance."

Pro- AT: FISA Good

FISA's outdated definitions create loopholes that allow NSA domestic surveillance.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

Apart from the issue of private corporations gathering and sharing intelligence, FISA's surveillance definition is antiquated due to the distinction it makes between data acquired inside or outside of the U.S. Again, government observation only qualifies as surveillance if the data is acquired inside the U.S. or if one or more of the parties is a known U.S. person, inside the U.S., who the government is targeting intentionally. In other words, unrestrained and indiscriminate eavesdropping by the NSA is allowed under FISA as long as the communication is not physically intercepted within the U.S., and the target is either: (1) someone known to be a non-U.S. person, (2) someone who is intentionally targeted but whose identity is unknown, or (3) anyone else in the world who is not intentionally being targeted.

Today, the requirement that the interception of electronic communications takes place outside U.S. borders is hardly an obstacle to intelligence agencies. The proliferation of the Internet and other global communication networks has made physical distance and political borders a nonfactor in the realm of communications. To increase efficiency, Internet traffic is often routed through the least congested server regardless of the server's physical location. n58 For instance, two neighbors in Nebraska chatting on an instant messenger program might have their communications routed through servers in Hong Kong and back, despite being only 30 feet apart.

The third caveat discussed above, the predicate requirement that an individual be intentionally targeted in order to satisfy the definition of surveillance, is likely to be the NSA's most useful loophole in the FISA statute. As computing power has increased over the past 25 years, the U.S. intelligence community has become capable of capturing and analyzing huge amounts of data, beginning with no particular target of surveillance. These "pattern based" searches rely on sophisticated models of criminal [*435] behavior with which to compare the captured data. n59

Pro- AT: NSA Monitors All Electronic Communication

NSA reads less than one part of a million of Internet data.
National Security Agency; August 9, 2013 ("The National Security Agency: Missions, Authorities, Oversight, and Partnerships"; http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf)

According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that. However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA part in a million. Put another way, if a standard basketball court represented the global collection would be represented by an area smaller than a dime on that basketball court.

Pro- AT: Privacy

Foreign intelligence sharing makes privacy violations inevitable.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

The Echelon Interception System has been described as an effort to do away with formal borders in the intelligence community. n106 If FISA and the Fourth Amendment are to provide meaningful protection to Americans in this new community, their application (to the extent possible) must also become global. To that end, the government's practice of accepting and utilizing intelligence provided by foreign agencies against Americans must be subject to the common law exclusionary rule. When the government accepts the surveillance product of foreign intelligence agencies, regardless of whether the Fourth Amendment is implicated, it is tacitly (if not overtly) encouraging a foreign government to violate the privacy rights of Americans. In the context of Echelon and the UKUSA intelligence sharing pact, the failure to apply the exclusionary rule to shared evidence is tantamount to recognizing a conceptual right to privacy, but in reality withholding the freedom and enjoyment it provides.

Electronic surveillance can't violate privacy
Richard Posner, U.S. 7th Circuit Court Appeals & Senior Lecturer Law @ Univ Chicago; December 21, 2005 (Washington Post; "Our domestic intelligence crisis"; http://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html)

These programs are criticized as grave threats to civil liberties. They are not. Their significance is in flagging the existence of gaps in our defenses against terrorism. The Defense Department is rushing to fill those gaps, though there may be better ways.
The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer.

Pro- AT: Surveillance Bad

Surveillance has positive benefits.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

So far so bad. Or maybe not. Putting the oppression of totalitarian states to one side, public and private surveillance can have beneficial effects. All other things being equal, greater security from crime and terrorism is a good thing. n61 So too are the conveniences of modern communications, email, and the power of a search engine in our pockets valuable advances that improve our quality of life. And a sensible system of automated traffic regulation can save money and direct scarce police resources to serious criminals rather than ordinary motorists.

Pro- AT: Totalitarianism

NSA does not compile files on every individual. They are not comparable to the East Germans.
Joel Brenner, former NSA inspector general; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

JOEL BRENNER: This the program only involves telephony metadata, not e-mails, not geographic location information. The idea that NSA is keeping files on Americans, as a general rule, just isn't true. There's no basis for believing that. The idea that NSA is compiling dossiers on people the way J. Edgar Hoover did in the '40s and '50s or the way the East German police did, as some people allege, that's just not true.

Not analogous to 1984.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

As a society, we are thus of two minds about surveillance. On the one hand, it is creepy, Orwellian, and corrosive of civil liberties. On the other hand, it keeps us and our children safe. It makes our lives more convenient and gives us the benefit of a putatively free Internet. Moreover, some influential thinkers argue that data surveillance does not affect privacy at all. As Judge Posner puts it:

The collection, mainly through electronic means, of vast amounts of personal data is said to invade privacy. But machine collection and processing of data cannot, as such, invade privacy. Because of their volume, the data are first sifted by computers, which search for names, addresses, phone numbers, etc., that may have intelligence value. This initial [*1945] sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer. n62 Surveillance is thus confusing. We like its benefits, though we are fearful (and sometimes dismissive) of its costs. This confusion points to a larger problem: civil liberties advocates lack a compelling account of when and why (if at all) surveillance is harmful. As a society, we have an intuitive understanding that public- and private-sector surveillance is potentially bad, but we do not have an articulate explanation of why it is bad. Some of our intuitions stem from literature, such as George Orwell's chilling portrait of Big Brother in Nineteen Eighty-Four. n63 But few critics of government surveillance such as the NSA wiretapping program and the British data-retention regulations would suggest that these programs are directly analogous to the evil regime depicted in Orwell's dystopia. Moreover, the Orwell metaphor seems wholly inapplicable to databases used to personalize targeted advertising on the web, the efforts of insurance companies to promote safe driving, and the practices of online booksellers to sell more books by monitoring consumers' shopping habits in ways that used to be impossible. n64

Con- 1st Amendment

Domestic electronic surveillance threatens the infrastructure of free expression, the 1st Amendment, and democratic government.

Jack M. Balkin, Knight Prof Constitutional Law & 1st Amendment @ Yale; Fall 2012 (Hofstra Law Review; 41 Hofstra L. Rev. 1; "The First Amendment is an information policy")

Right now there is enormous pressure in the United States to build back doors to allow surveillance on Internet networks and digital platforms in the United States, and to implement technologies that will make it easy for governments and corporations to filter content and block access to disfavored content. n83

[*29] The pressure on the United States to do these things is not coming from authoritarian strongmen in the Middle East. It is not coming from the People's Republic of China. It is coming from our government and from the content industry. The government is worried about potential criminal activities and terrorist networks that use Skype, Facebook, and Gmail. The content industry is worried about file sharing and intellectual property. Meanwhile, telecommunications and broadband companies, which oppose some of these proposals, have their own shopping list: they want to protect the right to block and filter traffic that interferes with their business models or to favor traffic by their business partners. That is why the industry vigorously opposes network neutrality.

The danger in these proposals is that, however well-intentioned, they may also threaten the American infrastructure of free expression. Building networks that allow you to filter for intellectual property also allows you to filter for anticompetitive reasons, or even for ideological reasons. Implementing broadband technologies to slow and block traffic that your business partners do not like allows slowing and blocking traffic for other reasons as well.

Moreover, building a back door into everyday online communications means building a surveillance system into every aspect of our lives that uses digital communications systems, ranging from e-mail to Facebook to gaming software to Google Docs. If the government required that building contractors install bugs and hidden cameras in every home or apartment, people would object strenuously even if the government assured them that the bugs and cameras would only be turned on when the government had very good reasons.

Building a backdoor greatly lowers the costs of routine surveillance. In the pre-digital world the government had to decide whether the cost of a wiretap or a surveillance stakeout was worth the manpower and the expense. When government builds surveillance into digital communications systems, the cost of surveillance, including unnecessary surveillance, declines rapidly, so it is reasonable to expect that there will be more of it. And if there will be more of it, it is imperative to design systems to help ensure that surveillance is not abused.

The same is true of proposals to require that broadband providers install filtering systems or deep packet inspection systems to look for contraband intellectual property. Once these facilities are built into a [*30] system, they greatly reduce the costs of blocking, filtering, and censoring. Designing an infrastructure in this way shifts the cost of surveillance and censorship away from government and onto citizens.

The First Amendment is an information policy for democracy, but it is only one information policy among many. It needs the assistance of an infrastructure of free expression to make good on its promises. The fight over free speech today, around the world, is a fight over how that infrastructure will be designed and implemented. If we want to preserve a free Internet, we must have networks that cannot easily be abused in the future. We must design democratic values into the infrastructure of free expression if we want an infrastructure that protects democracy.

Con- 1st Amendment

Chilling effect on 1st Amendment

Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

Intellectual-privacy theory explains why we should extend chilling-effect protections to intellectual surveillance, especially traditional-style surveillance by the state. If we care about the development of eccentric individuality and freedom of thought as First Amendment values, then we should be especially wary of surveillance of activities through which those aspects of the self are constructed. n90 Professor Timothy Macklem argues that "the isolating shield of privacy enables people to develop and exchange ideas, or to foster and share activities, that the presence or even awareness of other people might stifle. For better and for worse, then, privacy is sponsor and guardian to the creative and the subversive." n91 A meaningful measure of intellectual privacy should be erected to shield these activities from the normalizing gaze of surveillance. This shield should be justified on the basis of our cultural intuitions and empirical insights about the normalizing effects of surveillance. But it must also be tempered by the chilling-effect doctrine's normative commitment to err on the side of First Amendment values even if proof is imperfect.

Con- 4th Amendment

NSA domestic surveillance violates the 4th Amendment.
Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

Like me, he became discomforted by what he was exposed to and what he saw: the industrial-scale systematic surveillance that is scooping up vast amounts of information not only around the world but in the United States, in direct violation of the fourth amendment of the US constitution.
The NSA programs that Snowden has revealed are nothing new: they date back to the days and weeks after 9/11. I had direct exposure to similar programs, such as Stellar Wind, in 2001. In the first week of October, I had an extraordinary conversation with NSA's lead attorney. When I pressed hard about the unconstitutionality of Stellar Wind, he said: "The White House has approved the program; it's all legal. NSA is the executive agent."
It was made clear to me that the original intent of government was to gain access to all the information it could without regard for constitutional safeguards. "You don't understand," I was told. "We just need the data."

Con- 4th Amendment- AT: Computers can't search

Data mining is an unreasonable search.

Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

Some commentators believe that a computer cannot perform a "search" within the meaning of the Fourth Amendment. n132 Judge Richard Posner, for example, has stated that "processing of data cannot ... invade privacy. . . . This initial sifting, far from invading privacy (a computer is not a sentient being), keeps most private data from being read by any intelligence officer." n133 Another leading Fourth Amendment scholar has advocated the "exposure-based approach," in which data is not search until it "is exposed to human observation." n134

[*458] No perfect datamining program exists, and thus human eyes will eventually view the data, resulting in a search that implicates the Fourth Amendment. n135 Additionally, in the binary world, the NSA could possibly perform a significant number of searches n136 in what would take the police a lifetime to perform in the physical world. Moreover, unlike the physical world, where any search conducted would require probable cause, n137 the binary world has no judicial oversight or statutory procedures to follow n138 and consequently there is a greater chance for abuse of power. n139 Further, unlike in the physical world, the person in the binary world would have no notice n140 that a search was even performed. n141 Because there is no notice, a person could not deter the government through voting or political pressure or even "regulate their behaviour to avoid unwanted intrusions." n142 Thus, datamining should be considered a search and be examined for reasonableness by balancing the government and private interests. n143 Mining a database so large lacks reasonableness [*459] because it is inefficient, that is, many false positives are going to occur, resulting in innocent people being jailed or suffering reputational harm. n144

Con- 4th Amendment- AT: Incidentally obtained

The exception of incidentally obtained information risks becoming the rule when NSA surveillance systems can monitor all global communications.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

Although the concept of using incidentally acquired information is not intuitively problematic, the sheer enormity of Echelon's surveillance capacity means the exception could potentially swallow the entire rule. A system that is essentially capable of intercepting every communication in the world could conceivably allow the government to thereby "incidentally acquire" all of those communications. If and when the government attains such a capability, FISA and the Fourth Amendment will be circumvented, and Americans will no longer have any statutory or constitutional protection of their privacy in the sphere of foreign intelligence surveillance.

Con- 4th Amendment- AT: Materials/Tangible things

4th Amendment covers conversations not just materials and tangible things.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The Fourth Amendment of the United States Constitution, and the common law jurisprudence interpreting it, provide the current body of law regulating domestic search and seizure, including domestic electronic surveillance. The Fourth Amendment protects Americans from unreasonable searches and seizures by requiring probable cause and particularity for a search warrant (which then makes the search reasonable), and requiring a search warrant except in exceptional circumstances. n72 [*182] Though Fourth Amendment jurisprudence originally applied only to tangible things, the Supreme Court eventually extended the Fourth Amendment's reach to include conversations; and the Court continued this expansion as technology advanced. n73 In Katz v. United States, the Supreme Court held "for the first time that the protections of the Fourth Amendment extend to circumstances involving electronic surveillance of oral communications without physical intrusion." n74 Katz was groundbreaking because it overruled an earlier case, Olmstead v. United States, which held that the Fourth Amendment did not apply to wiretapping phone conversations because words were intangible, and, therefore, no search and/or seizure had occurred. n75 Because Katz established that the Fourth Amendment applies to electronic surveillance activities, and the Protect America Act permits warrantless domestic surveillance through electronic communication, the Act implicates the Fourth Amendment.

Con- 4th Amendment- AT: National Security Exception

National security exception to 4th amendment does not apply to domestic surveillance of U.S. citizens- probable cause and a warrant are required.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

[*516] The rights protected by the Fourth Amendment are subject to some important limitations. For example, since World War II, U.S. presidents have asserted that the executive branch has the power to order warrantless electronic surveillance when national security is at stake. n64 This exception has become known as the national security exception to the Fourth Amendment. n65 Although the exception is not specifically enumerated in the Constitution, caselaw has recognized a limited set of circumstances under which the President's power to control foreign affairs may allow warrantless searches to be ordered to effectuate that purpose. n66 Courts have, however, allowed the exception to be invoked only in a limited set of situations, all of which have involved some form of foreign security effort. n67 Moreover, the Supreme Court has specifically refused to recognize the national security exception in cases involving domestic surveillance operations targeting American citizens within U.S. borders. n68 For instance, in 1972, in *United States v. U.S. District Court (Keith)*, the Supreme Court held that the President's power to protect national security did not eliminate the need for the Central Intelligence Agency to obtain a warrant before conducting electronic surveillance of suspected terrorists within the territorial boundaries of the United States. n69 This holding proved [*517] problematic for U.S. intelligence agencies, which feared that seeking a warrant through traditional avenues would require divulging secret information about agency methods and ongoing operations. n70 The *Keith* Court had, however, specifically refused to address the issue of whether the agency was required to obtain a traditional warrant in matters involving foreign powers or agents, n71 which left room for Congress to step in and create an alternative means of satisfying the warrant requirement while also protecting classified information. n72

Con- 4th Amendment- AT: National Security Exception

US Supreme Court decision known as Keith proves executive cannot override warrant requirement because of national security.

Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

Five years after Katz, the Supreme Court addressed electronic surveillance for domestic intelligence purposes in United States v. United States District Court (known as Keith). n76 The Court extended Katz's holding when it found that "the President violated the Fourth Amendment by authorizing warrantless wiretaps in national security cases." n77 Boston University School of Law Professor Tracey Maclin notes:

Powell's reasoning [in Keith] was succinct and categorical: The warrant requirement applied to national security wiretaps and there was no basis for exempting the President from the requirement. There was no nuance and no room for manipulation by the government. n78

Additionally, Keith made clear that the warrant requirement applies even when the Executive believes national security is at risk. n79 The court recognized the President's constitutional duty to protect national security with the caveat that "it must be exercised in a manner compatible with the Fourth Amendment." n80 Thus, while the Keith decision did not express a view on "the scope of the President's surveillance power with respect to the activities of foreign powers, within or without the country," n81 it firmly established that warrantless domestic surveillance is constitutionally impermissible even in the name of national [*183] security. n82

Con- 4th Amendment- AT: Places not people

4th Amendment covers people not places. The Protect America Act violates the 4th Amendment even if the call is overseas or about a foreigner.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The critical point is that in Fourth Amendment jurisprudence the person being searched triggers the Fourth Amendment constitutional violation, not the place or content of the search. n131 Applied in this context, when the government monitors George and Sally's communications without a warrant or probable cause, their rights are violated. However, Jean's rights are not violated because she is merely the subject of George and Sally's communication. Although the government may seek information about Jean (the target of the surveillance), it is Sally's and George's constitutional rights that the government compromises. The end result is that the government violates the rights of the people whose communications it monitors, not the subject of the surveillance who is reasonably believed to be outside of the United States (and who could be a foreign national or a Untied States citizen). Thus, under the Protect America Act, in permitting surveillance of an American's communication about a foreign national, the government violates the American person's rights, not the foreign national's rights.
Another potential violation of Americans' rights arises because the Protect America Act does not provide language limiting permissible sources of information. n132 The Act includes language which limits communication collection specifically to communications about people outside of the United States, n133 but because the Act does not specify permissible or impermissible sources for that information, n134 the collection is virtually limitless; the source could be an American located within the United States. While the Act contains some limiting language, n135 it does not confine intelligence collection to information obtained from non-United States citizens n136 or from persons reasonably believed to be outside the United States; n137 the Act's sole limitation is to the subject of [*191] the collection. n138 By its silence, the Act permits warrantless, domestic spying, which is similar to the type of acquisition (intelligence gathering) regulated and prohibited by FISA's electronic surveillance definition. n139 The Protect America Act, however, lacks FISA protections strictly limiting such acquisitions. n140 Finally, the phrase "notwithstanding any other law," which begins Protect America Act section 2, asserts the Act's supremacy over other laws which may have otherwise limited it. n141

4th Amendment covers people not places. A conversation should not lose protection once it is transmitted beyond the U.S. borders.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

Professor Kerr states that "the Fourth Amendment is not a roving privacy machine," but in many ways, it is. n220 The Supreme Court has long held that "the Fourth Amendment protects people, not places." n221 This protection travels with a person wherever he or she goes, and it covers all situations where a legitimate expectation of privacy can be held. n222 The Supreme Court has made it clear that it is the reasonableness of a person's expectation of privacy, not the geographic location of the conversation in question, that determines whether or not a conversation is protected. n223 American citizens do not lose their Fourth Amendment rights simply because they set foot outside the United States; likewise, their conversations do not become fair game once the electrons transmitting them pass beyond U.S. borders. n224

Con- 4th Amendment- Data Mining- AT: Miller

Exceptions to Miller exist- inadvertent disclosure or particularly private data, as well as specific refusal to disclose information to the government create a reasonable expectation of privacy.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

Ferguson and Randolph signal that the Court is willing to consider at least minor exceptions to Miller's dictate that the government does not effect a constitutionally regulated search when it accesses information the subject shared with a third party. If information is disclosed inadvertently or is particularly private (as with medical data), or if we specifically refuse to disclose it to the government, perhaps a reasonable expectation of privacy attaches. Should these exceptions be strengthened? Should they be broadened? If so, what form might they take?

Con- 4th Amendment- PATRIOT Act

ACLU argues the PATRIOT Act compromises the 4th Amendment in a number of ways: 1) probable cause 2) judicial oversight 3) domestic surveillance 4) detention and deportation.
Robert N. Davis, Prof Law @ Stetson Univ, member of ABA Standing Committee on Law & National Security, & active U.S. Navy Reserve; 2003 (Brooklyn Journal of International Law; 29 Brooklyn J. Int'l L. 175; "Striking the balance: national security vs. civil liberties")

In its review of the USA Patriot Act, the ACLU criticized the Act as compromising Fourth Amendment protections. The ACLU argued that the Act eviscerated the probable cause requirement of the Fourth Amendment, n389 limited judicial oversight of telephone and internet surveillance, n390 put the CIA back in the business of spying on Americans, n391 and allowed for detention and deportation of people engaging in innocent associational activity. n392
The ACLU argues that the USA Patriot Act limits judicial oversight of electronic surveillance by changing current law. n393 The ACLU contends that the low hurdle required to get telephone numbers traced during an ongoing criminal investigation is now imported, through the USA Patriot Act, to internet communications which involve more content than just telephone numbers alone. n394 Under current law, in order to obtain a pen register or trap and trace order, a law enforcement officer need only certify that the information sought is "relevant to an ongoing criminal investigation." n395 The order requires a "telephone [*231] company to reveal the 'numbers dialed' to and from a particular telephone." n396 Under Section 216 of the USA Patriot Act, the judge has no discretion and "must grant the order upon receiving the certification." n397 "Section 216 of the USA Patriot Act...extend[s] this low threshold of proof to internet communications..." n398 These communications reveal more content than simply the numbers dialed to or from a telephone. n399 Unlike with telephone calls, the email address cannot always be easily separated from the content of the message. n400
The ACLU also criticizes the USA Patriot Act for putting the CIA back in the business of spying on American citizens. n401 This concern is based on the fact that the FBI, CIA and NSA spied on student activists and others who opposed the war in Vietnam during the 1960s and 1970s. n402 FISA was passed in response to this abuse of power. n403 The USA Patriot Act "permits wide sharing of sensitive information gathered in criminal investigations by law enforcement agencies with intelligence agencies including the CIA, and the NSA, and other federal agencies including the INS, Secret Service and Department of Defense." n404 The ACLU fears that the USA Patriot Act gives the government a dangerously enhanced role in domestic intelligence gathering against U.S citizens, n405 a role that is "contrary to the statutory prohibition in the CIA charter barring it from engaging" in domestic security operations." n406

Con- 4th Amendment- Protect America Act

Protect America Act violates 4th Amendment: 1) probable cause for warrant 2) particularly clause 3) primary purpose does not have to be related to terrorism or national security 4) information used in other legal contexts

Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

Under the Protect America Act, U.S. intelligence agencies do not need a warrant, probable cause, or even a description of when or from whom they will collect information in order to conduct surveillance. n150 Each of these elements contrasts with the protections contained in FISA. First, the Act permits search and seizure without a warrant. n151 FISA, in contrast, "was an acknowledgement by Congress that the Fourth Amendment required prior judicial approval before the communications of Americans within the country could be monitored ... [*193] for foreign intelligence purposes." n152 FISA was rooted in Katz and Keith. n153 In Keith, the Court held that "the President violated the Fourth Amendment by authorizing warrantless wiretaps in national security cases." n154 In that case, "no justice voted to uphold the government's claim that warrantless wiretaps in national security cases were reasonable under the Fourth Amendment." n155 Thus, even before FISA, the Supreme Court upheld the proposition that domestic wiretaps, even to promote national security, were unconstitutional without a warrant. FISA codified these sentiments by requiring third party approval of domestic surveillance by the FISA court. n156 The Protect America Act requires neither a warrant nor probable cause to conduct its surveillance activities. n157 The only standard the Act requires is "reasonable belief" that the person about whom the communication is collected is not in the United States, a lower standard than probable cause. n158 Probable cause is the historic and constitutionally sanctioned standard for government intrusions which implicate the Fourth Amendment, including those intrusions permitted by the Protect America Act. n159

Second, the Protect America Act does not require intelligence agencies to describe the person, location, and/or information they seek, as required by the Fourth Amendment's particularity clause. n160 The particularity requirement for domestic surveillance is a cornerstone of Fourth Amendment jurisprudence. Under the Act, however, certification of these activities by the Director of National intelligence "is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence will be directed." n161

Third, even if domestic wiretapping for foreign intelligence were constitutional under the special needs doctrine, n162 the primary purpose of Protect [*194] America Act surveillance does not need to be foreign intelligence collection to be permissible under the statute. n163 The Act states only that "a significant purpose of the acquisition [must be] to obtain foreign intelligence information." n164 Thus, although the Act's asserted purpose was to further national security goals, that does need to be the primary or only impetus for collecting intelligence under the Act. n165 Conducting warrantless, domestic, surveillance activities for purposes other than discovering terrorist activities is therefore also permissible under the Act. n166

Fourth, the Protect America Act leaves open the question of whether information gathered through its procedures could be used in other legal contexts. If potentially incriminating evidence were discovered during a Protect America Act collection, that information could potentially be used in an unrelated investigation. For example, if, while authorities listened to Sally and George's conversation, Sally mentioned she just robbed a bank or accepted delivery of 2 kilos of cocaine, it is possible that Sally's statement could be used against her in an ordinary civil or criminal proceeding. The Act's alleged purpose is to provide additional procedures to acquire foreign intelligence, n167 but its permissions are broader; it could potentially lead to the collection and use of information with no bearing on terrorism or national security. This question has yet to be answered; however the assumption remains that laws are constitutional until a court rules otherwise. Therefore, unless a court rules otherwise, it appears that any information acquired under the Protect America Act could be used in other legal contexts.

Con- 4th Amendment- Protect America Act

Protect America Act authorizes unconstitutional warrantless surveillance.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The powers granted by the Protect America Act are inconsistent with FISA, despite the fact that the Act is codified within FISA. The Protect America Act provides fewer protections for Americans, greater discretion for the intelligence community, and fewer objective evaluations of government intelligence acquisition than does FISA. All of these distinctions render the Protect America Act constitutionally suspect. The issue is not whether information gathered under the Act is useful or whether the government finds incriminating information using these procedures. A constitutional violation occurs regardless of what the government does or does not find in exercising its Protect America Act powers. A Fourth Amendment violation occurs at the moment of unwarranted intrusion. Thus, the critical question is whether the Protect America Act violates Americans' constitutional rights by permitting unreasonable, warrantless surveillance of Americans.

The Protect America Act exists outside of FISA and expands executive power for warrantless domestic surveillance.
Emily Arthur Cardy; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

As Public Law 110-55, the Protect America Act is codified within and amends FISA section 105. n70 Although being a part of FISA could seem to lend legitimacy to the Act, it does not, because FISA's safeguards do not extend to the Act. n71 The Protect America Act explicitly situates its provisions outside of FISA and outside of FISC's purview. While hailed as a success in forcing the Administration to codify and bring the TSP into FISA, the Protect America Act actually provides broader executive power than the original TSP, and places the program substantially outside of the United States' legal standard governing intelligence collection. The provisions in the Protect America Act permit activities in contravention of Fourth Amendment jurisprudence.

Use of concerning instead of from allows warrantless domestic surveillance.
Emily Arthur Cardy; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

With one word, the Protect America Act immediately implicates the Fourth Amendment. Section 2's meaning turns on Section 2(a)'s use of the word "concerning," which broadens the class of people at whom this surveillance activity can be directed. The relevant part of Section 2(a) reads:

Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States n123

Although the Act purports to close a loophole in foreign surveillance powers, this clause permits the United States' intelligence agencies to reach far beyond that purpose. n124 The statute's text permits the government to listen to conversations and collect emails between and among people who are in the United States, including United States citizens, without a warrant, provided that the communication is about a person "reasonably believed to be outside the country." n125 The section does not require the foreign target to be a party to the conversation being collected; the conversation need only be about that person and the sources may be American citizens inside the United States. n126 The Act accomplishes this by using the word "concerning" instead of "from." n127

Con- 4th Amendment- Protect America Act- AT: Amendments/Revisions

Revisions do not provide remedies for rights violations already committed.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The Protect America Act of 2007 expired on February 1, 2008. Congress and the President extended the Act for six months, and on July 9, 2008 President Bush signed into law new amendments to FISA. n174 The permanent FISA amendments include different and potentially less constitutionally suspect language than does the Protect America Act. n175 Although the new language appears to be less constitutionally suspect, these new amendments provide immunity to companies which aid the government in collections procedures. n176 Once again, United States citizens are left without a remedy for constitutional violations. Additionally, these amendments do nothing to remedy Fourth Amendment violations which potentially occurred between August 5, 2007, and February 1, 2008. Nor does amending the Act reveal how many Americans' conversations and/or emails were warrantlessly searched and seized by the government. Thus, this Act's history and implications remain important.

FAA revisions keep reasonable suspicion and significant purpose language in tact.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

FAA amends FISA to permit "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." n47 The person targeted must not be a United States person. The critical substantive requirements are (1) the "target" of the surveillance is located overseas, and (2) a "significant purpose" of the surveillance must be to acquire foreign intelligence information. n48 The collection of the information must be carried out pursuant to certain "targeting procedures" that ensure that the collection is targeted at persons located outside the United States. n49 The acquisition must also involve new minimization procedures, which the attorney general is to adopt. n50 The FAA's requirement of minimization is not a new one for FISA. As the leading FISA treatise explains, the idea of minimization generally is that electronic surveillance pursuant to FISA be implemented to ensure conformity to its "authorized purpose and scope" and in a fashion that requires the government to collect the least amount of "irrelevant [*416] information." n51 The attorney general's minimization procedures under the FAA, regarding the targeting of persons outside the United States, must comply with FISA's existing requirements. It should be noted, moreover, that these requirements contain a significant possible escape valve. FISA states that minimization must be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." n52 Finally, in advance of surveillance activity, the FAA also requires the DOJ and the Director of National Intelligence to certify that targeting and minimization procedures meet the statutory standards and that "a significant purpose" of the surveillance is to acquire foreign intelligence information. n53

Con- 4th Amendment- Protect America Act- AT: Not electronic surveillance

Sly semantics meant to avoid constitutional questions should not circumnavigate the 4th Amendment. Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

The Protect America Act implicates the Fourth Amendment because it permits domestic, warrantless surveillance. Supporters of the Act argue that Fourth Amendment electronic surveillance jurisprudence is irrelevant to the Act's application because the Act defined the activities it sanctions as not being [*189] electronic surveillance within the meaning of FISA, thus removing its activities from FISA's strictures. Such use of sly semantics should not circumnavigate the Fourth Amendment.

Con- Accountability

Public private intelligence partnerships prevent accountability.
Jon D. Michaels, Prof Law @ UCLA; August 2008 (California Law Review; 96 Calif. L. Rev. 901; "All the president's spies: Private-public intelligence partnerships in the War on Terror")

Transcending these particular concerns are questions of national security accountability n10 - how "privatization," in the guise of informal intelligence agreements with corporations, can help the Executive direct broad swaths of intelligence policy without having to seek ex ante authorization or submit to meaningful oversight. This evasion leaves Congress and the courts ill-equipped to weigh in on important policy considerations regarding the proper scope and calibration of counterterrorism and homeland security operations, not to mention ill-equipped to intervene to remedy individual instances or patterns of injustice. Whether intentional or not, working around the legislative and judicial branches through shadowy collaborations is especially troubling given that many of today's surveillance programs rely on brand-new technologies and cut more broadly and deeply into the domestic fabric than ever before. Thus, [*905] the need for careful consideration by the full range of government actors, especially those further removed from the immediate responsibility of hunting terrorists, is particularly acute. Greater scrutiny is essential both to ensure fidelity to existing laws and to determine whether new, informal surveillance and data-mining practices operating in the interstices of the extant legal framework warrant legislative or administrative responses to fill in those regulatory gaps. In other words, with respect to initiatives that are not currently regulated (and not readily observable), these lawmakers, regulators, and judges need accurate information to determine whether, normatively speaking, the unregulated terrain is in fact underregulated. n11

Congressional oversight of electronic surveillance is a privacy theater- more show than substance.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

As promising as these opportunities are for congressional involvement, it is necessary to note a poor past track record for this branch of government in carrying out oversight in a far simpler and less controversial area of telecommunications surveillance. As I have discussed elsewhere, Congress has manifested a notable lack of interest in obtaining pen register reports from the Department of Justice as required by statute. n107 Pen registers are devices that record not the content of telephone conversations, but the telephone numbers of outgoing and incoming calls. The Patriot Act of 2001 amended the Pen Register Act to more broadly include "dialing, routing, addressing, or signaling information" ("DRAS information") in its definition of data that fall under the [*428] statute. n108 IP addresses and email addressing data ("to" and "from" lines on email and routing) are an example of DRAS information. n109
The lack of pen register reports leads to a significant gap in knowledge about law enforcement use of its authorities under the Pen Register Act, an essential part of the framework for domestic electronic surveillance in the United States. More broadly, much of the past congressional oversight of telecommunications surveillance law has represented a kind of "privacy theater." n110 By this term, I mean that the law creates rituals of behavior, such as a formal requirement that pen register reports be sent to Congress, and the payoff is the creation of a myth of oversight. It is likely, moreover, to be far more difficult for Congress to engage in effective engagement with executive branch behavior in the foreign intelligence area. There is also a real risk that the FAA's oversight requirements will simply contribute to a new kind of privacy theater and bolster the old, reassuring myth that if excesses exist, Congress will respond by enacting reforms.

