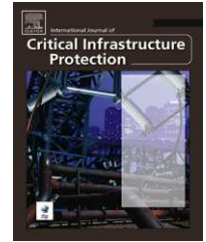


available at [www.sciencedirect.com](http://www.sciencedirect.com)journal homepage: [www.elsevier.com/locate/ijcip](http://www.elsevier.com/locate/ijcip)

# May the US government monitor private critical infrastructure assets to combat foreign cyberspace threats?

Mason Rice, Robert Miller<sup>1</sup>, Sujeet Shenoj\*

Department of Computer Science, University of Tulsa, Tulsa, Oklahoma 74104, USA

## ARTICLE INFO

### Article history:

Received 6 October 2010

Accepted 11 February 2011

Published online 18 February 2011

### Keywords:

Critical infrastructure

Threats

Government monitoring

Legal issues

## ABSTRACT

The government “owns” the entire US airspace—it can install radar systems, enforce no-fly zones and interdict hostile aircraft. Since the critical infrastructure and the associated cyberspace are just as vital to national security, could the US government protect major assets—including privately-owned assets—by positioning sensors and defensive systems? This paper discusses the legal issues related to the government’s deployment of sensors in privately owned assets to gain broad situational awareness of foreign threats. This paper does not necessarily advocate pervasive government monitoring of the critical infrastructure; rather, it attempts to analyze the legal principles that would permit or preclude various forms of monitoring.

© 2011 Elsevier B.V. All rights reserved.

## 1. Introduction

In the early 1960s, the United States ringed major population centers and strategic assets with radar systems and Nike missile batteries—the Chicago Defense Area alone had 22 batteries [1]. The Nike missiles were deemed vital to combat the Soviet bomber threat. Fifty years later, the US critical infrastructure faces potentially serious threats from cyberspace. The most credible threats come from nation state actors, especially military and intelligence services.

The critical infrastructure and the associated cyberspace are vital to national security. On May 21, 2010, America established the US Cyber Command to safeguard Department of Defense (DoD) cyberspace assets and to ensure freedom of action in cyberspace while denying the same to adversaries [2]. However, Cyber Command’s charter does not appear to cover non-DoD assets.

More than 85% of the US critical infrastructure is in private hands [3]. At this time, the task of protecting these critical infrastructure assets and the associated cyberspace is left to

owners and operators, with regulatory oversight and limited technical assistance from government entities. The current environment is similar to a scenario where the radar systems and Nike batteries of the Cold War only protected military facilities. Indeed, to paraphrase Clarke and Knake [4], it is as if the Pentagon told US Steel and General Motors to purchase their own Nike missiles to protect themselves.

The nature of the critical infrastructure demands that cyberspace protection efforts be comprehensive to the extent possible. How can Cyber Command effectively secure military networks when operating them requires electricity, gas and telecommunications, which are often supplied by private sector entities whose assets may or may not be secure? Because of the strong interdependencies that exist between the critical infrastructures, a failure in one infrastructure would cause cascading failures in the other infrastructures. Clearly, it is unwise to only protect islands in cyberspace.

This paper considers a controversial question—to provide more comprehensive protection to critical infrastructure assets and the population centers they support, could the

\* Corresponding author.

E-mail address: [sujeet@utulsa.edu](mailto:sujeet@utulsa.edu) (S. Shenoj).

<sup>1</sup> Information Resources Management College, National Defense University, Fort Lesley McNair, Washington, District of Columbia 20319, USA.

1874-5482/\$ - see front matter © 2011 Elsevier B.V. All rights reserved.

doi:10.1016/j.ijcip.2011.02.001

US government ring major cyberspace assets with sensors and defensive systems? In particular, the paper discusses the legal issues related to the government's deployment of sensors in privately owned assets to direct security and mitigation efforts. Three scenarios with increasing levels of intrusiveness are presented to focus and clarify the legal issues.

---

## 2. Government monitoring

Two prime examples of government monitoring are the North American Aerospace Defense Command (NORAD) and the US Nationally Notifiable Diseases Surveillance System (NNDSS). The systems demonstrate two distinct government monitoring philosophies.

NORAD's Air Warning Center (AWC) is under the command and control of the US and Canadian military [5,6]. The AWC incorporates an array of radar systems to monitor approximately 5000 aircraft flying within or entering US and Canadian airspace. It detects, validates and issues warnings of attacks by aircraft, missiles or space vehicles.

The NNDSS, on the other hand, is a decentralized surveillance system for infectious diseases that is implemented at the grassroots level [7]. Private healthcare providers and state and local health agencies pass potential cases to the appropriate state health department for investigation. Cases of infectious diseases are reported to the Centers for Disease Control and Prevention (CDC), which takes the appropriate actions.

As with airspace protection and disease containment, monitoring critical infrastructure assets is vital to achieving robust protection. Monitoring provides situational awareness of the health and well-being of infrastructure assets. Monitoring facilitates the analysis of security breaches and supports the design and implementation of new defensive measures.

Currently, the monitoring of the cyberspace components of the critical infrastructure is performed in a highly decentralized manner. More than 85% of the US critical infrastructure assets are privately owned and operated [3]. Entities in key sectors such as energy, telecommunications, and banking and finance, are regulated by government agencies and/or industry bodies (e.g., North American Electric Reliability Council (NERC) for bulk power systems). However, limited regulations are in place for cyberspace security. Monitoring is complicated by the fact that the private actors range from small companies to multinational corporations. The private actors differ greatly in their use of technology, awareness of threats and vulnerabilities, and availability of trained personnel and resources. Monitoring activities vary in their scope, precision, accuracy and timeliness. The detection and reporting of cybersecurity breaches are haphazard at best.

Because of the interconnectivity of assets within a sector and the interdependencies existing between sectors, it is important that the monitoring and reporting of security breaches in the infrastructure as a whole be substantive and comprehensive to the extent possible. The current structure and procedures, while decentralized, do not approach the levels of those used by the NNDSS for infectious diseases.

The Comprehensive National Cybersecurity Initiative (CNCI) is a key step [8]. One of its goals is to facilitate shared

situational awareness of network vulnerabilities, threats and incidents by deploying sensors across the federal enterprise. Additionally, it recommends that the Department of Homeland Security work with private sector entities on a shared action plan for extending cybersecurity to the critical infrastructure. However, even if the decentralized structures and procedures were to be enhanced, one might posit that infrastructure monitoring would not improve significantly. The most compelling argument is that serious attacks are typically launched by the military and intelligence services of nation states; even multinational corporations may not have the technology and expertise to detect sophisticated attacks. Furthermore, it is unreasonable to expect that all private sector entities – given the rollercoaster economy and the focus on shareholder value – would have the ability and resources to perform robust monitoring of their infrastructure assets.