Con- Data Mining

NSA conducts data mining and plans on storing Yottabytes of data.
Cindy Cohn, Legal Director Electronic Frontier Foundation; Spring 2010 (Journal on Telecommunications and High Technology Law; 8 J. on Telecomm. & High Tech. L. 351; "Privacy and law enforcement: Lawless surveillance, warrantless rationales")

While the exact details are unknown, credible evidence indicates that billions of everyday communications of ordinary Americans are swept up by government computers and run through data-mining or other technical processes, likely culminating in human review of computer-selected communications. n7 That means that even the most personal and private of our electronic communications - between doctors and patients, between husbands and wives, or between children and parents - are subject to review by computer algorithms programmed by government bureaucrats, with some unknown portion reviewed by the bureaucrats themselves.
[*353] The scale of the surveillance seems overwhelming, almost impossible. Yet the NSA apparently thinks it can do it. The agency is building a million square foot data storage facility at a cost of $ 2 billion in Utah and another large facility in San Antonio. n8 Noted author and NSA-watcher James Bamford notes that the NSA is planning to have gathered Yottabytes of data, or 1,000,000,000,000,000,000,000,000 pages of text, by 2015. n9 According to Bamford, the new facilities in Utah and Texas will be used "to house trillions of phone calls, email messages and data trails: Web searches, parking receipts, bookstore visits, and other digital "pocket litter."' n10 This massive collection continues despite increasing indications that such data mining is "not well suited to the terrorist discovery problem." n11

Three constitutional implications from data mining: 1) Due Process Clause 2) 1st Amendment protection of speech and association 3) 4th Amendment prohibition of unreasonable searches.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

Data mining possibly implicates at least three constitutional provisions: the Due Process Clause's guarantee of fair process, the First Amendment's protection of speech and association, and the Fourth Amendment's prohibition on unreasonable searches. n49 The Due Process Clause might require that government make a good faith effort to secure its databases n50 and that it provide some sort of procedure for challenging erroneous inclusion on no-fly lists and other databases used in match-driven surveillance when such surveillance results in deprivations of liberty or property. n51 The First Amendment's application to data mining is more complicated. It has been argued, on the one hand, that commercial data brokers' speech rights are infringed by rules inhibiting disclosure of the information they acquire n52 and, on the other, that the First Amendment provides special protection for any personal information that evidences one's political views or associations. n53 [*329] I will not enter this debate here, because I think Fourth Amendment analysis subsumes it. n54 It is to that analysis that I now turn.

Data mining leads to profiling and mission creep.
Christopher Slobogin; Winter 2008 (75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

The use of algorithms that produce a high false positive rate exacerbates two other phenomena: invidious profiling and what data mining aficionados call "mission creep." Match- and event-driven data mining can be, and probably have been, heavily dependent on ethnic, religious, and political profiling; n39 while such discrimination is a possibility during traditional investigations as well, it is vastly facilitated by [*326] computers. And match- or event-driven data mining designed to ferret out terrorists can easily transform into a campaign to grab illegal immigrants, deadbeat dads, and welfare scammers. The CAPPS II program, for instance, appears to have been used to identify any individual who is in the country illegally. n40 The terrorist watchlist has now grown to over one-half million subjects, suggesting a very broad definition of terrorism. n41 These are not necessarily unmitigated harms, of course, but they should be recognized as a likely byproduct of data mining operations.

Con- Data Mining

Potential individual profiles from data mining create a chilling effect on behavior.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

All of these concerns can add up to a sense of unease about data mining. For those innocent people who are kept off airplanes, interviewed, or arrested based on erroneous data, or who lose their identities because of government sloppiness, the unease is palpable. For the rest of us, the harm is admittedly not as obvious. Many of those whose records are accessed through data mining don't know it is happening, [*327] and if nothing incriminating is found, may never find out. But we still know that data mining allows the government to accumulate and analyze vast amounts of information about us, sufficient perhaps to create what some have called personality or psychological "mosaics" of its subjects. n44 That capacity for data aggregation may be a cost in itself. As Daniel Solove has argued, one result of government's entry into the information age is that faceless bureaucrats will be able to compile dossiers on anyone and everyone, for any reason or for no reason at all. n45 The possibility, even if slim, that this information could somehow be used to our detriment or simply revealed to others can create a chilling effect on all activity. It may have been some vague sense of this possibility that led Congress, however ineffectually, to declare its opposition to the concept of Total Information Awareness, with its epithet "knowledge is power."

Data mining leads to misinformation and false positives.
Christopher Slobogin , Prof Law @ Univ Florida; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 317; "Surveillance: Government data mining and the Fourth Amendment")

The costs of data mining can be significant as well. A first, obvious cost is that data mining might lead to the wrong people being arrested, kept off airplanes, or subject to further investigation. Unfortunately, those occurrences are routine, for numerous reasons.
Most fundamentally, the information in the records accessed through data mining can be inaccurate. The government's no-fly list, for instance, is notorious for including people who should not be blacklisted. n32 Even more prosaic records are astonishingly inaccurate. Approximately one in four credit reports contain errors serious enough to result in a denial of credit, employment, or housing. n33 According to one study, 54 percent of the reports contain personal demographic information that is misspelled, long outdated, belongs to a stranger, or is otherwise incorrect. n34 Even if the information is accurate, [*325] integrating disparate databases may lead to distortions in the information obtained, and computers or analysts can misconstrue it. n35
With event-driven data mining, inaccuracy is heightened by the difficulty of producing useful algorithms. Even when the base rate for the activity in question is relatively high (for example, credit card fraud) and the profile used is highly sophisticated, data mining will generate more "false positives" (innocent people identified as criminals) than true positives. n36 When the base rate of the criminal activity is low (for example, potential terrorists) and the algorithm less precise (as is probably true of any "terrorist profile"), the ratio of false positives to true positives is likely to be extremely high. n37 In fact, what little we know suggests the government's event-driven antiterrorist data mining efforts have been singularly unsuccessful. n38

Con- Democracy

Domestic surveillance is eating our democracy alive from the inside out.
Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

Since the government unchained itself from the constitution after 9/11, it has been eating our democracy alive from the inside out. There's no room in a democracy for this kind of secrecy: it's anathema to our form of a constitutional republic, which was born out of the struggle to free ourselves from the abuse of such powers, which led to the American revolution. That is what's at stake here: to an NSA with these unwarranted powers, we're all potentially guilty; we're all potential suspects until we prove otherwise. That is what happens when the government has all the data.

Con- Disciplinary Power

Domestic surveillance is a 24-hour panopticon.
Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

General Michael Hayden, who was head of the NSA when I worked there, and then director of the CIA, said, "We need to own the net." And that is what they're implementing here. They have this extraordinary system: in effect, a 24/7 panopticon on a vast scale that it is gazing at you with an all-seeing eye.

Domestic surveillance of entire populations.
Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

ALAN RUSBRIDGER: Well, to begin with, we needed some help from Snowden to point us to what he thought was important. This is not a world that is easily — these are not documents in which the stories sit up and show themselves. This is a complex world. A lot is written in acronyms, if not in actually code, and so we had to be guided to, initially, to some of the stories that Snowden felt were most newsworthy. And it was important for him, I think, that the world had some sense of what he was trying to say before he outed himself, and so, we started doing stories about this intersection between Silicon Valley, telecom companies, and the intelligence agencies. What is, I think, something new, is putting entire populations under a form of surveillance. So, that is what we did in that first week before Snowden came out and revealed himself to be the whistleblower.

Con- Domestic Surveillance Bad

The quantity and form of surveillance matters more to privacy than the quality and content.
Danielle Keats Citron, Lois K. Macht Research Prof Law @ Univ Maryland, Affiliate Scholar Stanford Center Internet & Society, & Affiliate Fellow @ Yale Information Society Project, & David Gray, Assoc Prof Law @ Univ Maryland; May 2013 (Harvard Law Review Forum; 126 Harv. L. Rev. F. 262; "Addressing the harm of total surveillance: A reply to professor Neil Richards")

In assessing the privacy interests threatened by such totalizing surveillance, we have in mind some of the lessons taught by Samuel Warren and Louis Brandeis in their foundational article *The Right to Privacy*. n62 Of course, the surveillance technologies of their era could only record discrete slices of life. Nonetheless, Warren and Brandeis recognized that emerging surveillance capacities threatened individuals' interests in being "let alone" in their "private life, habits, acts, and relations." n63 In Warren and Brandeis's view, the watchful eye of "any other modern device for recording or reproducing scenes or sounds" interfered with the development of a person's "inviolate personality" n64 In discussing a husband's note to his son that he did not dine with his wife -- a pedestrian communication by any measure -- Warren and Brandeis explained that the privacy interest protected was "not the intellectual act of recording the fact that the husband did not dine with [*270] his wife," but the unwanted observance of the "domestic occurrence" itself. n65 Of course, these are precisely the concerns echoed by Justice Scalia on behalf of the Court in *Kyllo*. n66 The threat posed by contemporary surveillance technologies lies in how much and how often people are watched. Modern technologies allow observers to detect, gather, and aggregate mass quantities of data about mundane daily acts and habits as well as "intellectual" ones. n67
The continuous and indiscriminate surveillance they accomplish is damaging because it violates reasonable expectations of *quantitative* privacy, by which we mean privacy interests in large aggregations of information that are independent from particular interests in constituent parts of that whole. n68 To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.

Domestic surveillance is bad for two reasons. First, it eliminates intellectual privacy. Second, it gives power to the watcher over the watched.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

At the level of theory, I will explain why and when surveillance is particularly dangerous and when it is not. First, surveillance is harmful because it can chill the exercise of our civil liberties. With respect to civil liberties, consider surveillance of people when they are thinking, reading, and communicating with others in order to make up their minds about political and social issues. Such intellectual surveillance is especially dangerous because it can cause people not to experiment with new, controversial, or deviant ideas. To protect our intellectual freedom to think without state oversight or interference, we need what I have elsewhere called "intellectual privacy." n5 A second special harm that surveillance poses is its effect on the power dynamic between the watcher and the watched. This disparity creates the risk of a variety of harms, such as discrimination, coercion, and the threat of selective enforcement, where critics of the government can be prosecuted or blackmailed for wrongdoing unrelated to the purpose of the surveillance.

Con- Domestic Surveillance Bad

Surveillance undermines intellectual privacy and intellectual freedom.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

The most salient harm of surveillance is that it threatens a value I have elsewhere called "intellectual privacy." n65 Intellectual-privacy [*1946] theory suggests that new ideas often develop best away from the intense scrutiny of public exposure; that people should be able to make up their minds at times and places of their own choosing; and that a meaningful guarantee of privacy - protection from surveillance or interference - is necessary to promote this kind of intellectual freedom. It rests on the idea that free minds are the foundation of a free society, and that surveillance of the activities of belief formation and idea generation can affect those activities profoundly and for the worse. n66 I want to be clear at the outset that intellectual-privacy theory protects "intellectual" activities, broadly defined - the processes of thinking and making sense of the world with our minds. Intellectual privacy has its limits - it is a subset of all things that we might call "privacy," albeit a very important subset. But importantly, intellectual privacy is not just for intellectuals; it is an essential kind of privacy for us all.
At the core of the theory of intellectual privacy are two claims, one normative and one empirical. The normative claim is that the foundation of Anglo-American civil liberties is our commitment to free and unfettered thought and belief - that free citizens should be able to make up their own minds about ideas big and small, political and trivial. This claim requires at a minimum protecting individuals' rights to think and read, as well as the social practice of private consultation with confidantes. It may also require some protection of broader social rights, whether we call them rights of association or assembly. n67 Protection of these individual rights and social practices allows individuals to develop both intellectual diversity and eccentric individuality. They reflect the conviction that big ideas like truth, value, and culture should be generated from the bottom up rather than from the top down. n68

Surveillance leads to power for the watcher over the watched- can lead to blackmail, discrimination, and persuasion.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

Second, surveillance (even secret surveillance) can create additional harms that are separate from the ones suggested by intellectual-privacy theory. Scholars working in surveillance studies have explored the phenomenon of surveillance in all of its contemporary complexity, going beyond the Panopticon to consider private surveillance, the relationships between watchers and watched, and the wide variety of dangers that modern surveillance societies raise. n97 Recall in this regard that Lyon's definition of surveillance notes that surveillance has a purpose, n98 but in the modern era this purpose is rarely totalitarian domination. All the same, most forms of surveillance seek some form [*1953] of subtler influence or control over others. Even when surveillance is not Orwellian, it is usually about influencing or being able to respond to someone else's behavior. And while surveillance can sometimes have benign goals (like traffic safety, or parents using baby monitors or GPS trackers to keep tabs on their children), it is invariably tied to a particular purpose. Critically, the gathering of information affects the power dynamic between the watcher and the watched, giving the watcher greater power to influence or direct the subject of surveillance. n99 It might sound trite to say that "information is power," but the power of personal information lies at the heart of surveillance. The power effects of surveillance illustrate three additional dangers of surveillance: blackmail, discrimination, and persuasion.

Con- Domestic Surveillance Bad

Blackmail.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

Information collected surreptitiously can be used to blackmail or discredit opponents by revealing embarrassing secrets. American political history over the past hundred years furnishes numerous examples of this phenomenon, but perhaps the most compelling is the treatment of Martin Luther King, Jr., by the FBI. Concerned that Dr. King was a threat to public order, the FBI listened to his private telephone conversations in order to seek information with which to blackmail him. As the official government investigation into the Dr. King wiretaps concluded in 1976:

The FBI collected information about Dr. King's plans and activities through an extensive surveillance program, employing nearly every intelligence-gathering technique at the Bureau's disposal. Wiretaps, which were initially approved by Attorney General Robert F. Kennedy, were maintained on Dr. King's home telephone from October 1963 until mid-1965; the SCLC headquarter's [sic] telephones were covered by wiretaps for an even longer period. Phones in the homes and offices of some of Dr. King's close advisers were also wiretapped. The FBI has acknowledged 16 occasions on which microphones were hidden in Dr. King's hotel and motel rooms in an "attempt" to obtain information about the "private activities of King and his advisers" for use to "completely discredit" them. n100 Imagine a dissident like Dr. King living in today's information age. A government (or political opponent) that wanted him silenced might be able to obtain not just access to his telephone conversations, but also to his reading habits and emails. This critic could be blackmailed outright, or he could be discredited by disclosure of the information as an example to others. Perhaps he has not been having an affair, but has some other secret. Maybe he is gay, or has a medical condition, or [*1954] visits embarrassing web sites, or has cheated on his expenses or his taxes. All of us have secrets we would prefer not be made public. Surveillance allows those secrets greater opportunities to come out, and it gives the watchers power that can be used nefariously.

Surveillance leads to persuasion and control of behavior.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

The bottom line about surveillance and persuasion is that surveillance gives the watcher information about the watched. That information gives the watcher increased power over the watched that can be used to persuade, influence, or otherwise control them, even if they do not know they are being watched or persuaded. Sometimes this power is arguably a good thing, for example when police are engaged in riot control. But we should not forget that surveillance represents a persuasive power shift whether the watcher is a government agent or a corporate marketer, and whether the target is a rioter or law-abiding citizen. The legal system has rules dealing with power imbalances between consumers and businesses, such as the doctrine of unconscionability and much of consumer protection law. There are also rules protecting citizens from state coercion, such as the unconstitutional conditions doctrine and the First Amendment's protections of freedom of thought and conscience. In our age of surveillance, where technological change has given the watcher enhanced powers of persuasion, it may well be time to think about updating those doctrines to restore the balance.

Con- Domestic Surveillance Bad

Surveillance can follow patterns of discrimination and profiling.
Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

From one perspective, the use of the fruits of data surveillance in this way might look like ordinary marketing. But consider the power that data-driven marketing gives companies in relation to their customers. The power of sorting can bleed imperceptibly into the power of discrimination. A coupon for a frequent shopper might seem innocuous, but consider the power to offer shorter airport security lines (and less onerous procedures) to rich frequent fliers, or to discriminate against customers or citizens on the basis of wealth, geography, gender, race, or ethnicity. The power to treat people differently is a dangerous one, as our many legal rules in the areas of fair credit, civil rights, and constitutional law recognize. Surveillance, especially when fuelled by Big Data, puts pressure on those laws and threatens to upend the basic power balance on which our consumer protection and constitutional laws operate. As Professor Danielle Citron argues, algorithmic decisionmaking based on data raises issues of "technological due process." n116 The sorting power of surveillance only raises the stakes of these issues. After all, what sociologists call "sorting" has many other [*1958] names in the law, with "profiling" and "discrimination" being just two of them.

Con- Domestic Surveillance Bad

Surveillance undermines intellectual privacy, leading to normalizing, mainstreaming, and eliminating intellectual diversity, individuality, and free speech.

Neil M. Richards, Prof Law @ Washington Univ; May 2013 (Harvard Law Review; 126 Harv. L. Rev. 1934; "Privacy and technology: The dangers of surveillance")

The second claim at the core of the theory of intellectual privacy is an empirical one - that surveillance inclines us to the mainstream and the boring. It is a claim that when we are watched while engaging in intellectual activities, broadly defined - thinking, reading, web-surfing, or private communication - we are deterred from engaging in thoughts or deeds that others might find deviant. Surveillance thus menaces our society's foundational commitments to intellectual diversity and eccentric individuality.

Three different kinds of arguments highlight the ways in which surveillance can restrain intellectual activities. The first set of arguments relies on cultural and literary works exploring the idea that surveillance deters eccentric or deviant behavior. Many such works owe a debt to Jeremy Bentham's idea of the Panopticon, a prison designed around a central surveillance tower from which a warden could see into all of the cells. In the Panopticon, prisoners had to conform their activities to those desired by the prison staff because they had no idea when they were being watched. As Bentham describes this system, "to be incessantly under the eyes of an Inspector is to lose in fact the power of doing ill, and almost the very wish." n75 Of course, the most famous cultural exploration of the conforming effects of surveillance is Orwell's harrowing depiction in Nineteen Eighty-Four of the totalitarian state personified by Big Brother. n76 Orwell's fictional state sought to prohibit not just verbal dissent from the state but even the thinking of such ideas, an act punished as "thoughtcrime" and deterred by constant state surveillance. n77 Some scholars have documented how the modern surveillance environment differs from both the classic Panopticon and a fully realized Big Brother in important ways. n78 Nevertheless, Orwell's insight about the effects of surveillance on thought and behavior remains valid - the fear of being watched causes people to act and think differently from the way they might otherwise.

Our cultural intuitions about the effects of surveillance are supported by a second set of arguments that comes from the empirical work of scholars in the interdisciplinary field of surveillance studies. Moving beyond the classic metaphors of the Panopticon and Big Brother, these scholars have tried to understand modern forms of surveillance by governments, companies, and individuals in all of their [*1949] complexities. n79 The scope of this burgeoning literature has been wide-ranging and provides many examples of the normalizing effects of surveillance in a wide variety of contexts. In his pioneering work in the 1980s, for example, Professor Anthony Giddens argues that surveillance continually seeks the supervision of social actors and carries with it a permanent risk that supervision could lead to domination. n80 More recent scholars have explored the risks that surveillance poses to democratic self-governance. n81 One such risk is that of self-censorship, in terms of speech, action, or even belief. Studies of communist states give social-scientific accounts of many of the cultural intuitions about these self-censoring effects of surveillance, n82 but so too do studies of modern forms of surveillance in democratic societies. For example, one study of the EU Data Retention Directive notes that "under pervasive surveillance, individuals are inclined to make choices that conform to mainstream expectations." n83 As I explore below, the scope of surveillance studies is much broader than merely the study of panoptic state surveillance; scholars working in this field have examined the full scope of modern forms of watching, including data surveillance by private actors. But above all, surveillance scholars continually reaffirm that, while surveillance by government and others can have many purposes, a recurrent purpose of surveillance is to control behavior. n84

A third and final set of arguments for intellectual privacy comes from First Amendment doctrine. A basic principle of free speech law as it has developed over the past century is that free speech is so important that its protection should err on the side of caution. Given the uncertainty of litigation, the Supreme Court has created a series of procedural devices to attempt to ensure that errors in the adjudication of free speech cases tend to allow unlawful speech rather than engage in mistaken censorship. These doctrines form what Professor Lee Bollinger calls the "First Pillar" of First Amendment law - the "extraordinary protection against censorship." n85 Such doctrines take various forms, such as those of prior restraint, overbreadth, and vagueness, but they are often characterized under the idea of the "chilling effect." This idea maintains that rules that might deter potentially valuable expression should be treated with a high level of suspicion [*1950] by courts. As the Supreme Court put it in perhaps its most important free speech decision of the twentieth century, New York Times Co. v. Sullivan, n86 the importance of uninhibited public debate means that, although "erroneous statement is inevitable in free debate, ... it must be protected if the freedoms of expression are to have the "breathing space' that they "need ... to survive.'" n87 As Professor Frederick Schauer explains, "the chilling effect doctrine recognizes the fact that the legal system is imperfect and mandates the formulation of legal rules that reflect our preference for errors made in favor of free speech." n88 Although the chilling-effect doctrine has been criticized on grounds that it overprotects free speech and makes empirically unsupported judgments, n89 such criticisms miss the point. The doctrines encapsulated by the chilling effect reflect the substantive value judgment that First Amendment values are too important to require scrupulous proof to vindicate them, and that it is (constitutionally speaking) a better bargain to allow more speech, even if society must endure some of that speech's undesirable consequences.

Con- Domestic Surveillance Numbers

FISA searches increased over 342% in the last decade and the number does not include any of Bush's domestic surveillance outside of approval.
Paul M. Schwartz , Prof Law @ UC-Berkeley; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 287; "Surveillance: Reviving telecommunications surveillance law")

FISA reports reveal a dramatic increase in FISA orders. In 1997, there were 748 orders granted; in 2002, there were 932; in 2006, there were 2,181. n106 The increase over the last decade was 342 percent. These statistics are less than helpful, however, in understanding telecommunications surveillance for two reasons.
First, the numbers represent applications for both electronic and physical searches with no further breakdown given. In 1994, Congress amended FISA to allow physical searches as well as electronic ones. n107 The annual FISA reports henceforth lumped together both kinds of surveillance into one figure. Second, and even more significantly, these reports considerably undercount counterterrorism electronic surveillance because of one "semi-known unknown" to be discussed below: the Bush administration has carried out electronic surveillance of the type that FISA circumscribes, but without following this statute's requirements and without revealing the extent and precise nature of these activities.
The available evidence, nonetheless, indicates that 2006 was a highly active year for input from the FISA court. During this year, the FISC denied five of the government's applications, a number of refusals exceeded only in 1999. n108 The court also made substantive modifications to seventy-three proposed orders and denied one application in part. n109

Over 46,000 National Security Letter requests for personal information, or meta-data, in 2005! Official number are underreported. Between 2003 and 2005 over 143,00 NSL requests were issued.
Paul M. Schwartz , Prof Law @ UC-Berkeley; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 287; "Surveillance: Reviving telecommunications surveillance law")

The first kind of reporting is similar to that under FISA -- it calls for release of a limited amount of statistical information. The attorney general is to submit "an aggregate report" to Congress that sets forth "with respect to the preceding year the total number of requests" made pursuant to NSL authority. n113 The NSL report for 2005 listed 9,254 NSLs that included US persons, and 3,501 different US persons implicated by these requests. n114 Yet, as the audit by the Inspector General reveals, these numbers substantially underreported the actual number of NSLs that the FBI issued. Instead of 9,254 NSL requests in 2005, the FBI issued 47,221 NSL requests. n115
The flaws with the reporting begin with the explicit statutory exclusion for the public reports regarding "the number of requests for subscriber information." n116 Subscriber data are of particular interest for law enforcement, and hence, this omission skews the publicly released numbers downward and creates a misleading impression of the level of NSL activity. In addition, wide-reaching flaws existed in the FBI's tracking of NSLs. These involved shortcomings in the way that "the FBI records, forwards, and accounts for information about its use of NSLs." n117
We now reach the second kind of reporting, which comes through the audit requirement. In its Patriot Reauthorization Act, Congress required a detailed examination by the DOJ's inspector general "of the effectiveness and use, including any improper or illegal use" of NSLs. n118 This kind of audit proved valuable in March 2006 when the Inspector General issued the first part of his review of the FBI's use of NSLs. As noted, the Inspector General found a dramatic underreporting of NSLs. Indeed, the total number of NSL requests between 2003 and 2005 totaled [*305] at least 143,074. n119 Of these NSLs requests, as the Inspector General found, "the overwhelming majority . . . sought telephone toll billing records information, subscriber information (telephone or e-mail) or electronic communication transactional records under the [Electronic Communications Protection Act] NSL statute." n120

Con- Economy

Domestic surveillance hurts the long-term business of telecommunication companies
Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

ALAN RUSBRIDGER: Well, I mean, I know some people have a weary shrug and they say, well spies spy and, you know, what is new about that, but, I think it is surprising the degree to which apparently friendly nations are eavesdropping each other, at heads of state level, or cabinet level. We did the story about the G20 meeting in London in which the British government set up a kind of phony tent, an internet cafe, in which delegates could go in and do their emails, not knowing that the British Government or the British intelligence service was logging all their email passwords in order to carry on spying on them when they went home. Most of these were friendly allies, and there was no justification for that except the economic well-being of the U.K. So, I think these are troubling revelations; Brazil is another country. I think it gets to be a big, big story for American innovation and business, if the rest of the world comes to associate these companies with forms of surveillance. That is going to damage American companies. And I think the Silicon Valley companies know this and they are worried. And it also applies to the standards — the international standards by which the internet as a whole operates, and this sense that the Internet is, in some sense, American, or that the American should have an overall role in deciding these standards. There is going be a lot of pushback on that in future and all these things. This is a short-term gain in this kind of behavior and a long term loss.

Con- Hoarding

Government has a pathological hoarding complex.
Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

I am now reliving the last 12 years from what's been disclosed in the past week. I feel a kinship with Snowden: he is essentially the equivalent of me. He saw the surveillance state from within and saw how far it's gone. The government has a pathological incentive to collect more and more and more; they just can't help themselves – they have an insatiable hoarding complex.

Con- National Security Secrets Bad

The entire system of accountability rests on information. National security secrecy prevents the free flow of information and collapses accountability mechanisms.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

This Article has outlined the multiple mechanisms that can help ensure that the executive branch complies with the law, and hold the executive branch accountable when it violates that law. At first glance, it would appear that this complicated network of multiple overlapping accountability mechanisms would provide a plethora of protections and ensure a robust system of accountability. But all of these accountability mechanisms have one factor in common: their dependence on information. If the mechanism does not or cannot obtain information about a particular program, it cannot ensure legal accountability for that program. Remove the information, and the entire structure of apparently robust accountability collapses.
By reviewing the complex narrative of the Bush Administration's warrantless surveillance program and how accountability mechanisms responded to it, one can see how this central weakness - vulnerability to claims of national security secrecy - played out. The Bush Administration systematically used national security secrecy to prevent multiple accountability mechanisms from scrutinizing its warrantless surveillance program. The case study reveals what is essentially a design flaw in our system of accountability: the executive branch's ability to avoid accountability through claims of national security secrecy. This leads to the next question: How can one cure this design flaw?

Information key to democracy.
Jack M. Balkin, Knight Prof Constitutional Law & 1st Amendment @ Yale; Fall 2012 (Hofstra Law Review; 41 Hofstra L. Rev. 1; "The First Amendment is an information policy")

The emergence of democracies changed the purpose of knowledge and information policy. In a democracy, sovereignty rests in the people. But if the people are the rulers, they need information in order to hold their representatives accountable. The public needs access to information about public issues, and about what government officials are doing in their name; it needs relatively inexpensive ways to communicate with other citizens, organize, discuss, protest, and form public opinion. In a democracy, political legitimacy necessarily depends on the free flow of information, and on the maintenance of a robust public sphere of discussion and opinion. In fact, the first democracy in Ancient Athens also pioneered techniques for spreading information among its citizens. n6

Secret regulations undermine open, existing regulations.
Paul M. Schwartz , Prof Law @ UC-Berkeley; Winter 2008 (University of Chicago Law Review; 75 U. Chi. L. Rev. 287; "Surveillance: Reviving telecommunications surveillance law")

Other parts of the surveillance landscape represent an even greater expanse of blank spaces on the legal map. There are a number of "semi-known unknowns" (to coin a phrase); these are kinds of telecommunications surveillance about which only limited public information exists -- this surveillance also occurs outside a detailed legal framework. Specifically, the National Security Administration (NSA) is now engaged in telecommunications surveillance activities in the US of unknown dimensions. This surveillance activity poses a considerable threat to the legal structure of existing regulation: it takes place through secret authorities, rests on secret DOJ opinions, and information gathered from it is fed back into the established system, including the judicial structure for issuing warrants, in a secret fashion.

Con- National Security Secrets Bad

National security secretes prevented adequate Congressional constraints on domestic electronic surveillance, undermining accountability mechanisms.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

While the executive branch is statutorily required to "keep the [full] congressional intelligence committees fully and currently informed of all intelligence activities," n172 the Bush Administration informed only the chair and ranking members of those committees, [*395] along with the Speaker and minority leader of the House of Representatives, and the majority and minority leaders of the Senate about the program. n173 The Bush Administration used a claim of national security secrecy to prevent even this smaller group of legislators from effectively exercising any oversight regarding the program by insisting that they not discuss this issue with other members of the intelligence committees or even their staffs. n174 The powerlessness of these legislators is illustrated by the handwritten note that Senator Jay Rockefeller sent to Vice President Cheney, noting that Rockefeller is "neither a technician nor an attorney," and decrying his "inability to consult staff or counsel" in order to evaluate the legality of the program. n175

National security secrecy prevents private party plaintiffs from proving they were under surveillance, preventing them from gaining the requirement of standing.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

In all of the NSA cases involving private plaintiffs, the government filed motions to dismiss based on the state secrets [*400] privilege. n204 Until recently, the government invoked the state secrets privilege to prevent a private party in civil litigation from accessing or putting into evidence specific items of information that the government asserted must be kept secret for national security or foreign policy reasons. In these NSA cases, the government invoked the state secrets privilege to dismiss the cases in their entirety, asserting either that the plaintiffs could not prove standing or that the defense could not prove its case without accessing information subject to the privilege. While this broad use of the state secrets privilege is not unprecedented, it is occurring on a larger scale than in the past. In the first case to reach a federal appellate court, ACLU v. NSA, the Sixth Circuit ruled for the government on standing grounds, finding that the plaintiffs could not prove that they had been subject to the surveillance, and could not get discovery because of the secrets privilege. n205

National secrecy restricted the Attorney General and members of Congress flow of information the very act they were required to oversee.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

Regarding the impact of secrecy on government behavior, the analysis is, at least initially, more straightforward. As Holmes discusses, the Bush administration was adept at keeping secrets not only from the public and other branches of government, but from itself. Even then-Attorney General John Ashcroft faced restrictions on his ability to receive legal advice within the Department of Justice about NSA activities, the legality of which he was required to oversee. It is also striking how little Congress knew about NSA activities while amending FISA. The larger lessons, however, prove more complicated: strong structural and political factors are likely to limit the involvement of Congress and courts in this area. This Essay concludes by confronting these institutional lessons and evaluating elements of a response that would improve the government's performance by crafting new informational and deliberative structures for it.

Con- Outsourcing of intelligence

NSA privately contracts domestic surveillance.
Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "Inside the NSA's domestic surveillance apparatus: Whistleblower William Binney speaks out"; http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out)

WILLIAM BINNEY: Well, I think it gets back to what Glenn Beck was—or, Glenn Greenwald was talking about: the outsourcing of the intelligence process to contractors. I mean, that's what's been going on for about at least 10 years. They've been outsourcing the dependency on contractors to run their programs. So that means these contractors all have access to all this information about U.S. citizens in all these programs that they're running. I mean, they're depending on them to support it and make it happen and operate so their analysts can access the information.