A case can, therefore, be made for substantive and comprehensive government monitoring of the cyberspace components of the critical infrastructure, similar to NORAD's monitoring of US airspace. Such monitoring would have to be administered by a federal entity such as the Department of Homeland Security because many infrastructure assets (e.g., power grids, pipelines and telecommunications networks) span state boundaries, which limits the ability of state and local governments to conduct monitoring.

---

## 3. Constitutional authorities

The Constitution is the supreme law of the United States. It separates federal powers into the executive branch led by the President; the legislative branch comprising the House and Senate (Congress); and the judicial branch where the Supreme Court is the final arbiter. Each branch is independent, but subject to restraint by the other branches through a complex system of checks and balances. The Constitution also establishes the framework for the federal government's relationship with the states and the people.

This section describes some of the principal authorities granted by the Constitution to Congress and to the President with respect to regulatory powers as interpreted by the Supreme Court. These regulatory powers are relevant to any legal discussion of government monitoring of critical infrastructures.

### 3.1. Congressional power

The Commerce Clause of the Constitution arguably provides the most significant authority for regulatory actions by the federal government. For almost two centuries, the scope of federal commerce power has been a source of controversy. Nevertheless, current regulatory agencies, such as the Federal Energy Regulatory Commission (FERC) and the Federal Communications Commission (FCC), base their authority on the commerce power.

Gibbons vs. Ogden [9] in 1824 was an early landmark Supreme Court case that defined the scope of the Commerce Clause. In this case, the Court ruled that ferryboat traffic between New York and New Jersey constituted interstate commerce and was, therefore, subject to federal regulation [10]. However, Marshall noted that any trade that

was purely within a state would not be subject to federal regulation.

The case of *Wickard vs. Filburn* [11] in 1942 changed the scope of the federal commerce power [10]. Federal agents penalized Farmer Filburn, who was growing wheat in excess of a federal quota, despite the fact that his wheat was only used to feed his family and livestock. The Supreme Court found that federal regulatory power extended to Farmer Filburn's wheat growing because his production, while trivial in quantity and not sold into commerce, impacted the national aggregate supply and demand for wheat, and, thus, interstate commerce to a sufficient degree, to justify federal regulation.

Since *Wickard vs. Filburn*, the Supreme Court has not struck down a federal law regulating economic activity on the grounds that the law exceeded Congress's Commerce Clause power, no matter how minimal or local the economic activity [10]. After *Wickard* and similar opinions [10], the federal regulatory apparatus and its reach grew significantly, leading to the establishment of several regulatory agencies (e.g., FERC).

In the 1960s and 1970s, the federal commerce power was used to regulate non-economic matters based on their impact on interstate commerce [10]. For example, in 1964, the Supreme Court upheld the Civil Rights Act as a proper exercise of federal commerce power in *Katzenbach vs. McClung* [12]. The Court has also held federal environmental laws to be proper exercises of Commerce Clause power.

The Supreme Court has established three general categories in which federal regulation based on the Commerce Clause is authorized: (i) to regulate the use of the channels of interstate commerce; (ii) to regulate and protect the instrumentalities of interstate commerce even if the threat comes only from intrastate activities; and (iii) to regulate activities having a substantial relation to interstate commerce.

The first two categories are likely not controversial because they fit within the text and history of the Commerce Clause. The third category, however, which has been used to justify federal regulatory power since the 1940s, is very controversial, especially outside the context of economic regulation and for activities that are local in nature.

The Supreme Court's interpretation of the activities that have a substantial effect on interstate commerce underwent a notable change in 1995 with the case of *US vs. Lopez* [13]. In the *Lopez* case, the Court struck down the criminal conviction of a youth who had violated a federal law by bringing a gun to school. Chief Justice Rehnquist, writing for a narrow majority, held that the law exceeded the federal commerce power because the act of bringing a gun to school neither involved any channels or instrumentalities of interstate commerce nor affected interstate commerce in a substantial manner.

In 2000, the Supreme Court struck down provisions of the Violence Against Women Act of 1994 in the case of *US vs. Morrison* [10,14]. The case involved a female student at Virginia Tech who alleged that she had been raped in a dorm room by a member of the football team. She initiated a civil action in federal court against her assailant as authorized by the Violence Against Women Act. However, the Supreme Court, following its reasoning in *US vs. Lopez*, ruled that the federal law exceeded the commerce power. The Court

declared the case was a matter for the state's general police power, not federal law.

After placing limits on commerce power in the 1990s, the Supreme Court's interpretation of the Commerce Clause expanded in 2005. In *Gonzales vs. Raich* [15], a six-member majority of the Supreme Court refused to uphold California's medical marijuana law. Surprisingly, Justice Scalia, given his earlier views about a limited Commerce Clause, voted to allow the federal law to override the state law [10]. Scalia said that the federal law in this case was part of a comprehensive nationwide scheme to regulate certain controlled substances and, under the Necessary and Proper Clause of the Constitution, Congress had the power to override state laws that could frustrate a federal regulatory scheme exercising the commerce power. Scalia distinguished the *Lopez* and *Morrison* cases by saying that, unlike the regulation of controlled substances on a national basis, the federal laws at issue in the *Lopez* and *Morrison* cases were not proper exercises of federal commerce power. Scalia's opinion has major ramifications should Congress enact legislation authorizing the government to monitor critical infrastructure assets.

### 3.2. Executive power

In January 2008, the Bush Administration established the CNCI by a classified presidential directive [16]. CNCI's authority – like any other executive action – is based on statutory or constitutional law. Several legal authorities provide the basis for executive actions that respond to cyber threats. These include various criminal code provisions that establish federal cyber crime offenses and authorize prosecution; statutes such as the Federal Information Security Management Act (FISMA), which directs executive agencies to establish specific administrative procedures to protect against cyber attacks; general statutes authorizing executive management of federal agencies; and executive powers inherent in the Commander-in-Chief Clause and other constitutional provisions.

Most criminal provisions are reactive in nature. They generally do not authorize preventative measures to defend against cyber threats, and jurisdictional and practical hurdles often hamper law enforcement investigations of foreign hackers [16]. In contrast, FISMA and related statutes take a proactive approach to dealing with cyber intrusions. Statutes related to the executive management of the civil service can authorize changes to government Internet portals and changes in agency personnel, but they do not explicitly cover cybersecurity issues.

The President's foreign affairs powers may provide an inherent constitutional authorization for executive actions related to cybersecurity [16]. Given the nature of cyberspace, it is difficult to distinguish between foreign and domestic affairs. Thus, the President's oath-based obligation to defend the nation from imminent threats offers a constitutional basis for executive action to defend against cyber threats.

US jurisprudence does not prevent the President from taking action in cyberspace (at least until Congress takes further action). Congress and the President can address matters of national security, but no precise line divides the

powers of the two branches [16]. Scholars have identified a narrow sphere of Article II (executive) authority, sometimes called “preclusive power” that congressional action cannot limit. However, in most situations, Justice Jackson’s 1952 opinion in *Youngstown Sheet & Tube Co. vs. Sawyer* [17] establishes the doctrine governing the executive branch’s constitutional authority vis-a-vis Congress.

This landmark case, known as the Steel Seizure Case, considered if the President, as Chief Executive and Commander-in-Chief, has the power to act in a lawmaking capacity in an emergency situation. In the Steel Seizure Case, the government claimed that presidential powers inherent in the Article II provisions authorized President Truman to seize production facilities and operate them under federal direction [16]. The government characterized the seizure as the action of a Commander-in-Chief prompted by the fact that steel production was vital for military operations in Korea. The Supreme Court rejected this claim because it was not within the constitutional system to hold that the Commander-in-Chief of the armed forces has the ultimate power to seize private property in order to keep labor disputes from stopping production.

In the same case, Jackson argued that the President’s inherent constitutional powers “fluctuate”, from relatively high powers when authorized by Congress to their “lowest ebb” when the President “takes measures incompatible with the express or implied will of Congress” [16]. Specifically, Jackson articulated three categories of executive action: (i) action supported by an express or implied grant of authority from Congress; (ii) a “zone of twilight” between the other categories, in which “congressional inertia” can occasionally “enable, if not invite, measures on independent presidential responsibility;” and (iii) action that conflicts with statutes or congressional intent. Under Jackson’s framework, the President and Congress may have concurrent authority related to the second category, but it is not always clear what, if any, power one branch has to supersede actions of the other. Jackson found that President Truman’s actions fit within the third category because Congress had not left the issue of property seizure during labor disputes to an “open field” [16]. Maintaining that Congress had previously passed statutes to stabilize markets when the government required supplies, Jackson joined the majority to strike down President Truman’s seizure of the steel industry.

## 4. Principal legal issues

This section discusses the legal authorities and interpretations associated with specific congressional and executive actions pertaining to: (i) regulatory takings (eminent domain); (ii) surveillance; (iii) privacy; and (iv) non-disclosure (national security letters). These four issues have significant ramifications with regard to the government’s monitoring of critical infrastructure assets.

### 4.1. Regulatory takings

In April 2010, the owners of Rainville Dairy Farm in Vermont were told that the US Customs and Border Protection Agency wanted their hayfield on the Canadian border for reasons of

national security and that, if they did not accept the offer of \$39,500, the US Government would use the power of eminent domain to seize the property [18].

The Takings Clause in the Fifth Amendment allows the government to exercise eminent domain if: (i) the taking is for a public use and (ii) the property owner is paid fairly for the property [10]. However, even with the public purpose limitation on eminent domain, the government, in its judicial or legislative capacity, can and has interpreted the notion of public purpose very broadly [19].

The initial determination of public purpose is typically a legislative decision [19]. However, the courts have the final authority to decide the extent of control over private property based on whether or not the legislative determination of public use is permitted. This final authority is exercised with great deference to the legislature, resulting in considerable legislative power to seize private property for various purposes.

There are two aspects of regulatory takings [20]. The first is eminent domain for “public use”. The second arises when the government does not formally use eminent domain, but still regulates the use of private property—this may force the property owner to sue to establish the “taking” and obtain compensation.

Until the 1920s, the Takings Clause was considered to be applicable only to direct government expropriation of private property [10]. This view was expanded in the landmark 1922 case of *Pennsylvania Coal Company vs. Mahon* [21], when the Supreme Court established the concept of a “regulatory taking”. In a regulatory taking, the original property owner holds the title to the property. However, if the government regulation so impacts the owner’s right to use the property or diminishes its market value, then the regulation is held to be a *de facto* taking. In *Pennsylvania Coal Company vs. Mahon*, the Supreme Court struck down the regulatory taking of property because the public purpose involved was not sufficient to justify the property value reduction suffered by the coal company [22].

In 1987, the Supreme Court clarified the definition of “regulatory taking” in the case of *Keystone Bituminous Coal Association vs. DeBenedictis* [23]. In this case, the Keystone Bituminous Coal Association petitioned a US District Court to enjoin the Pennsylvania Department of Environmental Resources to enforce the state’s Subsidence Act. Relying on the Supreme Court decision in *Pennsylvania Coal Company vs. Mahon*, the coal association’s primary argument was that the Subsidence Act violated the Takings Clause because the property was confiscated without providing fair compensation. According to the act, coal mining must preserve at least 50% of the coal *in situ* to prevent subsidence damage to buildings and other structures. The issue was if the Subsidence Act was used to effectively seize the coal association’s property without fair compensation. The Supreme Court stated that, unlike the *Pennsylvania Coal* case, the Subsidence Act served genuine, substantial and legitimate public interests related to the health, environment and fiscal integrity of the area. The Court reasoned that since no part of the act was solely for the benefit of private parties (as in the *Pennsylvania Coal* case), the legislation was not a regulatory taking and that it sought to prevent activities that were tantamount to public nuisances.

There has been little controversy when eminent domain is used for a public highway or on behalf of a state-regulated public service corporation [10]. Major controversy occurs, however, when the public use requirement is in question. The meaning of public use rose to prominence in the 2005 case of *Kelo vs. City of New London* [24], when the Supreme Court held that the condemnation of private land for transfer to another party could be a public use if it is a part of an area-wide redevelopment plan that does not favor any private party.

In 2006, following the *Kelo* decision, President Bush issued Executive Order 13406 stating that it is United States policy to protect the private property rights of Americans. This includes limiting the taking of private property by the federal government to situations where the taking is for public use, with just compensation, and for the purpose of benefiting the general public and not merely for advancing the economic interest of private parties [25].

However, there are specific exemptions to this order. These include projects designated for public, common carrier, public transportation or public utility use that serve the general public and are subject to regulation by a governmental entity; conveying property to a non-governmental entity (e.g., a telecommunications or transportation common carrier) that makes the property available for use by the general public as of right; preventing or mitigating a harmful use of land that constitutes a threat to public health, safety or the environment; acquiring ownership or use by a public utility; and meeting military, law enforcement, public safety, public transportation or public health emergencies.

#### 4.2. Surveillance

Presidents since Franklin Roosevelt have claimed the right to conduct warrantless electronic surveillance in matters involving national security. Each successive administration broadened this “amorphous national security exception” to the warrant requirement of the Fourth Amendment [26]. Public concern about surveillance ultimately led to the enactment of the Foreign Intelligence Surveillance Act (FISA) in 1978.

FISA created the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR) to provide judicial oversight [27]. An agency seeking to perform foreign intelligence surveillance within the United States must apply for a FISA order from a FISC judge. If the order is denied, the agency may file an appeal with the three-judge FISCR panel. Various congressional committees provide legislative oversight over the FISA application and review processes.

The courts have held that FISA balances the government's need to gather national intelligence information and the Fourth Amendment rights of individuals [26]. Key cases include *US vs. Falvey* [28] and *US vs. Duggan* [29]. Since the government's interest in gathering intelligence information is different from that for a criminal investigation, the courts have ruled that the standard of probable cause for a FISA order passes constitutional muster, even if it may not meet the standard of probable cause for a criminal investigation wiretap.