Private intelligence gathering often used to skirt search warrants and legal requirements.
Jon D. Michaels, Prof Law @ UCLA; August 2008 (California Law Review; 96 Calif. L. Rev. 901; "All the president's spies: Private-public intelligence partnerships in the War on Terror")

The "War on Terror" has dramatically increased the nation's need for intelligence, and the federal government is increasingly relying, as it does in so many other contexts, on private actors to deliver that information. While private-public collaboration in intelligence gathering is not new, what is novel today - and what drives this inquiry - is that some of these collaborations are orchestrated around handshakes rather than legal formalities, such as search warrants, and may be arranged this way to evade oversight and, at times, to defy the law.

Private surveillance threatens privacy, separation of powers, the rule of law, legitimacy of governmental institutions, and undermine the integrity and consumer trust in the marketplace.
Jon D. Michaels, Prof Law @ UCLA; August 2008 (California Law Review; 96 Calif. L. Rev. 901; "All the president's spies: Private-public intelligence partnerships in the War on Terror")

To date, the Executive's apparent practice of identifying and then courting private actors, persuading, coaxing, and sometimes deceiving them to enter into "informal" intelligence-gathering partnerships that often are inscrutable to Congress and the courts, has gone largely unexamined by policymakers and scholars alike. These "handshake agreements," n9 which spawned the now-notorious National Security Agency (NSA) warrantless eavesdropping and call-data programs, as well as a range of lesser-known collaborations with the likes of FedEx and Western Union, have enabled the Executive to operate outside of the congressionally imposed framework of court orders and subpoenas, and also outside of the ambit of inter-branch oversight. In the process, these informal collaborations may unduly threaten privacy rights, separation of powers, the rule of law, and the legitimacy and vitality of bypassed government institutions. In addition, these private-public partnerships may undermine the integrity of the marketplace and weaken consumer trust in key industries.

Con- Privacy

VoIP conversations meet both prongs of the 4th Amendment privacy tests. The 4th Amendment should even extend to unintentional surveillance.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

The Supreme Court has established a two-part analysis that is used to determine whether a particular area is entitled to Fourth Amendment protection. n196 First, the person must have "manifested a subjective expectation of privacy" in that area. n197 It would be difficult to argue that this prong is not satisfied in the case of either encrypted or un-encrypted VoIP because it can be assumed that most people hold a subjective expectation that their private telephonic conversations will not be overheard by unknown third parties. This subjective expectation is manifested even more clearly when users choose to protect their conversations through encryption.
Second, the expectation of privacy must be one that "society is willing to recognize as legitimate." n198 The Supreme Court has generally adopted a rights-based approach to handling this second criterion, finding that one must have a right of privacy in the disputed area enforceable outside of the Fourth Amendment to claim a legally justifiable expectation of privacy. n199 Society has long recognized the [*537] legitimacy of one's expectation of privacy during telecommunications. For example, both FISA and the ECPA make it a felony to engage in nonconsensual telephonic eavesdropping without a warrant. n200 VoIP is essentially a telephone call that is made using alternative means. Accordingly, it is illogical to argue that society would be willing to accept phone conversations as legitimately private when conducted via traditional phone networks but somehow illegitimate and unprotected when conducted via secure Internet telephony. n201 Thus, both prongs of the test are satisfied. Accordingly, VoIP conversations should be protected by the Fourth Amendment, and the government should be required to obtain a warrant prior to undertaking targeted surveillance of such conversations. n202
[*538] Although it is clear that U.S. persons are protected from warrantless government surveillance targeting their VoIP conversations, U.S. persons are not currently protected from situations where such conversations are surveilled indirectly by the government during the otherwise lawful warrantless surveillance of non-U.S. persons abroad. When such a situation occurs, and information to and from U.S. persons is collected without a warrant, the Fourth Amendment should still apply, and the reasonable expectations of protected persons should be respected.

Encrypted VoIP conversations have a higher expectation of privacy than other forms of communication.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

Arguably, a U.S. citizen's expectation of privacy in international communications has never been more reasonable. According to estimates, it would take a computer trillions of years to decipher a message encrypted using an encryption standard that employs a key length half of that currently used by Skype. n203 Consequently, encrypted VoIP users can be certain not only that their communications are virtually immune from random eavesdropping, but that even the NSA would find it difficult -- perhaps even impossible -- to surveil those conversations purposefully, even with the extraordinary computational resources at their disposal. n204 Because encrypted VoIP is so secure, it stands to reason that one's expectation of privacy in such communications is much higher than it is with almost any other form of communication. Because Fourth Amendment protection is based largely on the reasonableness of one's expectations, it would seem that using encrypted VoIP should provide U.S. citizens with the highest level of Fourth Amendment protection. n205

Con- Privacy

There is a reasonable expectation of privacy on encrypted VoIP calls. FISA should be revised to guarantee the privacy of U.S. residents making calls outside the U.S. so they will not be subject to warrantless searches.

DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

The NSA's attempt to answer these questions can be found in the agency's minimization procedures, which are detailed in United States Signals Intelligence Directive 18 ("USSID 18"). n13 Under most circumstances, the directive requires the NSA to destroy information gained inadvertently from unsuspecting U.S. persons without a warrant; n14 however, section 7.2(c)(4) allows the agency to disseminate such "inadvertently acquired" information to U.S. law enforcement if it appears to implicate the U.S. person in criminal conduct. n15

This Article discusses this loophole in light of recent advancements in encrypted Voice over Internet Protocol ("VoIP") technology. It concludes that the minimization procedures set forth in USSID 18 are constitutionally deficient because they fail to take into account the growing expectation of privacy that has resulted from advancements in encryption technology. The directive should be redrafted to mandate greater consideration of an individual's reasonable expectation of privacy when determining how information collected without a warrant may be disseminated and used by the agency.

Con- Privacy- AT: Criminal exception

Criminal exception incentivizes obtaining inadvertently acquired information.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

USSID 18 must be redrafted to forbid the use of inadvertently obtained information for the purpose of initiating criminal investigations against U.S. citizens unless exigent circumstances are presented. By disallowing the use of such information for these purposes, the government would be ensuring that the NSA stays focused on its primary mission -- protecting the United States from terrorism and foreign intelligence operations -- and not engaging in general criminal investigations domestically. Under the current directive, the NSA has an incentive to collect as much "inadvertently acquired" information as possible. If the possibility of using such information to initiate unrelated criminal investigations were removed, the agency would cease to have an incentive to collect information unrelated to its national security mission. This would provide the agency with an incentive to maintain its focus on foreign terrorism and counterintelligence, and it would curb the temptation to stray into unrelated matters more appropriately left to those charged with domestic law enforcement.

No distinction made on seriousness of crime.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

Under the provision as it is currently written, evidence that an American citizen may have committed a misdemeanor could properly be disseminated to police for local criminal investigation. n229 There is no differentiation or qualification regarding the seriousness of the offense revealed. n230 Without any limitation on the type of "criminal" information that can be turned over to law enforcement, this provision represents a violation of the Fourth Amendment rights of those surveilled. n231 A reasonable limitation must be placed on this dissemination power, limiting it to situations where grave national security or other emergency situations are presented. Most of the other exceptions listed under USSID 18 section 7.2(c) require some form of exigent circumstance to exist before a U.S. citizen's identity may be divulged. n232 Section 7.2(c)(4) likewise should contain such limits.

Con- Totalitarianism

Domestic surveillance is like 1984.
Mark Klein, technician @ AT&T for over 20 years & whistleblower; January 9, 2007 (PBS Frontline Interview; "Spying on the home front"; http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html)

... As you get this picture of this spreading network, ... what do you think you're looking at?
I think I'm looking at something Orwellian. It's a government, many-tentacled operation to gather daily information on what everybody in the country is doing. Your daily transactions on the Internet can be monitored with this kind of system, not just your Web surfing. All kinds of business that people do on the Internet these days -- your bank transactions, your e-mail, everything -- it sort of opens a window into your entire private life, and that's why I thought of the term "Orwellian." As you know, in [George] Orwell's story [*1984*], they have cameras in your house, watching you. Well, this is the next best thing. ...

Domestic surveillance is a slippery slope to totalitarianism.
Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "On a Slippery Slope to a Totalitarian State": NSA Whistleblower Rejects Gov't Defense of Spying"; http://www.democracynow.org/2013/6/10/on_a_slippery_slope_to_a)

WILLIAM BINNEY: Well, it's certainly an extension of what I've been trying to say, that we were on a slippery slope to a totalitarian state. And that was simply based on the idea that the government was collecting so much information about all the citizens inside the country, that it gave them so much power. They could target people in the—for example, use it, use the knowledge to collectively assemble all of the people participating in the tea party, target them, and do—they could even do active attack on them with, going across the network, taking material out of their computers. So it was a very dangerous situation, in my mind. And still is.

Domestic surveillance returns us to the time of King George III and general warrants that inspired the American Revolution and 4th Amendment.
Cindy Cohn, Legal Director Electronic Frontier Foundation; Spring 2010 (Journal on Telecommunications and High Technology Law; 8 J. on Telecomm. & High Tech. L. 351; "Privacy and law enforcement: Lawless surveillance, warrantless rationales")

It's a remarkable turn of events, this shift from the traditional limitations on search and seizure to the wholesale scooping up and storing of our communications, our communications records, and indeed our entire digital lives. The United States was founded on the rejection of such wholesale collection of citizen communications and papers. In the late 1700s, "general warrants" were pieces of paper that gave the Executive (then the King) power to search colonial Americans without cause. n12 These general warrants were routinely used by British customs inspectors to search and seize papers in colonial homes in search of evidence of smuggling. n13 Indeed, John Adams noted that "the child Independence was born" when Boston merchants represented by James Otis unsuccessfully sued to stop these unchecked powers. n14 The Fourth Amendment was adopted in part to stop these "hated writs" n15 and to make sure that searches of the papers of Americans required an individualized, probable cause showing to a court. n16
[*354] The wholesale collection of American "papers" as part of the warrantless surveillance programs then returns us to the policies of King George III - only with a digital boost. The programs collect our emails, phone calls, Internet searches, website visits, Facebook posts, and other Internet data and subject them to computer review to pick out what will be reviewed by human analysts. This first step can lead to even more intrusive review by faceless government computers and bureaucrats when the computer programs written by the bureaucrats determine that our communications or communications patterns merit further scrutiny. n17

Con- Unrestrained Executive Power Bad

A blank check for executive powers over domestic surveillance could lead to abuses of speech, association, and liberty rights, subverting the functioning of American democracy. The Supreme Court has consistently struck a balance between security and liberty during wartime.
Jeremy Neff, Former Associate Member Univ Cincinnati Law Review; Winter 2006 (University of Cinncinnati Law Review; 75 U. Cin. L. Rev. 887; "Does (FISA + NSA) AUMF – Hamdi = Illegal domestic spying?")

Hamdi did not give blanket approval for the detention of American citizens. In the prophetic words of Justice O'Connor, "a state of war is not a blank check for the President when it comes to the rights of the Nation's citizens." n178 Rather, Hamdi gave such detention very narrow approval based on the facts of the case - namely, the fact that Hamdi was captured armed on the battlefield with the enemy. Even then, the Court required that Hamdi be granted some basic form of due process rights. This result is quite distinct from what the Administration is asserting when it claims an unfettered right to violate Fourth Amendment rights with no basic protections, no judicial review, and [*914] within a very different context - unarmed citizens within the bounds of U.S. territory.
To suggest that the Bush Administration is the first to conduct warrantless spy operations against U.S. citizens would be misleading. The White House and Department of Justice have asserted repeatedly that warrantless wiretapping has been authorized by presidents "at least since the administration of Franklin Roosevelt in 1940." n179 However, the source cited for this assertion is a thirty-five-year-old court opinion - calling into question whether any recent administration has conducted such a domestic spying program. n180 Interestingly, in 1973, the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities (Church Committee) reached the same conclusion when it conducted an investigation in the aftermath of the Nixon Administration Watergate scandal. It was in large part because of the Church Committee's troubling findings regarding the domestic surveillance conducted by past presidents that Congress adopted FISA in 1978 to curb Executive abuses of domestic wiretapping. n181 The legislative history of FISA reveals that the statute's purpose was to balance concerns about the presidential abuse of power through "unilateral determinations" of when national security justifies domestic spying against the need for the "legitimate use of electronic surveillance to obtain foreign intelligence information." n182
Because Congress already conducted the balancing of liberty and security interests regarding wiretapping when it adopted FISA, n183 the courts should not legislate from the bench in contravention of the statute. FISA eases the normal restrictions on domestic surveillance while still retaining a role for the judicial branch, much like the limited detention rights prescribed by the Court in Hamdi. In the words of the Hamdi Court, "whatever power the United States Constitution envisions for the Executive" during times of war, "it most assuredly envisions a role for all three branches when individual liberties are at stake." n184 Absent any check on Executive power, the potential for abuses of speech, association, and liberty rights are staggering, and there is the possibility [*915] of subverting the very functioning of the American democratic system. n185 In the years following the Nixon White House, Congress recognized and addressed this concern with FISA. The courts should reject the NSA program because it completely circumscribes the role of the judicial branch in an issue that impacts very fundamental American liberties.

Con- Civil Liberties Outweigh Security

Laws are even more important when responding to the threat of terrorism. Without requiring plausible reasons for governmental action, governments will stop having plausible reasons for acting. Laws and liberties facilitate midstream adjustments and help people discover mistakes that damage national security. Liberty improves security by preventing errors from hiding under a veil of national security secrecy. Prefer this evidence because it is compares domestic electronic surveillance to the threat of terrorism.

Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

Law should play a similar role for our leaders, and it is one that becomes more, and not less, important in responding to the terrorist threat to the United States. Holmes astutely builds on his analogy to the relatively rigid protocols upon which emergency room personnel rely. n3 He argues that rights embodied in law "demarcate provisional no-go zones into which government entry is prohibited unless and until an adequate justification can be given." n4 Thus, legal rights serve as "a trip-wire and a demand for government explanation." n5

This mandatory process forces the Executive to explain her behavior and to confront other views. As Holmes warns, "If a government no longer has to provide plausible reasons for its actions ... it is very likely, in the relative short [*408] term, to stop having plausible reasons for its actions." n6 Beyond its steadying function then, law can help the Executive "to make appropriate midstream adjustments in a timely fashion" and help everyone discover mistakes. n7 Legal rules help facilitate an "adaptation to reality." n8 In contrast, when executive behavior is shielded in secrecy, inordinate delays in correcting terrible mistakes may damage national security.

The Jorde Lecture by Holmes burns with the light of clear analysis and calm rationality. In this Essay, I wish to build on it by considering Holmes's model of "public liberty" in greater depth. Public liberty improves security by preventing policymakers from hiding errors under a veil of secrecy. It even opens up the process of debate within the executive branch itself. This Essay develops Holmes's model by discussing how private liberty, and information privacy in particular, is a precondition for public liberty. For Holmes, private liberty is largely a negative right - a right to be free from governmental interference. In contrast, my view is that privacy is also an element of public liberty. Participation in a democracy requires individuals to have an underlying capacity for self-determination, which requires some personal privacy.

This Essay then analyzes a number of Holmesian concepts through the lens of the recent process of the amendment of the Foreign Intelligence Surveillance Act (FISA). n9 Since information privacy stands at the intersection of private and public liberty, it is an ideal topic for evaluating Holmesian principles about the contribution of law during times of national emergency. This Essay considers, in particular, the Bush administration's policies toward FISA and Congress's amendment of this statute.