In 1980, a US Court of Appeals, in deciding the case of *US vs. Truong Dinh Hung* [30], which began before FISA was

enacted, noted that, while FISA suggests that the executive branch may conduct some types of foreign intelligence surveillance subject to a warrant requirement, the statute allows the imposition of a warrant requirement beyond the constitutional minimum to a legislative process involving Congress and the President. The *US vs. Falvey* and *US vs. Duggan* cases also supported electronic surveillance for foreign intelligence purposes without a warrant.

In the 1982 case of *US vs. US District Court* (“Keith case”) [31], the Supreme Court held that there is no warrant exception for “domestic security” surveillance, and explicitly stated that it did not consider issues related to activities of foreign powers or their agents. Years later, in the 2000 case of *US vs. Usama Bin Laden* [32], the government argued that surveillance targeting an agent of a foreign power does not require a warrant; however, the Supreme Court has yet to resolve this issue. The circuit courts that have applied the Keith case to the foreign intelligence context have affirmed a foreign intelligence exception to the warrant requirement for domestic searches that target foreign powers or their agents.

Responding to the 9/11 terrorist attacks, Congress passed the PATRIOT Act of 2001 that amended FISA and expanded the purposes for which surveillance could be conducted [27]. The original FISA (1978) authorized a FISA order only if the “primary purpose” was to obtain foreign intelligence information. On the other hand, the amended FISA permits an order if a “significant purpose” is to obtain foreign intelligence information. In a sealed case heard by FISCR in 2002, the court held that the amended FISA did not violate the Fourth Amendment [26].

The 2007 Protect America Act (PAA) granted authority to the US Attorney General and Director of National Intelligence to conduct surveillance of persons located outside the United States for one year without a FISA order. According to PAA, it is only necessary to provide the FISA court with a sealed certification that the criteria for a warrant are met along with a declaration that a significant purpose of the surveillance is to obtain foreign intelligence information.

A controversy arose in 2005 when the National Security Agency (NSA) collected foreign intelligence information from telecommunications companies via an executive order [27]. In particular, several telecommunications companies cooperated with the NSA in monitoring private communications from September 11, 2001, to January 17, 2007. The companies did not receive FISA orders, but were told that the Attorney General had approved the program. The controversy arose because it is not clear if private corporations may provide assistance without a FISA order or other explicit authorization.

The FISA Amendments Act of 2008 addresses surveillance conducted under the PATRIOT Act and PAA, and establishes procedures for authorizing certain acquisitions of foreign intelligence [27]. The amendments address the ability of the President to conduct surveillance as necessary and the requirement of telecommunications companies to conduct surveillance based on a presidential directive. Two main differences exist between the PAA and the FISA Amendments Act. First, the PAA states that the Attorney General and Director of National Intelligence may issue surveillance orders independently, while the FISA Amendments Act requires that the authority to provide surveillance orders must be exercised jointly. Second, the FISA Amendments Act

limits the targets for surveillance whereas the PAA is silent about this issue.

Congress has drafted other legislation related to electronic surveillance (e.g., Electronic Communications Privacy Act, Stored Communications Act and Wiretap Act). These acts are relevant to criminal investigations, not domestic intelligence surveillance.

The FISA has withstood other constitutional attacks. Courts have ruled that the FISA provisions are not “overbroad” so as to infringe on an individual’s First Amendment rights because the statute forces the government to meet specific standards before a surveillance order can be obtained [26]. The courts have also held that the different treatment of non-resident aliens as opposed to US persons is rationally related to the legitimate goal of protecting the United States from attack by foreign powers and to gather intelligence information and, therefore, does not deprive the non-resident alien of the right to equal protection under the law. Finally, the courts have held that FISA surveillance does not deprive a target of assistance from counsel.

#### 4.3. Privacy

The Constitution does not expressly grant a right of privacy. However, in the 1965 case of *Griswold vs. Connecticut* [33], the Supreme Court established a legal precedent known as the “zone of privacy” [34]. The court reasoned that individual privacy can be found in other constitutional protections such as the First Amendment’s guarantee of freedom of association and the Fourth Amendment’s protections against unreasonable search and seizures. The zone of privacy is the right of a person and his/her property to be free from unwarranted public scrutiny or exposure [35].

In his 1967 concurrence in *Katz vs. US* [36], Supreme Court Justice Harlan wrote that reasonableness is defined by the individual’s subjective expectation of privacy and by an objective expectation that society recognizes as reasonable [37]. The Court continues to apply this test to determine what is private under the Fourth Amendment.

The Supreme Court has refused to extend the Fourth Amendment to restrict government access to data held by third parties [37]. In the 1976 case of *US vs. Miller* [38], the Court held that a reasonable expectation of privacy does not exist for information held by a third party, even if the third party possesses it as a result of a legal obligation. Thus, the Fourth Amendment does not apply to the government’s seizure of private data [37].

In 1979, the Supreme Court reinforced its *Miller* case ruling in *Smith vs. Maryland* [39], which concerned information about telephone calls (not call content). The Court ruled that the Fourth Amendment is inapplicable to telecommunications data (e.g., dialed number, time of call and call duration) because they are necessarily available to the third parties that process the call [37]. Therefore, the use of pen registers to record outgoing call information and trap and trace devices to record incoming call information do not require a warrant because the information collected is necessarily disclosed to others [37].

During the past 20 years, the Supreme Court has rarely agreed with Fourth Amendment challenges to the use of new technologies to capture information, and all these

cases involved intrusions into the home [37]. Indeed, with the exception of physical searches inside the home, the Court is more likely to reduce, rather than preserve, Fourth Amendment privacy protections.

The Supreme Court’s decision to exempt third-party records from Fourth Amendment protection does not mean that the records are available to the government [37]. Congress has adopted several statutes that protect the privacy of personal information. For example, the Electronic Communications Privacy Act of 1986 regulates electronic surveillance [37], and the Pen Register Act controls the use of pen registers and trap and trace devices. The government requires a court order to obtain information similar to that contained in a phone bill or that is revealed by the caller ID feature, or to capture e-mail header information or the IP address of a site visited on the Internet. A court will issue an order only if the government certifies that the information is relevant to a criminal investigation.

The Privacy Act of 1974 is the broadest federal privacy law and represents the earliest effort by Congress to regulate the collection and use of personal information by the government [37]. Among other things, this act prohibits the disclosure, even to other government agencies, of personally identifiable information without the written consent of the subject or pursuant to a specific exception.

The Computer Matching and Privacy Protection Act of 1988 provides a series of procedural requirements (e.g., written agreements between agencies that share data) before an agency can disclose personal information obtained by data mining [37]. These requirements deal only with federal agencies that supply (not obtain) records for data mining. Note that the act does not cover data mining used for purposes of law enforcement, foreign counterintelligence and background checks.

The growing use of sophisticated surveillance technologies is raising difficult constitutional questions related to privacy. In August 2010, a US Court of Appeals overturned a drug trafficking conviction because evidence pertaining to the defendant’s whereabouts was obtained from a GPS receiver that the police hid under his vehicle without a warrant [40]. Traditionally, the courts have held that the Fourth Amendment does not cover tracking a suspect because there is no expectation of privacy for public actions. But the appeals court stated that individuals expect their overall movements to be private because strangers see only isolated portions of their movements. In fact, the judge noted that prolonged surveillance (as with a GPS device) yields information that is not revealed by short-term surveillance, such as what the person does repeatedly, what the person does not do, and what the person does as an ensemble.

#### 4.4. Non-disclosure

The First Amendment protects the freedom of speech. However, for nearly two decades, various statutes have authorized federal agencies, typically the Federal Bureau of Investigation (FBI), to issue national security letters (NSLs) to individuals and organizations to surrender certain records and refrain from disclosing the request [41]. The NSLs may owe much of their success to the secrecy surrounding them. Under the authorizing statutes, the first of which was passed

in 1978, a recipient cannot disclose to “any person” the fact that he/she has received an NSL. A recipient potentially breaks the law by informing his attorney about the letter.

Five federal statutes currently authorize intelligence officials to request business records in connection with national security investigations [42]. The authority to issue an NSL is comparable with the authority to issue an administrative subpoena. The most common statement of purpose of an NSL is “to protect against international terrorism or clandestine intelligence activities” [42]. One of the statutes, the Fair Credit Reporting Act, allows an NSL to be used by an intelligence agency for an investigation, activity or analysis. Another statute, the National Security Act, permits NSLs for law enforcement investigations, counterintelligence inquiries and security determinations. The PATRIOT Act expanded the authority under four earlier NSL statutes and enacted a fifth statute that created a judicial enforcement mechanism and a judicial review procedure for the requests and accompanying non-disclosure requirements, and, among other things, clarified that the non-disclosure requirements did not preclude a recipient from consulting an attorney.

Prior to their amendment in 2006, the NSL statutes generally featured an open-ended confidentiality clause [42]. The statutes did not indicate if a recipient could consult an attorney to ascertain his rights and obligations or if it might ever be lifted. The early court cases found this silence in the face of a seemingly absolute, permanent non-disclosure command to be constitutionally unacceptable. The current NSL statutes do not require absolute secrecy. Instead, NSL recipients are bound to secrecy only upon the certification of the requesting agency that the disclosure of the request or response may impact national security, may interfere with diplomatic relations or with a criminal, counterterrorism, or counterintelligence investigation, or may endanger the physical safety of an individual. A recipient may disclose the request to attorneys and to individuals who help comply with the request.

In the 2008 case of *Doe vs. Mukasey* [43], a US Court of Appeals found that the non-disclosure requirement of NSLs that request records from providers of wire or electronic communication services applies only when senior FBI officials certify that the disclosure may harm investigations of international terrorism or clandestine intelligence activities [43]. The court also declared that it was beyond the authority of court to interpret or revise NSL statutes to create the constitutional obligation of the government to initiate judicial review of a non-disclosure requirement.

In October 2009, a US District Court concluded in *Doe vs. Holder* [44] that the government must provide more than a conclusory assurance that a likelihood of harm from disclosure exists in order to satisfy its First Amendment burden and demonstrate a reason for compliance with a non-disclosure order. Furthermore, the court stated that in order to uphold a non-disclosure order as constitutional, the government must demonstrate that good reasons exist to believe that disclosure of the NSL or the recipient’s identity could harm an ongoing investigation of international terrorism or clandestine intelligence activities, that the link between disclosure and harm is substantial and that no less restrictive alternatives are as effective.

When reconsidering *Doe vs. Holder* [45] on March 18, 2010, a US District Court declared that an information disclosure sought by the FBI via NSL that requires an Internet service provider to produce customer records does not infringe on the service provider’s First Amendment rights. In the case, the government demonstrated reasonable likelihood that a disclosure would inform current and future targets of investigations about the types of records and other materials sought. Additionally, the government made plausible showing that public access to such information would provide knowledge about FBI investigative methods that could prompt changes in the behavior of targets to evade detection, or signal that particular targets are under active surveillance.

---

## 5. Government monitoring scenarios

This section discusses three scenarios that focus and clarify the principal legal issues related to the government monitoring of privately owned critical infrastructure assets to combat foreign cyberspace threats. The three scenarios, each with an increasing degree of intrusiveness, involve the use of: (i) government-operated honeynets; (ii) sensor deployment and integration; and (iii) embedded government employees.

Each of the following subsections describes a scenario and provides a legal analysis of its viability. The legal analyses draw on the constitutional authorities and jurisprudence discussed in the previous sections, with particular emphasis on regulatory takings, surveillance, privacy and non-disclosure.

### 5.1. Government-operated honeynets

*To gain an understanding of a nation state adversary’s intentions and capabilities, the Department of Homeland Security installs and operates sophisticated honeynets whose “front doors” are located at the control centers of major privately owned electrical utilities. The honeynets are designed to mimic genuine information technology and SCADA systems. An executive order provides the authority for installing and operating the honeynets.*

Foreign intelligence collection – as in the case of the deployed honeynets – is not enumerated as a power of Congress in Article I of the Constitution, nor is it expressly mentioned in Article II as a responsibility of the President [46]. Nevertheless, it is difficult to imagine that the framers of the Constitution intended to reserve foreign intelligence collection to the states or to deny this authority to the federal government. Were Congress to enact regulation requiring the installation of honeynets for foreign intelligence collection, it is likely that the courts would uphold the regulation using the same reasoning as was used to create FERC, which regulates a portion of the energy sector. Since one can safely assume that the war and foreign affairs powers of the President extend to national security efforts, the question becomes: Are these powers strengthened or weakened by congressional action?

The executive branch could justify its decision to install and operate honeynets based on existing legislation or by requesting a FISA warrant. If the argument is that the US critical infrastructure and associated cyberspace constitute a “battlefield”, then legislation such as the 2001

Joint Resolution of Authorization for Use of Military Force would authorize the use of force anywhere in the world, including US territory and potentially cyberspace [46]. When the US is under enemy attack, the President can order electronic surveillance just as the armed forces are ordered to gather intelligence about the enemy. Since FISA and its amendments were enacted to address foreign intelligence acquisition, it seems that a FISA order would be appropriate and non-controversial. The executive branch may decide that deploying honeynets without a warrant falls within its inherent authority to protect and defend the country. However, given the legislation currently in place (i.e., FISA and its amendments), presidential authority may be at its lowest ebb for the warrantless use of honeynets.