Con- Civil Liberties Outweigh National Security

Liberty and rights create a society worth defending.
Shahab Mossavar-Rahmani, JD Loyola Law; 2008/2009 (Loyola of Los Angeles Entertainment Law Review; 29 Loy. L. A. Ent. L. Rev. 133; "The Protect America Act: One nation under go surveillance")

Justice Warren once wrote: "Implicit in the term "national defense' is the notion of defending those values and ideals which set this Nation apart ... It would indeed be ironic if, in the name of national defense, we would sanction the subversion of ... those liberties ... which makes the defense of the Nation worthwhile." n272 A system of information collection that continuously chips away at the rights of Americans, while simultaneously impeding any possible legal remedy, turned our democratic system into an Orwellian one. n273

Public liberty improves national security by preventing policymakers from hiding error behind secrecy. Excessive secrecy leads to parts of the government concealing information from itself, leads to not only deceptions of others, but also a belief in one's own illusions.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

In this fashion, public liberty plays a significant role in improving security by preventing policymakers from hiding their errors from the public and Congress behind a veil of secrecy. Holmes points out another reason why [*410] excessive secrecy is problematic: "The executive branch cannot hide from Congress, the courts, the public, and the press, without hiding from itself as well." n13 When important executive branch officials conceal information from others with a need to know within their own branch of government, significant problems will arise. Indeed, as Holmes argues in The Matador's Cape, the Bush administration suffered at many junctures from a bad case of self-deception. n14 Its secrecy was accompanied not only by an eagerness to deceive others, but also a fervent belief in its own illusions. n15

Information privacy is a public, negative right, and a private, positive right.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

Here, one can build on an aspect of Holmes's analysis in his Jorde Lecture. Private liberty, as Holmes explains it, is merely equivalent to a negative right - a right to be free from government interference. n21 Yet, privacy is a personal interest that also plays an important role in preserving public rights. To relate this line of inquiry back to Holmes's idea of public liberty, examination and criticism of government behavior requires individuals to have an underlying capacity for self-determination, and this ability in turn requires some level of personal privacy. Holmes also shares this view. He notes that "democracy depends on maintaining a certain balance between the secrecy of government and the privacy of citizens." n22 He also warns, "At a certain point, we must worry that an under-scrutinized government ruling an over-scrutinized society will lose its essentially democratic character." n23
In particular, perfected surveillance of naked thought's expression, especially in a digital age, will short-circuit the individual's decision making process. As I have argued elsewhere, the role of information privacy is to set limits on access to information that will have an impact on the extent to which certain actions or expressions of identity are encouraged or discouraged. n24 Privacy is in this sense a constitutive element of personal and community identity alike. Like public liberty, private liberty, bolstered by laws that safeguard information privacy, is a way to bolster collective rationality.

Con- AT: National Security Outweighs Civil Liberties

All decisions over national security require a security-security tradeoff since there are scare resources and opportunity costs. Public liberties are critical to making sure leaders are accountable for their mistakes.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

Public liberty ultimately enhances collective rationality - it is a path to heightening our wisdom by increasing access to pertinent information and improving decision making. As Holmes notes, "all people, including politicians, are prone to error; all people, especially politicians, dislike admitting their blunders," but "all people relish disclosing the miscalculations and missteps of their bureaucratic or political rivals." n16 Because no one likes to admit mistakes, a real danger exists that an emphasis on secrecy and speed will impede this crucial source of error recognition and error correction and with it the government's ability to analyze new threats in a self-critical fashion. This danger proves quite critical because of the need for the government to engage in what Holmes terms "security-security tradeoffs." n17 As he observes, "There are no zero-risk options in the war on terror." n18 Due to scarce resources and opportunity costs, the government must make choices "of security along one dimension for security along another." n19

The risk of civil liberties violations outweighs the time of an imminent terrorist threat.
Paul M. Schwartz, Prof Law @ UC-Berkeley; April 2009 (California Law Review; 97 Calif. L. Rev.; "Warrantless wiretapping, FISA reform, and the lessons of public liberty: A comment on Holme's Jorde lecture")

In sum then, the NSA warrantless wiretapping and congressional response through FISA amendment raise a risk identified by Holmes, namely, an improper balance between the secrecy of government and the privacy of citizens. Holmes also points to the need, as noted above, to make choices among different aspects of security. These security-security tradeoffs require managing risk over time, and making complex choices between "security along one dimension for security along another." n129 Much about these surveillance activities remains secret, however, and for that reason it is difficult to assess the nature of the ensuing regulation, the FAA.

National security should not become a justification for sacrificing basic rights like privacy.
Jonathan D. Forgang, JD Fordham Univ Law; October 2009 (Fordham Law Review; 78 Fordham L. Rev. 217; " 'The right of the people': The NSA, the FISA amendments act of 2008, and foreign intelligence surveillance of Americans overseas")

It is not enough for a country to state its intention to uphold certain basic rights. The Founders knew that a government must include internal checks and balances to ensure the protection of important constitutional rights. Privacy is a basic right, protected by the laws and Constitution of the United States. While national security is an immensely important interest, the government should not sacrifice all else while trying to protect it.

Con- Authorization of the Use of Military Force

Based on the Supreme Court's interpretation of the AUMF in Hamdi they would not conclude that AUMF authorizes NSA domestic surveillance.

Jeremy Neff, Former Associate Member Univ Cincinnati Law Review; Winter 2006 (University of Cinncinnati Law Review; 75 U. Cin. L. Rev. 887; "Does (FISA + NSA) AUMF – Hamdi = Illegal domestic spying?")

Nothing in Hamdi suggests that the Court approves of the use of war powers as authorized by the AUMF within U.S. territory. In fact, by emphasizing Hamdi's capture in Afghanistan, n129 the Court seems to implicitly adopt the traditional limitation of executive war powers to the "theater of war" where "day-to-day fighting" is taking place. n130 In his dissent Justice Scalia cites Ex Parte Milligan, a decision granting the writ of habeas corpus to a Confederate sympathizer and agitator in Indiana during the Civil War, for the proposition that an American citizen cannot be subjected to military tribunals under the Executive war powers. n131

In contrast to Justice Scalia's interpretation, the plurality emphasized the location of the individual against whom war powers are being used as the determinant factor. Hamdi was captured overseas, while the farmer in Milligan was in Indiana, far from the Civil War front. n132 To bolster its interpretation the plurality noted that only one case cited by Justice Scalia, In re Territo, n133 involved a parallel factual situation to that in Hamdi involving a "United States citizen captured in a foreign combat zone." n134 Territo involved a U.S. citizen who was captured on the battlefield in Sicily while serving in the Italian army during World War II. The Hamdi plurality noted that the military detention was upheld in Territo because, much like Hamdi, the citizen was captured in a foreign combat zone.

In fairness, Justice Scalia also found the location rationale to be important. Justice Scalia concluded that "[a] view of the Constitution that gives the Executive authority to use military force rather than the force of law against citizens on American soil flies in the face of the [*907] mistrust" the Framers had for Executive military power. n135 Clearly, it was important to Scalia's reasoning that the alleged constitutional violation, the denial of basic due process rights, took place within the boundaries of U.S. territory. From Justice Scalia's perspective, though, the issue of location was secondary to the more fundamental issue of citizenship.

Justice Thomas offered the broadest interpretation of executive power under the AUMF in Hamdi. While he did not directly address the significance of citizenship status or the location in which war powers are applied, he did observe that the plurality had not "adequately explained the breadth of the President's authority." n136 Presumably, as applied to the NSA program, Justice Thomas's expansive view of executive power under the AUMF would allow for war powers to be used against U.S. citizens within U.S. territory.

Whether following the logic of Justice Scalia's dissent that war powers should not be used against U.S. citizens or the plurality's approach of only applying war powers when an individual is in the theater of war, the result regarding the NSA domestic spying program is the same: The war powers should not be used against U.S. citizens within U.S. territory.

Con- Authorization of the Use of Military Force

AUMF only covers necessary and appropriate force by the US Armed Forces. NSA domestic surveillance does not meet these three criteria.

Jeremy Neff, Former Associate Member Univ Cincinnati Law Review; Winter 2006 (University of Cinncinnati Law Review; 75 U. Cin. L. Rev. 887; "Does (FISA + NSA) AUMF – Hamdi = Illegal domestic spying?")

As in Hamdi, a challenge to the NSA domestic spying program will turn on what precisely was authorized by Congress through the AUMF. Domestic spying is not so clearly granted implicitly by the AUMF. First, the AUMF speaks exclusively of the use of the "United States Armed Forces" against those responsible for the 9/11 attacks. n147 [*909] Although the military's taking an armed enemy solider captive on a foreign battlefield seems to be an obvious example of such a use of force, the use of cutting-edge technology to intercept communications based at least partially inside the United States stretches Congress's meaning in the AUMF of "necessary and appropriate force." n148 The Hamdi plurality was careful to repeatedly limit its opinion to the particular facts of the case involving an armed enemy combatant captured overseas on the battlefield. n149 Justice Souter spoke to the question of "force" directly when he observed that despite the "generalities" of the AUMF, the scope of the law was clearly limited to the use of "military power." He further defined this as the "use of armies and weapons" against enemy armies and terrorists. n150 Furthermore, many critics question whether the NSA program was "necessary" in light of the existing methods provided by FISA for domestic spying. n151 From the beginning of the domestic spying controversy, the Bush Administration has argued that FISA does not provide the "speed and agility" needed to wage the "War on Terror." n152 However, FISA allows for the "emergency employment of electronic surveillance" without a court order for up to seventy-two hours upon determination by the Attorney General that the normal FISA conditions are met. n153 Given the Administration's claims that its domestic surveillance targets quick-moving suspects, a seventy-two hour period should be more than enough time to gather intelligence. n154 Moreover, in [*910] FISA, Congress provided a fifteen-day window after the commencement of a war during which the Executive can authorize surveillance without a court order. The legislative record indicates that Congress "intended that this period will allow time for consideration of any amendment to this act that may be appropriated during a wartime emergency." n155 Given these exceptions to normal FISA procedures, the courts should not accept the Administration argument that the program is "necessary" as required by the AUMF. Finally, the courts should find that the NSA program is not "appropriate" under the AUMF because the program contravenes clear congressional intent. The plurality upheld the detention of enemy combatants in Hamdi as a normal and "appropriate" aspect of war that Congress "clearly and unmistakably authorized." n156 On the other hand, three days after the existence of the NSA program was leaked, when a reporter asked the Attorney General why he did not seek a new statute that allowed something like the NSA program, the Attorney General responded that, "we were advised [by members of Congress] that that ... was not something we could likely get." n157 In light of the bipartisan criticism of the NSA program, the Administration's assessment of the viability of legislative authorization was probably accurate. n158 Characterizing the domestic spying program as "appropriate" pursuant to the AUMF is difficult when both the Administration and its critics acknowledge that Congress would not have directly approved of the program. Furthermore, a use of force cannot be considered "appropriate" when it conflicts with existing law. In contrast to the Hamdi plurality, which read a limited detention power into the AUMF, Justice Scalia observed that when a specific statute denies the Executive a power the AUMF must express a clear intent to override the original prohibition. n159 FISA criminalizes any warrantless wiretapping not authorized by statute, n160 and Congress clearly did not specifically authorize the NSA program in the AUMF. n161 Thus, the only reasonable conclusion is that the NSA [*911] program is not an "appropriate" action authorized by the AUMF. While in Hamdi there were also existing laws that explicitly denied the power sought by the Executive through the AUMF, the Court held that because taking prisoners is so fundamental to war it was unreasonable to argue that Congress did not intend to allow such detention. n162 In contrast, whether domestic wiretapping is inherent to war-making is less clear.

Con- Authorization of the Use of Military Force

AUMF and Hamdi decision would not cover NSA domestic surveillance. Data mining and domestic surveillance are not necessary and appropriate force, and collecting intelligence is not force.
Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

The first argument that the AUMF overrides FISA is not supported by FISA's text, which states that FISA "shall be the exclusive means by which electronic surveillance ... may be conducted." n164 One court has stated that the exclusivity language "makes it impossible for the President to "opt-out' of the legislative scheme." n165 It is a settled canon of statutory interpretation that general provisions are superseded by specific provisions. n166 FISA does not permit domestic electronic surveillance without a warrant, but the AUMF allows the President to use all "necessary and appropriate [*462] force." n167 Thus, it would take a strained reading to find that the AUMF's general provision overrides FISA's specific language n168 requiring a warrant for domestic surveillance. Notwithstanding FISA's text, it is unlikely that gathering and datamining numerous call records constitutes the "necessary and appropriate force" required to invoke the AUMF. n169

Similarly, the second argument for Presidential authority, relying on Hamdi, is also misplaced. While it is true that intelligence acquisition is an important part of any combat, "it is not clear that the collection of intelligence constitutes a use of force." n170 In Hamdi, the Court held that the AUMF authorized the detention of a United States citizen even though the Non-Detention Act provided that a United States citizen could not be detained unless Congress authorized it. n171 Justice O'Connor, writing for the plurality of the court, found that the AUMF does not support "indefinite detention for the purpose of interrogation." n172 Thus, the Court seemed to be indicating that intelligence gathering is not a necessary or appropriate force. Accordingly, because the NSA call database is for intelligence purposes, it would likely not constitute the use of force authorized by the AUMF's "necessary and appropriate force" clause.

Con- Examples- ECHELON

ECHELON is an international surveillance project that includes the UK, Canada, Australia, and New Zealand. ECHELON intercepts three billion communications every day and can capture all electronic communication.

DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

In recent years, several high-profile investigative reports have rekindled public interest in the ECHELON network. For example, in 2000, the CBS program *60 Minutes* aired a feature on the ECHELON system. n32 The program included an interview with Mike Frost, a former twenty-year employee of Canada's principal signals intelligence agency, the Communications Security Establishment (the "CSE"). n33 During the interview, Frost made revelations about the specific capabilities of the ECHELON system, stating at one point that the system captures "everything . . . from data transfers to cell phones to portable phones to baby monitors to ATMs." n34 Frost had been one of the first insiders to divulge specifics about the breadth of ECHELON's surveillance capabilities, and his account helped to spark renewed public interest in the system. n35

[*512] News reports concerning the ECHELON system raised concerns in Europe, and on July 5, 2000, the European Parliament established a temporary committee to investigate. n36 Approximately one year later, this committee issued its "Report on the Existence of a Global System for the Interception of Private and Commercial Communications." n37 The report detailed the existence of ECHELON, its legality under European and international law, and its implications for the privacy rights of European citizens. n38 Subsequently, the European Union began seeking ways to counter the effects of ECHELON through enhanced encryption protocols. n39 In 2004, the European Union created the SECOQC project. n40 Under the project, the European Union will spend $ 11 million on research and development for a new quantum encryption system that could be used to thwart the signals intelligence capabilities of ECHELON. n41

The ECHELON system is rumored to capture as many as three billion communications each day. n42 The system's reach spans the globe due to the strategic locations of its five member nations, which [*513] include the United States, the United Kingdom, Canada, Australia, and New Zealand. n43 Together, these nations comprise the UKUSA community, which has its roots in the BRUSA COMINT alliance established between the United States and the British Commonwealth during World War II. n44 Through satellite and other means, ECHELON is believed to be capable of capturing most electronic signals broadcast anywhere in the world. n45

Con- Examples- Highlander

Highlander monitored U.S. citizens in the Middle East making calls to the U.S.
Jonathan D. Forgang, JD Fordham Univ Law; October 2009 (Fordham Law Review; 78 Fordham L. Rev. 217; " 'The right of the people': The NSA, the FISA amendments act of 2008, and foreign intelligence surveillance of Americans overseas")

On October 9, 2008, the ABC News program Nightline presented an investigative report alleging that the National Security Agency (NSA) monitored satellite phone calls between American civilians in the Middle East and persons in the United States. n2 The report's most serious allegations came from two former intelligence officers who worked in the top secret NSA program "Highlander," n3 an NSA surveillance program that monitors satellite phone transmissions on the Inmarsat network in the Middle East. n4 The two former Highlander analysts Adrienne Kinne and [*220] David Murfee Faulk claimed they listened to and recorded hundreds of phone calls between American citizens in the Middle East and parties living inside the United States. n5 Among these American citizens in the Middle East were "US military officers, American journalists and American aid workers." n6 The analysts alleged that this surveillance would often continue even if the callers were American and there was no indication that the conversations contained foreign intelligence, in violation of American intelligence law. n7
In the years immediately prior to the start of the Highlander program, the NSA had diligently avoided eavesdropping on Americans. n8 Kinne alleged that during her involvement in Highlander, however, the government continued to monitor the calls even after the callers were identified as aid organizations. n9 The allegations, if true, are the first time that anyone with knowledge of the NSA's foreign surveillance operations has accused the agency of spying on Americans overseas. President George W. Bush previously disclosed, in 2005, that the government had approved a domestic surveillance program as a part of its "War on Terror" and monitored suspect overseas phone calls coming into the United States. n10 However, Bush claimed that the government limited this surveillance to known al Qaeda [*221] operatives or members of al Qaeda affiliated terrorist organizations calling to or from the United States. n11

Highlander violates privacy and leads to a chilling effect on communication with journalists, aid and human rights organizations.
Jonathan D. Forgang, JD Fordham Univ Law; October 2009 (Fordham Law Review; 78 Fordham L. Rev. 217; " 'The right of the people': The NSA, the FISA amendments act of 2008, and foreign intelligence surveillance of Americans overseas")

Despite these benefits, Kinne claims that the very utility of this type of intelligence only emphasizes how much eavesdropping on aid workers and other non-enemy combatants distracts intelligence officers from beneficial intelligence gathering. n14 The surveillance can have far-reaching negative repercussions. The aid organizations that have been targeted by Highlander claim that the surveillance requires them to "take burdensome and costly measures" to protect confidentiality. n15 It also discourages clients, journalistic sources, and victims of human rights abuses from sharing sensitive information with journalists and aid organizations out of fear for their own safety n16 and undermines the ethical responsibility of confidentiality between humanitarian organizations and their clients. n17

Con- Examples- Narus

Narus semantic traffic analyzers vacuum up electronic data and sift through it for the NSA. It is clearly illegal and unconstitutional.