In order to place honeynets in privately owned assets, the government may need to “seize” a portion of the control center via a regulatory taking. Eminent domain is commonly employed for public use, but this is problematic when the public use requirement is in question. Generally, the courts have not interfered with the government’s determination of public use and the Fifth Amendment’s Public Use Clause has offered little or no protection to property owners. Nevertheless, the regulatory taking power is often limited by requiring the government to show necessity, either based on a statutory requirement or by a court’s interpretation of valid public use. Thus, if it is determined that if the honeynets are required for the general health and safety of the public, and that the President is authorized to act against foreign threats, then the decision to deploy the honeynets would be upheld in court. Additionally, Executive Order 13406 allows for an exception of public takings for purposes of public safety, which fits the honeynet scenario.

Privacy does not appear to be a major issue in the honeynet scenario. While some may consider honeynet use to be tantamount to entrapment, it is important to note that the honeynets in the scenario are used for intelligence gathering and not directly in criminal investigations of US persons. Thus, the question of entrapment does not exist.

Secrecy is of utmost importance in the honeynet scenario. In the 2008 case of *Doe vs. Mukasey*, the government listed several cases where restraint regulators were held to a less demanding standard regarding pre-trial discovery gag orders, grand jury secrecy, etc. [42]. However, when the Supreme Court assessed the First Amendment validity of a pre-trial discovery gag order, it concluded that the relevant questions are: (i) if the practice in question furthers an important or substantial governmental interest unrelated to the suppression of expression and, (ii) if the limitation of First Amendment rights is no greater than that required to protect the particular government interest [42]. In the *Doe vs. Holder* case discussed earlier, secrecy orders were upheld when the government showed that any release of information would prompt changes in the behavior of targets to evade detection or signal that particular targets are under active surveillance. The same arguments could be used by the government to shield all information pertaining to the honeynets, including their locations and capabilities.

## 5.2. Sensor deployment and integration

*The US Government has discovered that a nation state adversary is attempting to compromise various energy sector assets, and*

*that the intrusions are being launched from multiple countries. The Department of Homeland Security has the technology to detect and mitigate the intrusions, but, in order to do so, must correlate backbone router traffic with data from energy sector assets. Government sensors are deployed in backbone routers as well as electric grid and pipeline assets, all of which are owned by private entities. An executive order provides the authority for installing the sensors and integrating the collected data for defensive purposes.*

The sensor deployment scenario is more intrusive than the honeynet deployment scenario because the sensors are planted in the backbone as well as in critical infrastructure assets. Also, data pertaining to network and system operations is collected and correlated for defensive purposes.

The executive order that provides the authority is similar to that used for the Terrorist Surveillance Program (TSP) conducted by the National Security Agency (NSA) following the 9/11 attacks. However, the scenario is less intrusive than the TSP because it does not involve listening in on phone calls or reading email. The fundamental question is: Can the President order large-scale sensor deployment and integration in privately owned assets to defend the nation from foreign intrusions?

Data mining is a useful tool for criminal investigations and national security efforts [37]. Following the 9/11 attacks, government officials sought to develop patterns of criminal and terrorist behavior and search for the patterns in data collected from various sources (e.g., airline ticketing and financial transactions). In the Homeland Security Act of 2002, Congress required the Department of Homeland Security to establish and utilize data mining and other advanced analytical tools to detect and identify threats. The sensor deployment and integration scenario is similar to – and much less intrusive than – collecting airline travel and financial records from private entities and mining the collected data to discern threats.

Although the existence of TSP was first revealed by the media in December 2005 [47], very little information about TSP has been released. However, President Bush has stated that he authorized the NSA to intercept international communications into and out of the United States for persons linked to Al Qaeda and other terrorist organizations without a FISA warrant. The Bush Administration also reported that surveillance activities were reviewed approximately every 45 days by the Attorney General to ensure that they were being conducted properly [37]. Administration officials have since acknowledged that TSP is one of several intelligence activities authorized by executive order.

TSP was created to identify unknown terrorists and discover new plots—to do this officials felt that a very wide net had to be cast [48]. The problem was that a FISA request required the identity or description of the target of the surveillance, the nature of the information sought and a description of the minimization procedures, among other details [49]. Consequently, an executive branch decision was made not to apply for FISA orders or seek legislation, but to rely on the President’s authority as Commander-in-Chief.

Legal challenges have yet to halt the warrantless surveillance of foreign actors, and the Obama Administration continues many of the same programs instituted by the Bush



administration. In the 2007 US Court of Appeals case of *ACLU vs. NSA* [50], the court ruled that the plaintiffs lacked the standing to file the lawsuit because (among other things) no concrete, actual or imminent harm was suffered. Several news stories have asserted that the NSA performed illegal wiretaps (see, e.g., [51]), but these stories have had little impact and no cases have reached the Supreme Court.

The deployment of sensors in the critical infrastructure is one step beyond CNCI, which intends to embed sensors in federal government assets. However, it is well short of DARPA's controversial Total Information Awareness (TIA) Program [37] that sought to mine information about almost everything – communications, finance, education, medicine, national borders, transportation, government records and housing – to combat terrorist threats. Responding to the storm of protest, the Senate on January 23, 2003, adopted an amendment that prohibited the deployment of TIA in connection with data about US persons without specific congressional authorization. Eight months later, Congress terminated TIA funding, with the exception of “[p]rocessing, analysis and collaboration tools for counterterrorism foreign intelligence” specified in a classified annex. It appears that this classified annex would likely support sensor deployment in the critical infrastructure if it only seeks to collect and correlate information about the activities of foreign actors.

Given the amount of legislation related to foreign surveillance, presidential power is currently at its lowest ebb with regard to issuing orders for warrantless surveillance. Note also that even if Congress were to proscribe these efforts and eliminate funding, the President may yet authorize sensor deployment, leading to a conflict that could only be resolved by the judicial branch. However, when considering the threat to the critical infrastructure and to the nation as a whole, the President's obligation to defend the nation would likely withstand challenges against an order to monitor foreign activities.

With regard to regulatory takings, the issues related to the deployment of sensors are similar to those discussed in the honeynet scenario. The only area of contention is the physical placement of the sensors and the equipment necessary to conduct surveillance. But this is not an issue as long as the government compensates the private entities fairly and the sensor placement does not provide the private entities with a competitive advantage.

Privacy is an obvious concern in the sensor deployment scenario. Since the government's purpose is to monitor foreign activity related to critical infrastructure intrusions, it cannot use any of the collected information to prosecute or cause any harm (e.g., levy fines) to US citizens who are not associated with a foreign power.

Finally, as in the previous scenario, NSLs can be used to obscure surveillance operations from public view. The same reasoning used to shield the use of honeynets and TSP would permit the use of NSLs to maintain the secrecy of the sensor deployment and data integration activities.