Mark Klein, technician @ AT&T for over 20 years & whistleblower; January 9, 2007 (PBS Frontline Interview; "Spying on the home front"; http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html)

February 2003?

February 2003. Then I was looking at the equipment list. All these three documents were obviously all part of the same project, which involved cutting this splitter cabinet in. I looked at the main one, which is called Study Group 3, San Francisco, kind of an innocent-sounding name. What are they studying?

On the equipment list were standard things ... like Juniper routers and Sun servers, which are very common, high-quality equipment, and Sun storage equipment to store data. And there was a whole list there.

But then there was one thing that was odd, because I didn't recognize it. It was not part of normal, day-to-day telecommunications equipment that I was familiar with in years of my work, and that was a Narus STA 6400. STA stands for Semantic Traffic Analyzer. I'd never heard of this, so I started doing a little Google research to find out what this is about; what's a Semantic Traffic Analyzer? And so I find, after doing some Googling, that it's not only designed for high-speed sifting through high-speed volumes of data, looking for something according to various program algorithms, something you'd think would be perfect for a spy agency.

Turns out it was perfect for a spy agency, and they were already using it and boasting about it. I found, for instance, there was a conference in 2003 in McLean, Va., whose agenda was posted on the Internet. I'm sure you know McLean, Va., is the hometown of the CIA. ... The sponsor of the show was Narus, and they posted the agenda for this computer show, which was semi-public, and everybody was there, from the phone companies like AT&T and Verizon to the intelligence agencies like the DEA [Drug Enforcement Administration] and the FBI and local police agencies and the FCC [Federal Communications Commission]. I have to assume the NSA was there, although they didn't list themselves. But one of the guys on the agenda was William Crowell. William Crowell was the former deputy director of the NSA. He was on one of the forum lists as a speaker, along with the founder of Narus and a whole bunch of them.

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." ...

When you spotted this, you'd been in the room; you've seen the splitter; you've now got the documents; you've seen the Narus; you've gone to the Internet; you've seen what this technology show is about. What is it you think is going on here? What's your reaction?

My reaction -- that's why I practically fell out of my chair -- was that from all the connections I saw, they were basically sweeping up, vacuum-cleaning the Internet through all the data, sweeping it all into this secret room. ... It's the sort of thing that very intrusive, repressive governments would do, finding out about everybody's personal data without a warrant. I knew right away that this was illegal and unconstitutional, and yet they were doing it.

So I was not only angry about it; I was also scared, because I knew this authorization came from very high up -- not only high up in AT&T, but high up in the government. So I was in a bit of a quandary as to what to do about it, but I thought this should be halted.

Con- Examples- Prism

Prism used probably forty telecom companies for domestic surveillance
Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "Inside the NSA's domestic surveillance apparatus: Whistleblower William Binney speaks out"; http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out)

WILLIAM BINNEY: Well, the only surprise I got—I mean, the PRISM program, I had assumed was going on anyway. But the court order that was published that showed the—it showed the serial number at the top, on the top right side of it. It was 13-80. That meant it was the 80th order of 2013 of the FISA court. And if that order was typical of all those other 79, which was authorizing them—or ordering them to turn over records that would—to NSA, even though it was the FBI doing the request, it shows you the relationship between FBI and NSA. It's really close, and they're depending on NSA to do their processing. But what it is, what that tells me, that serial number told me that, gee, if all those orders addressed individually every quarter—this was the second quarter of 2013—then there would be, at a minimum, 40 companies involved in this activity. So, it would be telcoms—it would be a mix of telcoms and Internet service providers.

Con- Examples- Stellar Wind

Stellar Wind was an unconstitutional NSA domestic surveillance program that did not receive approval from the courts.
Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "Inside the NSA's domestic surveillance apparatus: Whistleblower William Binney speaks out"; http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out)

And then they took me out and interrogated me on the back porch. And when they did that, they tried to get me—they said they wanted me to tell them something that would be—implicate someone in a crime. And I said, well, I didn't—I thought they were talking about someone other than the President Bush, Dick Cheney and Hayden and Tenet, so I said I didn't really know about anything. And they said they thought I was lying. Well, at that point, "OK," I said, "I'll tell you about the crime I know about," and that was that Hayden, Tenet, George Bush, Dick Cheney, they conspired to subvert the Constitution and the constitutional process of checks and balances, and here's how they did it. And I talked about program Stellar Wind, all the data coming in, about how they managed to graph it and also how they bypassed the courts. They didn't tell the courts about this program, and they didn't solicit any approval from the courts. And they also only told four people initially in Congress, that were the—they were the chiefs and deputies of the Intelligence Committee. That was on the House. That was Porter Goss and Nancy Pelosi. I don't remember the Senate side. But when you do that and—I mean, Senator Rockefeller, when he got briefed into those programs in 2003, said he wasn't capable of understanding any of it, because he wasn't—he wasn't a technician, he wasn't a lawyer, so he couldn't do anything about it. That was in his handwritten note to Dick Cheney. So, I mean, it was clear they were doing something that was unconstitutional and against any number of laws that existed at the time.

Con- AT: Bush not Obama

Obama has embraced Bush's policies of domestic surveillance and used the Justice Department to block court review.

Cindy Cohn, Legal Director Electronic Frontier Foundation; Spring 2010 (Journal on Telecommunications and High Technology Law; 8 J. on Telecomm. & High Tech. L. 351; "Privacy and law enforcement: Lawless surveillance, warrantless rationales")

Aside from the attempted justifications of Yoo and Hayden, the Bush Administration's central view was that, when taking steps that it deemed necessary for national security, the Executive branch was somehow above the niceties of the Constitution. n26 As a result, it is unsurprising that they believed the President could ignore the [*356] constitutional and statutory provisions that had long prevented the NSA from engaging in wholesale spying on Americans on American soil. What's clear now, and deeply distressing, is President Obama's embrace of this radical view, rejecting the bedrock principle that the Constitution and the rule of law place limits on Executive power. n27 Despite running on promises to return the country to the proper constitutional balance, President Obama's Justice Department has been pulling out all the stops to block the courts from reviewing the domestic surveillance programs while giving no indication that the surveillance itself has ceased. n28

Con- AT: FISA too slow

The NSA can obtain warrants ex parte, after the fact, and only five out of nineteen thousand were denied.
Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

Even if the government is conducting electronic surveillance, FISA provides two possible procedures that could permit the surveillance. The first procedure n42 is not important from a legal perspective, as the NSA did not seek a warrant for the acquisition of call records. n43 But the decision is perplexing from a strategic perspective, as only five applications out of nineteen thousand have been refused by the Foreign Intelligence Surveillance Court n44 and the government's submission is ex parte. n45 The government most likely did not follow the first procedure, for it believed that the court would not approve a program of the size and scope of the NSA call database. n46 When it was enacted, FISA did not contemplate a program like the call database, which involves millions of people and possibly thousands of targets. n47 Moreover, the Bush administration finds the procedures of FISA too slow to react to the threat of terrorism. n48

Seven out of 20,605 warrants were denied by FISC.
Matt Bedan, JD Indiana Univ Bloomington Law; March 2007 (Federal Communications Law Journal; 59 Fed. Comm. L. J. 425; "Echelon's effect: The obsolescence of the U.S. foreign intelligence legal regime")

Although its membership is made public, the FISC's proceedings and judgments are highly classified. n44 It is known that the FISC meets in a "secret windowless courtroom, sealed from the public by cipher-locked doors on the top floor of the Department of Justice." n45 Proceedings are nonadversarial and entirely ex parte. n46 DOJ attorneys have exclusive access to the FISC judges to present evidence and argue for FISA warrants. n47 When reviewing a FISA application, the presiding judge is explicitly forbidden from second-guessing or otherwise scrutinizing any factual allegation made by the government. n48 If the warrant request is denied, the government can appeal to a three judge panel termed the Foreign Intelligence Surveillance Court of Review. n49 In reality, however, the government's option to appeal is essentially superfluous; in the time since its inception, the FISC has approved 20,605 surveillance applications and denied seven. n50 Conversely, no target of a FISA warrant, U.S. citizen or [*433] otherwise, is allowed to appeal any order of the FISC.

Con- AT: Leaks undermine national security

Leaks do not put specific agents or operations at risk
Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

ALAN RUSBRIDGER: Yeah, they were, they were, they told us why they though we shouldn't publish some things. There were one or two things that were helpful, because we didn't want to go into this behaving irresponsibly or to puts agent at danger or operations. So, I think it was important to have those conversations.
AMY GOODMAN: Edward Snowden also made that a requirement, isn't that true? That people not be exposed.
ALAN RUSBRIDGER: Yes, yes, no, he said, look, you will have to form your own judgment, but I would like you to behave responsibly, and as you say not expose agents or ongoing sensitive operations, for instance, in Afghanistan or Iraq.

Terrorists will not learn anything new from leaked information about NSA domestic surveillance.

Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "On a Slippery Slope to a Totalitarian State": NSA Whistleblower Rejects Gov't Defense of Spying"; http://www.democracynow.org/2013/6/10/on_a_slippery_slope_to_a)

WILLIAM BINNEY: Sure. In my mind, that's a red herring. I mean, it's just a false issue. The point was, the terrorists have already known that we've been doing this for years, so there's no surprise there. They're not going to change the way they operate just because it comes out in the U.S. press. I mean, the point is, they already knew it, and they were operating the way they would operate anyway. So, the point is that they're—we're not—the government here is not trying to protect it from the terrorists; it's trying to protect it, that knowledge of that program, from the citizens of the United States. That's where I see it.

Con- AT: Leaks undermine national security

Key to freedom of press
Chris Hedges, award winning journalist & author; June 12, 2013 (DemocracyNow.Org; "Is Edward Snowden a hero? A debate with journalist Chris Hedges & law scholar Geoffrey Stone"; http://www.democracynow.org/2013/6/12/is_edward_snowden_a_hero_a)

CHRIS HEDGES: Well, what we're really having a debate about is whether or not we're going to have a free press left or not. If there are no Snowdens, if there are no Mannings, if there are no Assanges, there will be no free press. And if the press—and let's not forget that Snowden gave this to *The Guardian*. This was filtered through a press organization in a classic sort of way whistleblowers provide public information about unconstitutional, criminal activity by their government to the public. So the notion that he's just some individual standing up and releasing stuff over the Internet is false.

Law requires institutional memory
Mark Klein, technician @ AT&T for over 20 years & whistleblower; January 9, 2007 (PBS Frontline Interview; "Spying on the home front"; http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html)

You're an ordinary citizen. You're a hardworking guy. You worked 22 years for AT&T. You're talking like a lawyer. What is it that triggered this in you? I mean, you are very direct, very firm. Why?
Why? Because I remember the last time this happened. ... I did my share of anti-war marches when that was an active thing back in the '60s, and I remember the violations and traffic transgressions that the government pulled back then for a war that turned out to be wrong, and a lot of innocent people got killed over it. And I'm seeing all this happening again, only worse. When the [NSA] got caught in the '70s doing domestic spying, it was a big scandal, and that's why Congress passed the FISA [Foreign Intelligence Surveillance Act] law, as you know, to supposedly take care of that. So I remember all that.
And the only way any law is worth anything is if there's a memory so that people can say: "Wait a minute. This happened before." And you've got to step forward and say: "I remember this. This is the same bad thing happening again, and there should be a halt to it." And I'm a little bit of that institutional memory in the country; that's all. ...

Whistleblowing promotes accountability.
Kathleen Clark, Prof Law @ Washington University St. Louis; 2010 (Brigham Young University Law Review; 2010 B.Y.U. L. Rev. 357; "The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program")

Another accountability mechanism, whistleblowing, was also at play in connection with warrantless surveillance. Thomas Tamm, a career Justice Department lawyer who worked in the Office of Intelligence Policy and Review (which processes FISA warrant applications and files them with the Foreign Intelligence Surveillance Court), learned of the existence of the warrantless surveillance program and was concerned about its possible illegality. But he was stymied when he sought additional information about it from his supervisors and when he attempted to inform a congressional staff member about it. In the spring of 2004, he went to a payphone in a Washington subway station and called New York Times reporter, Eric Lichtblau, who co-authored the article that broke the story a year and a half later. n180 Tamm's information about the program was quite limited, but his "cold call" n181 on Lichtblau and their subsequent conversations prompted Lichtblau and his colleague, James Risen, to obtain additional information from other sources, eventually resulting in public disclosure of the program, congressional hearings, statutory reforms, and civil lawsuits over the program.

Con- AT: Meta-Data

No digital communication is secure.
Tim Clemente, former FBI counterterrorism agent; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

TIM CLEMENTE, former FBI counterterrorism agent: On the national security side of the house, in the federal government, you know, we have assets. There are lots of assets at our disposal throughout the intelligence community and also not just domestically, but overseas. Those assets allow us to gain information, intelligence on things that we can't use ordinarily in a criminal investigation.
All digital communications are -- there's a way to look at digital communications in the past. And I can't go into detail of how that's done or what's done. But I can tell you that no digital communication is secure.

Collecting everything, word for word!
Russell Tice, former NSA analyst & whistleblower; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

RUSSELL TICE: Well, two months ago, I contacted some colleagues at NSA. We had a little meeting, and the question came up, was NSA collecting everything now? Because we kind of figured that was the goal all along. And the answer came back. It was, yes, they are collecting everything, contents word for word, everything of every domestic communication in this country.

Meta-data is the index for content, and content is gold for information.
Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

It is technically true that the order applies only to meta-data. The problem is that in the digital space, metadata becomes the index for content. And content is gold for determining intent.

Con- AT: Meta-Data

Content is not the conversation itself.

Andrew P. MacArthur, JD Duke Univ Law; Spring 2007 (Duke Journal of Comparative & International Law; 17 Duke J. Comp. & Int'l L. 441; "The NSA phone call database: The problematic acquisition and mining of call records in the United States, Canada, the United Kingdom, and Australia")

The first legal question is whether the acquisition of call records constitutes "electronic surveillance," [*446] which is defined n35 in § 1801(f)(1) as "the acquisition by an electronic ... device ... of the contents of any wire ... sent by ... a particular, known United States person who is in the United States." n36 Section 1801(n) defines "contents" as "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." n37 Thus, § 1801(n) broad definition covers more than merely the contents of a phone call and extends to the existence of the communication. n38

Implicit in this definition of "electronic surveillance" is that the acquisition must occur in real time. In other words, the collection of historical records would not likely constitute "electronic surveillance." n39 The NSA is probably obtaining real time call records n40 as "it does them no good to have [the telecommunication providers] back up the truck and unload the tapes. It needs a live feed from the server." n41 While it is true that the call records are missing customer identifiable information, such as the caller's name, the NSA could cross-reference those records in a matter of seconds to identify the persons to the communication. The fact that an extra step is required [*447] to identify the person should not allow the government to bypass FISA.

Notwithstanding that the call records do not identify the parties to the communication, the call records do prove that a communication took place and thus would confirm the "existence" of the communication in § 1801(n); accordingly, the NSA would be acquiring "contents" in § 1801(f)(1) and therefore conducting electronic surveillance within the meaning of FISA.

U.S. government shared more than metadata with Israel.

Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

AMY GOODMAN: I mean, raw intelligence is what the U.S. was sharing that *The Guardian* exposed with Israel right, actual phone calls, not only metadata, but — and then saying to Israeli intelligence, you decide what to do with it?
ALAN RUSBRIDGER: That feels to me like a significant story, but I don't want to criticize the judgements of others.