### 5.3. Embedded government employees

*The US Government has discovered that major energy sector assets have been systematically compromised by a nation state adversary. Sophisticated rootkits have been installed in key computing assets,*

*enabling the adversary to manipulate certain portions of the power grid and other resources. The Department of Homeland Security embeds federal agency personnel in privately owned energy sector companies to implement classified security controls and countermeasures. Only the senior executives of the companies are aware that these individuals are not company employees. An executive order provides the authority for embedding agency personnel.*

This embedded employee scenario builds on the previous two scenarios. The executive order goes beyond automated intelligence collection: it requires private companies to host federal employees and allow them to implement classified security controls and countermeasures for their critical infrastructure assets. Note that Congress has addressed the issue of intelligence collection in FISA and its amendments, but the embedding of federal employees to combat foreign threats is an open issue, potentially leaving room for presidential action. Therefore, the primary questions are: Can the President order such an act, and what are the implications with regard to regulatory taking, privacy and disclosure as discussed in the preceding sections?

The Supreme Court's views regarding the separation of powers permit the President to occasionally act in accordance with the inherent powers under the Constitution without express or implied authorization from Congress [16]. The presidential powers most relevant to this scenario have a constitutional basis in the areas of foreign affairs, war and the oath-based obligation to defend the nation from imminent threats, sometimes called the “emergency theory”.

In 1875, the Supreme Court ruled in *Totten vs. US* [52] that President Lincoln was authorized as Commander-in-Chief to employ secret agents during the Civil War [53]. More than a century later, the Supreme Court stated in the 2005 case of *Tenet vs. Doe* [54] that the *Totten* case applied to Cold War spies as well. Thus, the argument can be made that the President can deploy secret agents in the scenario under consideration.

Note that Congress has authorized the executive branch to use undercover federal air marshals on commercial flights to detect, deter and defeat hostile acts [55]. In the current scenario, Congress could dictate the use of embedded agents, much like it did for air marshals on commercial flights under the Aviation and Transportation Security Act of 2001.

Short of a constitutional or congressional mandate prohibiting or dictating specific methods, the executive branch may use various methods – and at its own discretion – to defend the critical infrastructure from cyber attacks. Many areas of the critical infrastructure are heavily regulated, but it appears that regulations focusing on defenses against foreign attacks are inadequate. Given the advanced classified security controls and countermeasures necessary to combat foreign threats, it appears in this scenario that presidential authority is in the “zone of twilight”, at least until Congress takes further action. This is because Congress has not proscribed – nor is it likely to proscribe – inherent constitutional authority bestowed on the executive branch to protect and defend the nation from foreign cyber threats. If the purpose of embedding federal employees is to protect the citizenry from criminal acts by US citizens, then the President would have little room to maneuver based on the Tenth Amendment

and other federal regulations related to criminal activity and justice. Therefore, the President can authorize the deployment of embedded government personnel as agents to meet the legitimate goal of protecting the US from intrusions and cyber attacks by foreign powers.

With regard to regulatory taking, a federal employee could be embedded in a private entity. However, the government would be obligated to compensate the private entity for the overhead associated with the fictitious job. The government can also make a valid argument that the embedded employee serves a public purpose, but the embedded employee must not provide an advantage to one company over another by providing a protective service. Therefore, every attempt must be made to embed the federal employees as fairly as possible.

From a legal perspective, privacy considerations related to an individual's use of the critical infrastructure are not controversial. As discussed earlier, the Supreme Court ruled that the Fourth Amendment does not restrict government access to data held by third parties, even if the third party possesses the data because of a legal obligation. A potential concern is a situation where an embedded employee discovers that the company is not in compliance with certain regulations. But this is not an issue because the government has embedded the employee explicitly for the purpose of implementing security controls and countermeasures against the foreign adversary, and any information collected by the employee cannot be used to verify compliance with regulations.

Finally, an NSL that preserves the secrecy of embedded federal employees is justified by the need to shield clandestine activities from public view. The same reasoning used in the previous two scenarios and the arguments supporting the secrecy of federal air marshals could be used by the government to safeguard all information about embedded employees, including their locations and capabilities.

## 6. Conclusions

The most insidious cyber operations on US critical infrastructure assets are being conducted by the military and intelligence services of other nations [56]. Private sector entities are generally unable to detect and address the compromises because these cyber operations are sophisticated and well resourced.

Government agencies have the resources to perform robust monitoring of critical infrastructure assets. The authority for such monitoring would derive from legislative or executive action, albeit pursuant to judicial scrutiny. Absent congressional action, the President – drawing on the oath-based obligation to defend the nation from foreign threats – may issue executive orders to conduct monitoring operations. The principal areas of contention related to government monitoring are regulatory takings, surveillance, privacy and non-disclosure. Our legal analysis based on the three monitoring scenarios involving government-operated honeynets, sensor deployment and integration, and embedded government employees indicates that the President has the authority – and the constitutional obligation – to protect privately owned critical infrastructure assets from

foreign threats if the goal is national security and no less intrusive and less restrictive alternatives are unavailable.

The terrorist attacks of September 11, 2001, changed the government's approach to airline security. The government now screens all passengers, interdicts potentially hostile aircraft and deploys undercover marshals on commercial flights. While we are not necessarily advocating pervasive government monitoring of the critical infrastructure, we believe it is prudent to analyze the legal principles that would permit or preclude various forms of monitoring before devastating cyber attacks on the critical infrastructure push the government to action.

Note that the views expressed in this paper are those of the authors and do not reflect the official policy or position of the National Defense University, the Department of Defense, or the US Government.

## REFERENCES

- [1] TripAtlas.com, Project Nike, Toronto, Ontario, 2010. [TripAtlas.com/Project\\_Nike](http://TripAtlas.com/Project_Nike).
- [2] US Strategic Command, US Cyber Command, Offutt Air Force Base, Nebraska, 2010. [www.stratcom.mil/factsheets/cc](http://www.stratcom.mil/factsheets/cc).
- [3] G. Bush, The national strategy for the physical protection of critical infrastructures and key assets, The White House, Washington, DC, 2003.
- [4] R. Clarke, R. Knake, Cyberwar: The Next Threat to National Security and What to do About it, HarperCollins, New York, 2010.
- [5] North American Aerospace Defense Command, About NORAD, Peterson Air Force Base, Colorado, 2010. [www.norad.mil/about/CMOC\\_2.html](http://www.norad.mil/about/CMOC_2.html).
- [6] North American Aerospace Defense Command, About NORAD, Peterson Air Force Base, Colorado, 2010. [www.norad.mil/about/index.html](http://www.norad.mil/about/index.html).
- [7] R. Jajosky, S. Groseclose, Evaluation of reporting timeliness of public health surveillance systems for infectious diseases, BMC Public Health 4 (29) (2004). [www.biomedcentral.com/1471-2458/4/29](http://www.biomedcentral.com/1471-2458/4/29).
- [8] B. Obama, The comprehensive national cybersecurity initiative, The White House, Washington, DC, 2010. [www.whitehouse.gov/sites/default/files/cybersecurity.pdf](http://www.whitehouse.gov/sites/default/files/cybersecurity.pdf).
- [9] US Supreme Court, Gibbons v. Ogden, United States Reports 22 (1824) 1–186.
- [10] M. Christie, Economic regulation in the United States: The constitutional framework, University of Richmond Law Review 40 (3) (2006) 949–980.
- [11] US Supreme Court, Wickard v. Filburn, United States Reports 317 (1942) 111–133.
- [12] US Supreme Court, Katzenbach v. McClung, United States Reports 379 (1964) 294–304.
- [13] US Supreme Court, US v. Lopez, United States Reports 514 (1995) 549–644.
- [14] US Supreme Court, US v. Morrison, United States Reports 529 (2000) 598–663.
- [15] US Supreme Court, Gonzales v. Raich, United States Reports 545 (2005) 1–74.
- [16] J. Rollins, A. Henning, Comprehensive national cybersecurity initiative: Legal authorities and policy considerations, CRS Report for Congress, R40427, Congressional Research Service, Washington, DC, 2009.
- [17] US Supreme Court, Youngstown Sheet & Tube Co. v. Sawyer, United States Reports 343 (1952) 1–710.