Bluffdale facility proves storing content not metadata.

William Binney, former NSA analyst & whistleblower; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

WILLIAM BINNEY: Well, I don't believe that for a minute. OK?

I mean, that's why they had to build Bluffdale, that facility in Utah with that massive amount of storage that could store all these recordings and all the data being passed along the fiberoptic networks of the world. I mean, you could store 100 years of the world's communications here. That's for content storage. That's not for metadata.

Metadata if you were doing it and putting it into the systems we built, you could do it in a 12-by-20-foot room for the world. That's all the space you need. You don't need 100,000 square feet of space that they have at Bluffdale to do that. You need that kind of storage for content.

Con- AT: Not Listening

Even if they are not listening they could.
Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "Inside the NSA's domestic surveillance apparatus: Whistleblower William Binney speaks out"; http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out)

WILLIAM BINNEY: Well, it's pretty—it's pretty much true, yes. I think they are—my sense is that they are just looking at a target list. They have a target list that they input to the telephone network and use the switches to detect these phone calls going across the network and then download those to recorders and transcribe that. So that's what they're—I think that's what they're doing. But what Edward Snowden was talking about was having access to that network. What that meant was he could load—and what he was basically saying, he could load the attributes of anyone he wanted to target into the target list, and then that would start doing, executing and collecting all the information about them, including the content, and recording it, too. So they could—and someone would have to transcribe it, but they could, and all of that content for phones, as well as email, would be stored and collected in the base.

Con- AT: NSA Good

Despite the NSA's importance there should be checks and balances placed to protect the rights of American citizens.

DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

The NSA is perhaps the most important force protecting the United States from foreign terrorism and other threats to national security. The information provided by the agency informs national security and foreign policy decisionmakers, thereby also playing a vital role in ensuring international peace and security. While the incredible value of this agency cannot be overstated, neither can the risks posed by its vast capabilities. The broad scope of the agency's vigilant efforts has the potential to threaten the legitimate rights of American citizens, and appropriate checks must be in place. n234 FISA provides a well-established legal framework that has protected the rights of American citizens from unwarranted government surveillance since 1978. n235 Although it appears that this framework recently may have been circumvented through a secret executive order, n236 warrantless surveillance of Americans is nothing new. n237 Gaps in our legal protections have existed since FISA's enactment. n238

Con- AT: Oversight/Patriot Act

NSA was subverting the constitution before the Patriot Act authorized surveillance. Court and congressional oversight is a Kabuki dance for show.

Thomas Drake, former senior NSA executive & whistleblower; June 12, 2013 (The Guardian; "Snowden saw what I saw: surveillance criminally subverting the constitution"; http://www.theguardian.com/commentisfree/2013/jun/12/snowden-surveillance-subverting-constitution)

This executive fiat of 2001 violated not just the fourth amendment, but also Fisa rules at the time, which made it a felony – carrying a penalty of $10,000 and five years in prison for each and every instance. The supposed oversight, combined with enabling legislation – the Fisa court, the congressional committees – is all a kabuki dance, predicated on the national security claim that we need to find a threat. The reality is, they just want it all, period.
So I was there at the very nascent stages, when the government – wilfully and in deepest secrecy – subverted the constitution. All you need to know about so-called oversight is that the NSA was already in violation of the Patriot Act by the time it was signed into law.

Congressional oversight is meaningless if the people do not understand the technology.

Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

ALAN RUSBRIDGER: Yes, well, the debate never did happen, did it? Because the instinct of these agencies is always going to be to it as secret as possible and to criminalize people who talk about it. So, that debate didn't happen until Snowden came along. And who is overseeing this and do you trust them? Dianne Feinstein, a great public servant, but does she really understand the finer details of cryptology, and encryption, the capabilities which are expanding exponentially, and can they really match up what the law were intended to do and what engineers are now capable of doing? These are the questions. I think it is not enough just to say, take us on trust we are not doing that, because these secret courts, the FISA courts, we're now learning some of the things that were troubling them that they never made public. And so, it is a lot to take on trust.

Congressional approval does not prove something is constitutional. The Protect America Act is broader than FISA and authorizes warrantless domestic electronic surveillance.

Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

Congress reached a consensus on the eve of its August 2007 recess, approving the Protect America Act of 2007; on August 5, 2007, President Bush signed the bill into law. n22 The Act amended FISA to include intelligence collection procedures similar to, but arguably broader than those permitted by the TSP. n23 Instead of continuing to oppose an NSA-style program like the TSP, Congress sanctioned it. However, that Congress and the President approved the Act does not guarantee that it is constitutional. The Protect America Act's far-reaching provisions permit unconstitutional surveillance of United States citizens, implicating the Fourth Amendment. In some ways the Protect America Act is more constitutionally troubling than was the TSP. Whereas the secretly-established TSP over-extended Executive power, the Protect America Act was passed by a transparent legislative process, and permits unconstitutional domestic surveillance.

Con- AT: Sensationalism

Reporting on NSA surveillance is not sensationalist- they have been careful about what information they published. Surveillance is not just about security so there needs to be a debate that weighs privacy and civil liberty against security.

Alan Rusbridger, editor-in-chief of The Guardian; September 23, 2013 (DemocracyNow.Org; "Spilling the NSA's secrets: Guardian Editor Alan Rusbridger on the inside story of Snowden leaks"; http://www.democracynow.org/2013/9/23/spilling_the_nsas_secrets_guardian_editor)

JUAN GONZÁLEZ: Well, I wanted to read an excerpt from a recent letter sent by the NSA to family members of its employees. The letter, dated September 13the, is signed by NSA Director Keith Alexander and Deputy Director John Inglis. It says, "some media outlets have sensationalized the leaks to the press in a way that has called into question our motives and wrongly cast doubt on the integrity and commitment of the extraordinary people that work here at the NSA/CSS — your loved ones. It has been discouraging to see how our agency frequently has been portrayed in the news as more of a rogue element than a national treasure." I'm wondering, your response to the — I mean, obviously, the allegations of sensationalized reporting allude to *The Guardian* as well as other press outlets.

ALAN RUSBRIDGER: Well, we obviously reject that. I think we have been very careful in our reporting, and actually, the intelligence chiefs, when they speak in private, have been graceful enough to acknowledge that we have been responsible. I can understand why you would write a letter like that. And we are not saying that the people who work inside the NSA are bad people. I imagine they have very talented engineers who are capable of doing extraordinary things. I think what we are saying that there has to be a wider debate because it's not just about national security. There are other interests in society; privacy, civil liberties, of reporting which had to be weighed against security. And so, if you are write about this, you are not saying that the NSA is full of bad people. That would be silly. So, I perfectly understand that you write a letter to the families saying that much of what you do is good and important, which it is.

Con- AT: Terrorism

There's a way to protect against terrorism and preserve U.S. citizens' rights.

Binney, formerly a senior NSA crypto-mathematician largely responsible for automating the agency's worldwide eavesdropping network, one of the two co-founders of the agency's Signals Intelligence Automation Research Center who resigned after the Sept. 11 attacks; June 10, 2013 (William; DemocracyNow.org; "Inside the NSA's domestic surveillance apparatus: Whistleblower William Binney speaks out"; http://www.democracynow.org/blog/2013/6/10/inside_the_nsas_domestic_surveillance_apparatus_whistleblower_william_binney_speaks_out)

WILLIAM BINNEY: Yes. Personally, I've had the view for any—for quite a number of decades, that the Congress and the administration have been—have been fed by the intelligence community what I call technobabble. In other words, they're being bamboozled into thinking a certain way, that they have to do this in order to get terrorists. And that's simply false. There's a simple way to do it that would protect people's privacy and not invade anybody's telephone records or email. And that's to say, if you have a terrorist, and he calls somebody in the United States—I call this the two-degree principle—that's one degree of communication separation. Then you look at that as a target, and you collect that, and then you look also at the person in the United States and who they talk to. That could represent the—that's a zone of suspicion that would, in effect, be basically a support network for that person inside the country. That defines your terrorist relationship, and that's how you look at that. And the rest of the communication of the U.S. people don't mean anything, as relevant, and none of that's relevant to what's going on there. And you also have to look at the jihadi-type sites, those that advocate jihad or violence and so on, and you see who is accessing those sites. That's easy to monitor that, and it doesn't invade anybody's privacy that's been absolutely doing nothing of—that should be in any way considered suspicious.

Surveillance of non-suspected terrorists like former General Colin Powell and Supreme Court justice Samuel Alito.
Russell Tice, former NSA analyst & whistleblower; August 1, 2013 (PBS News Hour; "NSA collects 'word-for-word' every domestic communication, says former analyst"; http://www.pbs.org/newshour/bb/government_programs/july-dec13/whistleblowers_08-01.html)

RUSSELL TICE, former National Security Agency analyst: The United States were, at that time, using satellites to spy on American citizens. At that time, it was news organizations, the State Department, including Colin Powell, and an awful lot of senior military people and industrial types.
JUDY WOODRUFF: So, this is the early 2000s.
RUSSELL TICE: This was in 2002-2003 time frame. The NSA were targeting individuals. In that case, they were judges like the Supreme Court. I held in my hand Judge Alito's targeting information for his phones and his staff and his family.

Con- AT: Terrorism

Surveillance of U.S. Senators like Strom Thurmond.
DAVID ALAN JORDAN, Member DC Bar; May 2006 (Boston College Law Review; 47 B.C. L. Rev 505; "DECRYPTING THE FOURTH AMENDMENT: WARRANTLESS NSA SURVEILLANCE AND THE ENHANCED EXPECTATION OF PRIVACY PROVIDED BY ENCRYPTED VOICE OVER INTERNET PROTOCOL")

Although the scope of the NSA's SIGINT operations has always been the subject of wild speculation, the true number of communications intercepted by the agency has remained a closely guarded secret. Speculation about the number of communications intercepted by the NSA began to grow when rumors of a global signals intelligence network involving multilateral cooperation between several nations began [*511] to surface in 1988. In that year, Margaret Newsham, a former contract employee working at the NSA field station in Menwith Hill, Yorkshire, England, n27 complained to the U.S. House Permanent Select Committee on Intelligence about alleged corruption and impropriety surrounding the use of the NSA's signals intelligence resources. n28 She claimed to have witnessed employees of the agency intercepting a telephone call placed by then-U.S. Senator Strom Thurmond. n29 Her allegations also included details of a global surveillance system known as ECHELON. n30 This fueled public interest and a large number of newspaper articles, but the agency remained silent about the system, and media coverage fizzled shortly thereafter. n31

The NSA is not just listening to terrorists who call people in the U.S. They are monitoring the Internet and domestic-to-domestic communication.
Mark Klein, technician @ AT&T for over 20 years & whistleblower; January 9, 2007 (PBS Frontline Interview; "Spying on the home front"; http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html)

Much later the president comes out and says, you know, we're just monitoring Al Qaeda communications with America, and we're following specific calls, and we're trying to track terrorists. How do you know that it isn't what they say it is; that the Narus or some other piece of equipment isn't just targeted in on 50 individuals in this area, and all those billions of pieces of data are just flowing off into the ether?
... The administration's first presentation of it is disingenuous. They present it as about phone calls. They're just watching a few bad people who make phone calls to Al Qaeda and the Middle East, and you notice they don't talk about the Internet hardly at all. That part of it hasn't been revealed, because if they did, Americans would realize it's not just a few people; it's everybody, because the data they're handing over is not selected out. When you run fiber optics through a splitter and you send all that data to a secret room, there's no selecting going on there at all. ...
And they could be getting domestic-to-domestic [communications]?
That's right. They have no way of sifting it out unless they look through it later. Now they can claim, "Oh, we are right as rain; we're only doing the legal thing and selecting out a few people that we're legally entitled to," but that's only after they get all the data. The analogy I use: If the government claims, "Well, when you do your taxes, why don't you just write me a blank check and we'll fill in the amount? Don't worry. We'll do it legal. We'll fill in the right amount," would you do that? Nobody would trust the government by writing a blank check to them. It's the same thing with the data we're giving them. ...
When the founders wrote the Fourth Amendment, they had a specific antagonism against what were called general warrants, as you might know. General warrants is when the British troops would come in with a warrant and say: "We have the right to search your house. We're looking for something. Looking for what? We can't tell you. We're going to ransack your house." That's a general warrant. They can turn your life upside down, and the colonialists [sic] hated that. So the Fourth Amendment specifically bans general warrants. It calls for specific warrants in which the things to be seized and the persons to be seized are specifically named. There's a reason for that. It's to protect against arbitrary government power. And what they've done is to trample over the Fourth Amendment by basically instituting a general warrant on the Internet.

Con- AT: Terrorism

The government has information that could have prevented 9/11. The war on terror is an excuse for aggrandizing power for power's sake.
Mark Klein, technician @ AT&T for over 20 years & whistleblower; January 9, 2007 (PBS Frontline Interview; "Spying on the home front"; http://www.pbs.org/wgbh/pages/frontline/homefront/interviews/klein.html)

... There were terrorists who were living among us prior to 9/11. They were moving around; they were going to flight schools; they were renting apartments; they were traveling around. Doesn't the government need to do something in terms of gathering information to try to prevent the next terrorist attack?
I think if they needed anything, they had it already on the books. There's lots of -- maybe too much -- leeway for surveillance as it is. And they had lots of information that 9/11 was going to happen. But for some strange reason, they didn't act.
So I think you're asking this government -- which is full of prevarications and misleading statements and not very truthful and also a large component of simply incompetence -- handing them the keys to everybody's private information. I don't trust them with that. I think they're far more interested in just aggrandizing power for power's sake, and they're just using it as an excuse -- the so-called war on terror, which is their excuse for everything they do. Everything is aggrandizing power secretly, with no oversight. And I'm against that. It's dangerous. ...

Protect America Act does not even require suspicion of terrorism for warrantless domestic electronic surveillance.
Emily Arthur Cardy, Melville M. Bigelow Scholarship Award winner @ Boston University Law School; Fall 2008 (Boston University Public Interest Law Journal; 18 B.U. Pub. Int. L.J. 171; "THE UNCONSTITUTIONALITY OF THE PROTECT AMERICA ACT OF 2007")

Neither the Protect America Act nor FISA define the term "concerning," therefore common usage is appropriate. The Oxford English Dictionary defines "concern" as "to distinguish, discern, perceive" or "to have relation or reference to; to refer to, relate to; to be about." n128 Using the common meaning of "concerning" to interpret the Protect America Act demonstrates that the information collected through the Act need only be about or with reference to a foreign target. For example, if Sally in Toledo were talking to George in Austin about their cousin, Jean, who was on vacation in Germany, the Protect America Act permits intelligence agencies to "collect" this conversation without a warrant. The only thing that the government needs to know before proceeding [*190] with the collection is that the communication is about Jean, whom they reasonably believe to be outside of the United States. Contrary to administration and congressional statements, n129 the statute does not even require the government to suspect the subject of the conversation (Jean, in the example) of terrorist activities or of being a threat to national security. n130

Con- AT: Terrorism

NSA surveillance not as effective as claimed. Traditional law enforcement tools more important.
Peter Bergen, Director National Security Project @ New America Foundation, fellow Fordham Univ Center National Security, Bruce Hoffman, Prof Georgetown School Foreign Service, Michael Hurley, President Team 31 & advisor Bipartisan Policy Center's Homeland Security Project, & Erroll Southers, Assoc Director Research, Dept Homeland Security's National Center for Risk & Economic Analysis of Terrorism Events, & Adjunct Prof Sol Price School Public Policy @ Univ Southern California; September 2013 (Bipartisan Policy Center; "Jihadist terrorism: A threat assessment"; http://bipartisanpolicy.org/library/report/jihadist-terrorism-threat-assessment)

The public record suggests that few of these plots involved attacks within the United States, because traditional law enforcement methods have overwhelmingly played the most significant role in foiling terrorist attacks. According to a survey by the New America Foundation, jihadist extremists based in the United States have mounted 47 plots to conduct attacks within the United States since 2001.[326]
Of those plots, nine involved an actual terrorist act that was not prevented by any type of government action, such as the 2009 shooting spree at Fort Hood, Texas. Of the remaining 38 plots, the public record shows that at least 33 were uncovered by using standard policing practices such as informants, undercover officers, and tips to law enforcement.