- [18] J. Curran, Feds threaten eminent domain grab on Vermont farm, [Newsvine.com](#), May 2, 2010.
- [19] S. Saxer, Government power unleashed: Using eminent domain to acquire a public utility or other ongoing enterprise, *Indiana Law Review* 38 (1) (2005) 55–102.
- [20] R. Meltz, C. Copeland, E. Boyd, B. Yeh, D. Carpenter, S. Carmody, CRS issue statement on eminent domain and takings, CRS Report for Congress, IS40267, Congressional Research Service, Washington, DC, 2010.
- [21] US Supreme Court, *Pennsylvania Coal v. Mahon*, United States Reports 260 (1922) 393–422.
- [22] S. Krueger, *Keystone Bituminous Coal Association v. DeBenedictis: Toward redefining takings law*, *New York University Law Review* 64 (4) (1989) 877–907.
- [23] US Supreme Court, *Keystone Bituminous Coal Association v. DeBenedictis*, United States Reports 480 (1986) 470–521.
- [24] US Supreme Court, *Kelo v. City of New London*, United States Reports 545 (2005) 469–523.
- [25] G. Bush, Executive Order 13406, The White House, Washington, DC, 2006.
- [26] J. Dvorske, Validity, construction and application of the Foreign Intelligence Surveillance Act of 1978, *American Law Reports (Federal Series)* 190 (2003) 385–452.
- [27] E. Johnson, Surveillance and privacy under the Obama Administration: The Foreign Intelligence Surveillance Act of 1978 and the Attorney General's guidelines for domestic operations, *I/S: Journal of Law and Policy for the Information Society* 5 (3) (2010) 419–446.
- [28] US District Court (Eastern District of New York), *US v. Falvey*, Federal Supplement 540 (1982) 1306–1316.
- [29] US Court of Appeals (Second Circuit), *US v. Duggan*, Federal Supplement (Second Series) 743 (1984) 59–85.
- [30] US Court of Appeals (Second Circuit), *US v. Truong Dinh Hung*, Federal Supplement (Second Series) 629 (1980) 908–932.
- [31] US Supreme Court, *US v. United States District Court*, United States Reports 407 (1972) 297–344.
- [32] US District Court (Southern District of New York), *US v. bin Laden*, Federal Supplement (Second Series) 126 (2000) 264–290.
- [33] US Supreme Court, *Griswold v. Connecticut*, United States Reports 381 (1965) 479–531.
- [34] L. Curry, *The Human Body on Trial*, ABC-CLIO, Santa Barbara, California, 2002.
- [35] B. Garner, *Black's Law Dictionary*, Thomson West, St. Paul, Minnesota, 2004.
- [36] US Supreme Court, *Katz v. US*, United States Reports 389 (1967) 347–374.
- [37] F. Cate, Government data mining: The need for a legal framework, *Harvard Civil Rights—Civil Liberties Law Review* 43 (2) (2008) 435–489.
- [38] US Supreme Court, *US v. Miller*, United States Reports 425 (1976) 435–456.
- [39] US Supreme Court, *Smith v. Maryland*, United States Reports 442 (1979) 735–752.
- [40] C. Savage, Judges divided over rising GPS surveillance, *The New York Times*, 2010.
- [41] A. Nieland, National security letters and the amended PATRIOT Act, *Cornell Law Review* 92 (6) (2007) 1201–1236.
- [42] C. Doyle, National security letters in foreign intelligence investigations: Legal background and recent amendments, CRS Reports for Congress, RL33320, Congressional Research Service, Washington, DC, 2009.
- [43] US Court of Appeals (Second Circuit), *Doe v. Mukasey*, Federal Supplement (Third Series) 549 (2008) 861–885.
- [44] US District Court (Southern District of New York), *Doe v. Holder*, Federal Supplement (Second Series) 665 (2009) 426–434.
- [45] US District Court (Southern District of New York), *Doe v. Holder*, Westlaw 1253522, March 18, 2010.
- [46] E. Bazan, J. Elsea, Memorandum, subject: Presidential authority to conduct warrantless electronic surveillance to gather foreign intelligence information, Congressional Research Service, Washington, DC, 2006. [www.fas.org/sgp/crs/intel/m010506.pdf](http://www.fas.org/sgp/crs/intel/m010506.pdf).
- [47] E. Bazan, The Foreign Intelligence Surveillance Act: An overview of selected issues, CRS Report for Congress, RL34279, Congressional Research Service, Washington, DC, 2008.
- [48] B. Gellman, *Angler: The Cheney Vice Presidency*, Penguin, New York, 2008.
- [49] L. Chiarella, M. Newton, So, Judge, how do I get that FISA warrant? The policy and procedure for conducting electronic surveillance, *The Army Lawyer*, October 1997, pp. 25–36.
- [50] US Court of Appeals (Sixth Circuit), *American Civil Liberties Union v. National Security Agency*, Federal Supplement (Third Series) 493 (2007) 644–704.
- [51] C. Savage, J. Risen, Federal Judge finds NSA wiretaps were illegal, *The New York Times*, 2010.
- [52] US Supreme Court, *Totten v. Doe*, United States Reports 92 (1875) 105–107.
- [53] B. Decker, The war of information: The Foreign Intelligence Surveillance Act, *Hamdan v. Rumsfeld*, and the President's warrantless wiretapping program, *Journal of Constitutional Law* 9 (1) (2006) 292–356.
- [54] US Supreme Court, *Tenet v. Doe*, United States Reports 544 (2005) 1–12.
- [55] M. Randol, The Department of Homeland Security intelligence enterprise: Operational overview and oversight challenges for Congress, CRS Report for Congress, R70602, Congressional Research Service, Washington, DC, 2010.
- [56] J. Langevin, M. McCaul, S. Charney, H. Raduege, J. Lewis, *Securing cyberspace for the 44th Presidency*, Center for Strategic and International Studies, Washington, DC, 2008. [csis.org/files/media/csis/pubs/081208\\_securingcyberspace\\_44.pdf](http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf).