Privacy, Surveillance And The State: A Comparison Of U.S. And British Privacy Rights

2009

Angelina Lander
University of Central Florida

PRIVACY, SURVEILLANCE AND THE STATE: A COMPARISON OF U.S. AND BRITISH PRIVACY RIGHTS

by

ANGELINA M. LANDER
B.A. University of Central Florida, 2004

A thesis submitted in partial fulfillment of the requirements
for the degree of Master of Arts
in the Department of Political Science
in the College of Sciences
at the University of Central Florida
Orlando, Florida

Summer Term
2009

Major Professor: Barbara Sgouraki Kinsey

ABSTRACT

This study investigates the effects of institutional structure on the privacy rights regimes in the United States and the United Kingdom, from 2000-2006. The goal of this research is to analyze how variation in the institutional arrangements across these two countries allowed for more or less protection of privacy rights for citizens. Domestic terrorist attacks during the time period represent a catalyst for changes in police and government surveillance activities. Veto points literature provides the framework for institutional comparison.

The first part of the research provides a discussion of the historical evolution of privacy rights in both states, focusing on government and police surveillance and investigations. The second part of the research, based on veto points theory, compares the institutional arrangements of the United States and the United Kingdom, and suggests that the number of veto points and the ideological proximity of veto players have had an effect on the formulation of policy. Laws governing surveillance, investigations and privacy in the year 2000 provide a benchmark for analyzing how policies change over time.

ACKNOWLEDGMENTS

I would like to acknowledge and thank Dr. Barbara Kinsey for her patience and understanding during this process. Her guidance and support were instrumental in the completion of this thesis. I also thank the members of my graduate committee, Drs. Waltraud Q. Morales and Kerstin Hamann for their guidance and suggestions. Finally, I thank my husband, Steve, my brother Nick Schenk, Nicole Jobson and Mark Freeman and the rest of my family for encouraging me, over these many years, to graduate.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

Anti-terrorism, Crime and Security Act: ACSA

Central Intelligence Agency: CIA

Close Circuit Television: CCTV

Communications Assistance for Law Enforcement Act of 1994: CALEA

Data Protection Act of 1998: DPA

European Convention on Human Rights: ECHR

Federal Bureau of Investigation: FBI

Federal Intelligence Surveillance Act: FISA

Global Positioning System: GPS

Internet Service Provider: ISP

National Security Agency: NSA

National Security Letter: NSL

Radio Frequency Identification: RFID

Regulation of Investigatory Powers Act: RIPA

United States Postal Service: USPS

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001: USA PATRIOT Act

Voice-over-IP: VoIP

CHAPTER 1: OVERVIEW AND EXPECTATIONS

Introduction

"We need to be keenly aware of the startling advances in the sophistication of eavesdropping and surveillance technologies with their capacity to easily sweep up and analyze enormous quantities of information and then mine it for intelligence. And this adds significant vulnerability to the privacy and freedom of enormous numbers of innocent people at the same time as the potential power of those technologies grows. Those technologies do have the potential for shifting the balance of power between the apparatus of the state and the freedom of the individual in ways that are both subtle and profound." – Al Gore, Speech on Constitutional Issues, January 16, 2006 (Gore, 2006, pp. 565-566).

Technological breakthroughs in the previous century have enhanced communications capabilities to the point where information can be transmitted across the world in a matter of seconds. Data travels across borders and into homes, internet cafes, cell phones, and anywhere with Wi-Fi capabilities. The last 20 years has seen the birth and maturation of the cell phone industry, internet service providers, search engines, and the rise of social networking and blogging. An ever increasing number of satellites has allowed satellite TV, global positioning systems (GPS), and interactive mapping to develop into mainstream applications. There are many positive aspects to these technological developments, making life much more convenient for those able to access the services provided. These same technologies have been used by states to increase intelligence gathering capabilities, including: tracking personal financial transactions, recording detailed satellite images of neighborhoods, pinpointing cell phone locations, tapping phone lines, intercepting emails, collecting and storing video footage of public places, collecting virtual information through internet browser histories and online profiles, and even using infrared scanners to detect heat signatures through the walls of private residences (Etzioni, 2007; Gadzheva, 2008; Hentoff, 2008). Privacy advocates and scholars have raised concerns that some democratic governments may be using these technological advancements to collect information at the expense of civil liberties, including the right to privacy.

The protection of individual privacy is an important facet of a democratic society. Balancing state power and the rights of individuals is at the very core of democratic theory, and one which can be applied to the current issue of national security versus individual privacy. September 11, 2001 forced Western democracies, and the United States in particular, to focus more closely on internal security concerns. In addition to the U.S., the United Kingdom experienced a large-scale terrorist attack, the July 7, 2005 bombings, and responded by increasing domestic security. As the security apparatus expands, there have been policy changes in privacy protections across the United States and United Kingdom. The expectation is that the extent of policy change across these two countries will vary given their distinct institutional structure. Policies created to strengthen domestic intelligence gathering in the wake of these crises have come under scrutiny by privacy advocates for infringing on individual rights. It is important to understand how these two democracies created policies to expand their security apparatuses, and whether the policy making process itself affected the amount of privacy protections available to their citizens. To do so, it is essential to identify the institutional variations between the U.S. and U.K., and to understand how these differences affect policy change with respect to privacy rights. The purpose of this thesis is to determine if the different institutional arrangements of the United States and the United Kingdom affect the extent of privacy protection for individuals.

The institutional literature suggests that policy change is a function of the number of veto points and ideological proximity of the veto players. Veto points literature argues that in most cases policy change is less likely with a larger number of veto points, and deviations from the status quo more likely with a smaller number. The literature points out that ideological proximity and preferences of veto players also affect policy change, and where veto players have

convergent preferences, policy change is more likely (Crepaz, 2004; Kastner & Rector, 2003; O'Reilly, 2005; Tsebelis, 2000). As security comes to the fore in the U.S. and U.K., the expectation is that there will be some convergence of preferences, but that the U.S., with a larger number of veto points, will have less policy change than the U.K.

Assessing privacy protections will be a complicated task due to the ambiguity surrounding the concept and development of privacy rights in the U.S. and U.K. Despite the Fourth Amendment protections against unwarranted search and seizures, the U.S. Constitution does not specifically outline a right to privacy, and protections rely on legislation and case law. While the U.K. does not have a written constitution, and privacy protections are also reliant on legislation and case law, the U.K. is a signatory to the European Convention on Human Rights (ECHR), which does specify that individuals have a right to privacy. It is important to note that this research is not concerned with privacy rights as they relate to medical records, personal choice issues, such as personal choice, religious affiliations, abortion, or privacy from corporate marketing, data collection, and tracking. This research is expressly interested in privacy rights and protections for citizens involved in government or law enforcement agency investigations and surveillance. There is some overlap, however, between corporate data collection and surveillance activities when the information gathered from corporate sources is requested by law enforcement for evidentiary use, and this overlap will require further clarification.

The privacy protection research relies on primary source documents such as bills and statutes to provide information about what law enforcement powers are authorized by the government. I analyze the language of the law to identify unclear or underdeveloped concepts that leave room for interpretation and expansion of government power. Secondary print and

electronic magazine and newspaper source also provide analysis of law, and report on political tensions within government agencies regarding their passage.

Expectations

The main underlying assumption here is that an increase in surveillance, investigations, and intelligence gathering translates into less privacy for citizens, and since the U.S. and U.K. are democratic countries, the secondary assumption is that they value some level of privacy from intrusive government activities, as such privacy is important to democratic values of freedom of speech, expression, and dissent. On the surface, it appears that institutional variations across countries would result in differing levels of privacy protections. The bicameral presidential model of government in the U.S. government includes checks and balances that tend to produce policy stability by reducing the ability of one party to completely control the legislative process. The parliamentary system in the U.K. is controlled by the majority party in the lower house, which elects a Prime Minister, and has comparatively fewer checks on executive and legislative power. Policy changes in response to the terrorist attacks in both countries, and during the 'War on Terror' and the invasion of Iraq, have increased the amount of law enforcement activities sanctioned by the government, including surveillance and intelligence gathering. This research posits that the U.K. will be able to push through more legislation increasing government powers than the U.S. based on the institutional differences mentioned above. Put differently, the checks and balances inherent in the U.S. government should provide more privacy protection for citizens since all three branches must approve of new legislation and policies[1].

Conducting an analysis of privacy protections assumes that some amount of privacy exists in these countries, and that it is desirable to the populations. Thus, it is essential to come to

[1] The U.S. Supreme Court can rule whether or not laws are Constitutional, but there is significant lag time associated with the Court's ability to effect policy change, due to the sometimes lengthy appeals process and/or the refusal of the Court to grant standing to a particular case.

an understanding of what privacy means within the context of the liberal democratic traditions of the United States and the United Kingdom to answer the following questions: how did the concept of the right to privacy develop? And how has it evolved over time in these two states? Chapter 2 addresses these questions and discusses the evolution of individual privacy in the U.S. and U.K. Following the discussion of the concept of privacy, I turn to the theoretical framework to discern what privacy protections are, and how institutional differences may affect the amount of protection. These issues are discussed in Chapter 3. Chapter 4 includes the comparison of the U.S. and U.K. privacy protection regimes and presents the findings of this research. Finally, Chapter 5 concludes and provides an overview of the analysis of the research.

CHAPTER 2: THE RIGHT TO PRIVACY IN THE U.S. AND U.K

Privacy in the United States

Defining privacy has also been acknowledged within the fields of sociology, psychology, philosophy, and political science as a particularly difficult task, deserving of contextual information about whom and what is the object of privacy. For the purposes of this research, the relevant population are citizens and resident aliens in the United States and the United Kingdom, and privacy is defined as "that part of our lives insulated against the communal or public broadly construed, protected from unwanted intrusion by other, including political authorities, and the place where, in the last resort, we can clothe ourselves in anonymity" (Peterman, 1993, pp. 218-219). Such a concept of privacy is tied to democratic values, and the liberal traditions common to Western democracies. The fundamental rights to freedom of speech, religion, and expression are intricately tied to the "freedom of thought, control over one's body, solitude in one's home, control over information about oneself, freedom from surveillance, protection of one's reputation, and protection from searches and interrogations" (Solove, 2002, p. 1088). This is especially true in democratic countries, where citizens have the expectation of privacy in these regards, and moderate legal protections to ensure it.

Privacy protections in the United States are drawn from two main sources, the Supreme Court's interpretation of the Fourth Amendment and legislation enacted by Congress limiting the government's ability to conduct surveillance on its citizens. The right to privacy was first recognized in the early twentieth century by the Supreme Court, and the Court has since broadened the scope of the Fourth Amendment by reinterpreting unreasonable search and seizures. Several cases have been central to understanding what the Court has determined is protected under the Fourth Amendment, and what protections individuals can expect.

The most well-known definition of privacy in the U.S., and perhaps the simplest, written by Supreme Court Justice Brandeis, is “the right to be let alone-the most comprehensive of rights and the right most valued by civilized men” ("Olmstead et al. v. United States", 1928, p. 277 U.S. 471). This dissenting opinion, and Warren and Brandeis’ 1890 article in the Harvard Law Review, “The Right to Privacy”, were seminal in defining an interest in the right to privacy in American legal discourse, and provided the impetus necessary for the Court to consider more comprehensive privacy protections ("Olmstead et al. v. United States", 1928; Warren, 1890).

> “Prior to 1890 privacy had never been treated as an independent legal right; whatever legal protection it had received had been as a consequence of its association with other, more familiar legal rights – the right to property and its offspring, the laws of nuisance, trespass, and defamation, or under the rubric of family law and domestic relations” (Mindle, 1989, pp. 586-587).

If privacy did not exist in its own right, on what legal precedent had Brandeis based his dissent? Anuj C. Desai argues that “crucial among the precedents on which Brandeis relied was the 1878 case *Ex Parte Jackson*, the first case in which the Court ruled that the Fourth Amendment preserved a realm of communications privacy from government intrusion” (Desai, 2007, p. 556). According to Desai, when the Continental Congress established the United States Postal Service (USPS), they codified in the charter a right to communications privacy.

> “In October 1782, towards the end of the Revolutionary War, the Continental Congress passed a comprehensive postal ordinance. That law explicitly prohibited postal officials from opening the mail without ‘an express warrant under the hand of the President of the Congress of these United States or in time of war, of the Commander in Chief of the armies of these United States, or of the commanding officer of a separate [sic] army in these United States, or of the chief executive officer of one of the said states’” (Desai, 2007, pp. 565-566).

This was not a sweeping privacy law, and did not establish a broader right to privacy, but rather developed over time during the Revolutionary War as a reflection of specific challenges Colonialists faced when sending communications through the British post (Desai, 2007).

Protections such as this, however, were influential precursors to more comprehensive privacy rights established by the Court in the late Nineteenth and early Twentieth century, and espoused by Brandeis.

Thus, beginning with the *Olmstead* decision, the Supreme Court began expanding privacy rights under the Fourth Amendment, especially the landmark 1967 decision in *Katz v. United States* ("Katz v. United States", 1967, p. 389 U.S. 347). Since this research focuses specifically on privacy protections with regard to government surveillance, this chapter examines the evolution of such protections, and does not include a discussion of privacy rights as they relate to moral issues such as sexual preference, obscenity, abortion, or domestic relations. The next section outlines individual privacy protections under the Fourth Amendment, followed by a discussion of privacy protections under important legislation, such as the Federal Intelligence Surveillance Act (FISA), the Stored Communications Act, the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), and the relevant Court decisions concerning these acts.

Privacy Protections Under the Fourth Amendment

The Fourth Amendment also grew out of the experience of the colonists during the Revolutionary War, as a response to the blanket searches and seizures conducted by British Officers holding writs of assistance. It establishes:

> "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized" ("The Constitution of the United States, Amendment IV", 1791).

This Amendment was not originally drafted to protect the privacy of citizens from the government. Actually, Mindle argues that the Founders never intended to recognize a right to

privacy, as such a right “would have damaged that sense of citizenship or civil spirit indispensable to the integrity and welfare of the political community” (Mindle, 1989, p. 578). Instead, the Fourth Amendment specifically targeted indiscriminate searches and seizures of the kind perpetrated by the British before and during the Revolutionary War, and it took the Court quite a while to establish privacy as right protected by this amendment. However, “in recent years, protection of privacy has come to be viewed as ‘the principal object of the Fourth Amendment’” ("Protecting Privacy under the Fourth Amendment", 1981, p. 314). New interpretations of the Fourth Amendment fundamentally redefined ‘searches’ and ‘persons and effects’, allowing the Court to augment privacy rights.

The most important cases establishing privacy protections under the Fourth Amendment are the decisions in *Olmstead v. United States*, *Berger v. New York* and *Katz v. United States*, and these decisions ultimately are responsible for the shift in interpretation of the Fourth Amendment ("Berger v. New York", 1967, p. 388 U.S. 341; , "Katz v. United States", 1967, p. 389 U.S. 347; , "Olmstead et al. v. United States", 1928). *Berger v. New York* involved the audio surveillance of attorney Ralph Berger’s office for several months. Berger was suspected of bribery, and the New York Police bugged his office, eavesdropped on months of his conversations, until they ultimately had the evidence needed to convict him of bribery. In the Court’s ruling opinion, it broadened the protections of the Fourth Amendment by ruling that the conversations recorded by the blanket surveillance were protected as private, that the audio surveillance was considered a ‘search’, and as such, the search parameters were too broad to be Constitutional. Following the *Berger* decision, was the *Katz v. United States* decision, which again widened the scope of privacy protections.

Charles Katz was being investigated by the FBI for illegal gambling, and was known to use a public phone booth to make the suspected illicit phone calls. The FBI argued that since Katz was using a public booth, and was not making the calls from his own property, the FBI did not need a warrant to conduct audio surveillance of the phone booth. However, the Court found that Katz paid for the use of the phone, shut the door, and expected that his conversations were not being recorded or overheard. “In *Katz v. United Sates*, the Supreme Court has maintained that an individual is protected by the Fourth Amendment whenever he or she has a ‘reasonable expectation of privacy’” ("Protecting Privacy under the Fourth Amendment", 1981, p. 314). These decisions not only solidified the warrant requirement for government surveillance, but they also expanded individual privacy rights by disconnecting privacy from property ownership. “By protecting this privacy interest, the Court enlarged the Fourth Amendment’s protective scope to encompass governmental intrusions in any private context” ("Protecting Privacy under the Fourth Amendment", 1981, p. 316). The decoupling is important as it establishes an individual’s right to privacy even when they are not within their own home, but also when they are at their office, a public phone booth, or any space where they can expect a reasonable amount of privacy.

Furthermore, the warrant requirement established by the Fourth Amendment is a safeguard against unreasonable searches, and the Supreme Court has generally held, with few exceptions, the need for investigative officers to obtain such a warrant before conducting searches, intercepting communications, wiretapping phones, or using audio/video surveillance.

> “The basic warrant procedure is uncomplicated. To obtain a valid warrant, a law enforcement officer must demonstrate to a judicial officer through sworn affidavits that probable cause exists to believe that criminal contraband or evidence will be found at a particular location” ("Protecting Privacy under the Fourth Amendment", 1981, p. 318).

Through this process, individuals are supposed to be protected from arbitrary searches, though there have been exceptions to the warrant requirement, most notably at border crossings, airports, and in vehicles, or when the search can prevent imminent harm to the suspect, the destruction of evidence, or bodily harm to innocent bystanders.

These precedents were upheld in the 1972 case *United States v. U.S. District Court*, also known as the *Keith* case, involving warrantless surveillance of defendants involved in plotting the destruction of government property ("United States v. U.S. District Court", 1972). The Court "drew a further distinction – one between surveillance related to domestic threats to national security and surveillance related to foreign threats to national security" (Seamon, 2005, p. 332). Since the defendants were American citizens, they were still subject to protections outlined under the Fourth Amendment, including the warrant requirement. This is an important distinction. Non-U.S. citizens are thus not afforded the same protections under the Fourth Amendment, and the government can investigate foreign nationals and foreign threats to security without being subject to the warrant requirement.

There are three important privacy protections established under these landmark Fourth Amendment cases: 1. searches, seizures, or surveillance of an individual not under arrest and without probable cause requires that a warrant be obtained from an judicial official ("United States v. U.S. District Court", 1972); 2. information obtained without a warrant may not permissible in court if an individual is acting under the assumption of a reasonable expectation of privacy ("Berger v. New York", 1967; , "Katz v. United States", 1967); and 3. searches include audio and video surveillance, thermal imaging, or any device "that is not in general public use, to explore details of a private home that would previously have been unknowable without physical intrusion" ("Kyllo v. United States", 2001, pp. 3-13). The government has sought exceptions to

these rights, most notably with regard to investigations of national security issues. Starting with FISA, and most recently, with the passage of the USA PATRIOT Act, the Terrorist Surveillance Act, and the Protect America Act, some of these protections have been revised. A further discussion of these acts and their effect on privacy protections and the Fourth Amendment is needed.

Privacy Protections and National Security

"Before Congress enacted the Foreign Intelligence Surveillance Act ("FISA") in 1978, presidents beginning with Franklin Roosevelt authorized warrantless electronic surveillance in the name of national security. They claimed the 'inherent power' to do so" through the War Powers clause (Seamon, 2005, p. 330). Presidents had authorized warrantless surveillance of individuals suspected of endangering national security, but also surveillance of criminal activities, dissidents, radicals, or opposition leaders whether the suspects were foreigners, foreign nationals, or citizens. Congress passed the FISA in response to The Church Committee's findings involving the misuse of executive power since the end of World War II, most notably the Watergate scandal, and the FBI's Counter Intelligence Program (COINTELPRO), which conducted intrusive surveillance on civil rights and anti-war activists (Bedan, 2007, p. 429). The Church Committee recommended that the U.S. government could limit abusive surveillance behavior by separating foreign and domestic intelligence gathering activities. FISA limited the scope of warrantless intelligence gathering by reducing the executive branch's ability to conduct criminal investigations, and shifting its scope to primarily foreign threats to national security.

> "Congress did not deny the President's inherent power to conduct electronic surveillance for national security purposes. Instead, Congress took the position that even if the President had such power, Congress could regulate that power by prescribing reasonable procedures for its exercise" (Seamon, 2005, p. 336).

The procedures require the executive branch to submit surveillance orders to the a special court for review, demonstrate that the target of the surveillance is "a foreign power or an agent of a foreign power" and that the location under surveillance "is being used, or is about to be used, by a foreign power or an agent of a foreign power" (Seamon, 2005, p. 339). These provisions were sought in order to limit the executive branches ability to conduct warrantless surveillance of domestic targets, and to force the government to conduct such investigations either under the FISA or under previously established Fourth Amendment protections. Specifically, "the definition of 'agent of a foreign power' distinguishes 'United States persons' from everyone else…The FISA specially protects the privacy interests of U.S. persons" (Seamon, 2005, p. 340).

The FISA and Fourth Amendment protections for U.S. citizens and resident aliens remained basically unchanged until 2001. Following the terrorists attacks, serious questions arose as to how the government failed to detect and prevent the hijackers plot. The Bush administration and the Congress responded quickly to the crisis with the USA PATRIOT Act, which changed surveillance capabilities and procedures for law enforcement, including amendments to the FISA. Some of the powers granted under the PATRIOT Act amend the FISA by allowing law enforcement officers to gather "foreign intelligence information[2]", the ability to share such information with any Federal officers or agents authorized to receive it, and the ability for law enforcement officers, and Federal officers and agents to obtain such information electronically ("USA PATRIOT Act", 2001). The PATRIOT Act also grants the Federal government broader ability to subpoena personal and business records including internet service, banking, library, and telecommunications records; broader ability to conduct roving wiretaps on cell phones and email accounts; broadens authorization of pen registers and trap and trace

[2] For the PATRIOT Act definition of foreign intelligence information please see H.R. 3162, Section 203, page 11.

devices[3] in internet communications; and relaxes the provision that FISA authorized surveillance is conducted strictly for the purpose of gathering foreign intelligence information ("USA PATRIOT Act", 2001). The PATRIOT Act replaces the FISA requirement stating that executive branch surveillance be conducted for the primary purpose of investigating foreign threats to national security, with a much less stringent requirement. The new requirement states only that surveillance may be conducted under the FISA if a foreign threat to national security is a significant part of the investigation. Since the government applies for the FISA warrants through the secret FISA court, the debate over what significance an investigation takes place with little oversight.

Privacy advocates argue that these new abilities remove the American exception under the FISA, and that they infringes on privacy rights protected by the Fourth Amendment.

> "The PATRIOT Act disrupts the delicate [balance] inherent in our established surveillance laws, which prior to September 11th provided government with sufficient lee-way to conduct both criminal and intelligence surveillance while protecting Americans' Fourth and First Amendment rights to be free from "unreasonable searches and seizures" and to exercise freedom of expression" (Rackow, 2002, p. 1653).

The lack of transparency under which the FISA courts operate, and within the executive branch bureaucracies *en masse*, has been targeted by privacy advocates as a significant cause for alarm. Of particular concern are the national security letters (NSLs) issued by the FBI, under the PATRIOT Act provisions, "which allow investigators to demand records without the approval of a judge and to prohibit companies or institutions from disclosing the request" (Eggen, 2005, p. A11). However, the Court has shown that if and when citizens feel their privacy has been invaded, they have the ability to challenge the government under Fourth Amendment protections. There are a few important questions to ask concerning the use of NSLs, and other PATRIOT Act

[3] For information pertaining to pen registers and trap and trace devices, please see U.S. Code, Title 18, Chapter 119 – Wire and Electronic Communications Interception and Interception of Oral Communications

powers. Even though the Court has granted Fourth Amendment protections, and the FISA contains privacy protections for U.S. persons, do executive branch organizations operate within these parameters? Are there executive branch activities that fall outside the realm of Fourth Amendment and FISA protections, and what impact do they have on individual privacy? What are the other government branches doing, if anything, to put a check on such power? These questions will be taken up at greater length in Chapter 3 and Chapter 4.

Privacy in the United Kingdom

Privacy protections in the U.K evolved originally from a strong recognition of private property, and the tradition that ‘an Englishman’s home is his castle’. Private property dominated the English discourse on democratic theory, embodied in the works of Thomas Hobbes, John Locke, and John Stuart Mill. “By the 1760s and 1770s, moreover, the Court of Common Pleas was protecting the subject’s castle again the king himself, by striking down general search warrants and upholding large fine against revenue agents who committed unlawful trespass” (Seipp, 1983, p. 335). As far as government surveillance is concerned, however, the U.K. has far less cohesive legal tradition than the United States. The British parliament, despite EU pressure since the passage of the European Convention on Human Rights (ECHR), has failed to pass legislation protecting a comprehensive right to individual privacy, and the courts have relied on legal tradition in cases where privacy rights are challenged. Without parliamentary initiative, the courts have been reluctant to adopt any privacy standards despite their recognition that such laws are lacking.

Privacy Protections and British Common Law

Private property laws emerged as an integral part of classical liberal traditions in the U.K., and can be seen in the writing of famous British theorists such as Thomas Hobbes, John

Locke, and John Stuart Mill. Private property was held in such a high regard that in some cases, peering into a neighbor's windows could be seen as offense against privacy. Englishman sought rulings by the courts in order to protect themselves from privacy intrusions by neighbors, passersby, and anyone who saw fit to loiter around their property. One of the main areas of common law protection was the law against trespassing on another's land, either by physically entering without permission, or by peering in through open windows, doors, or otherwise attempting to gain unauthorized views of private gardens.

> "The law of trespass was extended in the last decade of the [19th] century to cover 'unreasonable' user of the highway adjoining the plaintiff's land, an activity that encompasses observation of the plaintiff's activities on his own land. The criminal law supplemented these remedies with longstanding sanctions against peeping Toms and eavesdroppers as well as new offenses of 'watching and besetting' aimed primarily at trade union picketers" (Seipp, 1983, p. 337).

English common law generally ruled in favor of property owners claiming injuries or damages from such unauthorized intrusions. An Englishman's home was opined to be a refuge from the world, and common law provided legal protections for property owners to enforce this.

In addition to the strong recognition of private property rights, the English courts eventually recognized a level of communications privacy, both from the government and private intrusion. In the 18th century, letter interception by the government was widespread, but by the mid-19th century "as a result of the public outcry, one of the secret offices conducting such work was disbanded and in the other one, specific warrants from the Secretary of State were henceforth required" (Seipp, 1983, p. 339). The warrant requirement for opening mail and reading telegraphs was extended to telecommunications after telephones became widespread. However, according to the decision in the 1979 decision *Malone v. Commissioner of Police of the Metropolis*, although the police had a warrant to tap Mr. Malone's phone, the warrant requirement was not totally necessary under English law as "there was no property right in words

transmitted across telephone lines" (Noone, 1997, p. 144). If this seems contradictory, it may well be so. Unlike the United States, the British legal system has only upheld a patchwork of privacy rights, although it recognizes the importance of such rights. The lack of a formalized and comprehensive privacy rights regime can be attributed to press opposition, a failure of the legislature to pass a all-inclusive privacy rights bill, and the courts' unwillingness to legislate such rights in the courtroom. This has often put British law in opposition to the European Convention on Human Rights, which it signed as part of it's acceptance into the European Union.

British Privacy Protections and the European Convention on Human Rights

The U.K. is a signatory to the European Convention on Human Rights (ECHR), which provides for a level of privacy protection not specifically granted under U.K. law. Article 8 covers the relevant rights protected under the ECHR:

1. "Everyone has the right to respect for his privacy and family life, his home and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others" ("The European Convention on Human Rights", 4 November 1950).

After the U.K. became a signatory to the ECHR, scholars and other European states began demanding a more comprehensive recognition of a right to privacy in the U.K. A provision under the ECHR allowed any British citizen that felt these rights had been violated the right to appeal to the European Court of Human Rights. This appeal process places the U.K. in a difficult position. Without recognizing a comprehensive right to privacy in common law, or through parliamentary legislation, U.K. citizens fall below the level of protection available to them in the EU Court. U.K. citizens can, and have, challenged their government's existing privacy

protections at the EU Court, but the rulings from the court have no legal standing in the U.K. Issues such as these put international pressure on the U.K. to bring its policies more in line with the rest of EU states. “Adjudication of privacy claims under Article 8 of the Convention in these international tribunals may have the indirect effect of spurring the creation of domestic remedies to forestall unfavourable world publicity” (Seipp, 1983, p. 353). However, the U.K. firmly maintains its right to be the final arbiter in legal matters pertaining to its citizens.

Privacy Protections and National Security

The U.K privacy rights regime has less stringent requirements on government surveillance of citizens, and a broader mandate for law enforcement officials to collect and analyze individuals’ conversations, correspondence, and digital records, especially if the target is suspected of criminal activity. The 1998 Data Protection Act provides citizens with the right to protect, view, and amend personal information collected from third parties, but are exempted from such protections in the event of a national security or criminal investigation. The Regulations of Investigatory Powers Act (RIPA), passed in 2000, authorizes covert surveillance, wiretapping, and digital interceptions, in some cases, without a warrant requirement as long as permission is granted by the Home Secretary. RIPA has come under scrutiny as local governments have used the Act to obtain information about citizens.

> “In 2006, more than 1,000 applications per day were being made to use Ripa powers. The Act allows councils to authorise surveillance, obtain phone records and details of email traffic from personal computers (though not their contents) and obtain details of websites individuals are logging on to” (Rayner, 2008).

Initially, RIPA allowed very few agencies the right to authorize surveillance under its guise. After 9/11 however, “RIPA was "updated" so that nearly 800 bodies were empowered to go into the spying business” (Porter, 2009). In addition to RIPA, the U.K. parliament passed a series of anti-terrorism acts, which further expanded law enforcement capabilities to search and detain

suspects. The Terrorism Act 2000 and the Anti-Terrorism, Crime and Security Act 2001, the Criminal Justice Act 2003, the Prevention of Terrorism Act 2005, and The Terrorism Act 2006 all authorized significant police powers to detain, search, and interrogate those suspected of terrorist related activities. In some cases, police are authorized to stop and search individuals even if the officer has no grounds to suspect them ("The Criminal Justice Act 2003 (c. 44)", 2003).

The U.K. has a history of dealing with terrorist attacks. During the late 1960's and 1970's, the IRA conducted a widespread bombing campaign in Northern Ireland and England. In 1988, Pan Am Flight 103 was bombed as it flew over Lockerbie, Scotland, resulting in nearly 300 casualties. As a result, prior to September 11, 2001, the U.K. had anti-terrorism laws authorizing the surveillance, search, and detention of suspected terrorists. Anti-terrorism laws overlap specific privacy protections if the suspect is considered a threat to national security. Some laws allow for unlimited detention of suspected terrorists, the collection of private information such as photographs and DNA evidence, even without formal criminal charges or offense ("The Criminal Justice Act 2003 (c. 44)", 2003; , "The Prevention of Terrorism Act 2005", 2005; , "The Terrorism Act 2000 (c. 11)", 2000). An increase in anti-terrorism legislation and expanding permissible law enforcement behavior will most likely have a negative impact on privacy protection laws, especially if being suspected of broadly defined terrorism negates privacy protections citizens would otherwise be privy to. In a system with a singular veto point, a major terrorist event has the potential to have a substantial legislative impact.

In the U.K., the parliament updates and revises existing legislation when changing security situations mandate different or increased security measures. Starting with The Terrorism Act 2000, the U.K. passed a series of terrorism acts, and the changing provisions give insight on

the debate over civil liberties within the controlling party. Looking at the succession of acts passed, one would expect the concerns over national security to trump concerns over privacy closely following terrorist events. Considering the lack of veto points within the system, parliament should be able to quickly move policies toward creating a more security focused environment. On the other hand, if concerns over civil liberties become an issue for the controlling party, it should be reflected in measures easing some of the more intrusive provisions in the next round of legislation.

Pre-9/11 anti-terrorism legislation in the U.K. was written with the domestic terrorism of the IRA in mind. The Terrorism Act of 2000 broadly defined terrorism as “the use or threat of action... is designed to influence the government or to intimidate the public or a section of the public, and…is made for the purpose of advancing a political, religious or ideological cause” ("The Terrorism Act 2000 (c. 11)", 2000, Part I). Suspected terrorists under this act could only be held for a maximum of 48 hours without being charged, and only persons designated as constables could rightfully search and seize property from those suspected of terrorism ("The Terrorism Act 2000 (c. 11)", 2000, Part V). Following the attacks on 9/11, however, the Anti-terrorism, Crime and Security Act (ACSA) expanded the power of law enforcement to search and detain suspects. Whereas previously police would have to show grounds for searching or detaining a suspected terrorist, under the ACSA “a constable may in the exercise of those powers stop any person or vehicle and make any search he thinks fit whether or not he has any grounds for suspecting that the person or vehicle is carrying weapons or dangerous instruments” ("Anti-Terrorism, Crime and Security Act 2001 (c. 24)", 2001, Part 10). In Part 4, law enforcement was also granted the ability to indefinitely detain an international terrorism suspect without charge. This controversial provision was challenged in the courts, and has since been repealed, as there

was no designation between a foreign national or a citizen, and under U.K. law and the European Convention on Human Rights (ECHR), citizens cannot be detained indefinitely without a trial.

Data Collection, Protection and Surveillance

Governments maintain their own databases of information about citizens and non-citizens, including criminal histories, civil court cases, tax information, traffic citations, immigration records, and biometric information, such as fingerprints, are maintained by government agencies. The United States and the EU have also recently considered, or adopted, measures to fingerprint all incoming foreign visitors and store the information in databases. The U.S. claims such information is necessary to combat the threat of terrorism, but privacy advocates argue that there is little proof in the measures effectiveness, and a high chance that the information could be lost, stolen, tampered with, or otherwise abused.

The U.S. and the U.K. have also been pursuing an increased amount of domestic surveillance under the pretext of national security and the prevention of terrorism, though the tactics of the U.S. government are arguably the most publicized. Both countries have begun watching their citizens by installing vast networks of CCTV cameras, or through less obvious efforts like sifting through emails, telephone records or internet browsing habits. Technological development has allowed governments to intercept and tap phone calls, install key stroke logs on suspected criminals' computers, track GPS devices or cell phones to locate individuals, use radio frequency identification (RFID) tags to store retrievable information about individuals, scan heat signatures through the walls of private residences, and soon there is the possibility that unmanned drones will conduct warrantless aerial surveillance of major cities (Wise, 2007). Without a legal apparatus designed to protect the privacy of citizens, these technologies could

easily be abused. Accompanied by any radical shifts in government power, the implications are frighteningly dystopian.

Sometimes citizens are apprised of security efforts, such as in the United Kingdom, where the existence of a countrywide video surveillance program has been touted by the government as a crime deterrent. "There are an estimated 4.2 million CCTV cameras in Britain", some with interactive capabilities, which is roughly equal to 14.5 people per camera based on projected population figures for July 2008 ("CIA World FactBook: United Kingdom", 2008; , "'Talking' CCTV scolds offenders", 2007). While the surveillance is overt, and people seem to be generally accepting of the presence of CCTV, has it altered their right to privacy? Or is privacy, as some have suggested, not a right but a good possessed by individuals within their specific socio-cultural framework, and tradable as such for other goods? In which case, the British are simply trading their privacy for increased security proxied by the presence of CCTV. However, the mere knowledge that someone is watching has the ability to alter an individual's behavior. Pervasive, systematic monitoring of citizen emails, phone calls, reading habits, and political opinions can have a chilling effect on public discourse, especially if the opinions are perceived to be anti-government or anti-establishment. This type of alteration could limit freedoms otherwise expected under democratic government, such as free expression, religion, and political opinions. Furthermore, if the goals of surveillance became ambiguous or blurred, there is certainly a risk that the government will begin to abuse its powers much more radically. In classic dystopian visions, it is when the government begins to abuse the power of surveillance that dissent, protest, and disagreeing with the government start to be monitored, or worse, punished. Classic American examples include McCarthyism and J. Edgar Hoover's notorious reign over the FBI during the Cold War. Suspected Communists were questioned, harassed, followed and often

times suffered more than just personal humiliation or insult. These historical events should serve as a reminder that allowing the government too much leeway into what should be private thoughts, opinions, and beliefs can have devastating effects on a democratic society.

Today, the breadth of the U.S. government's domestic spying program since 9/11 is now coming to light as new information is leaked to the press about warrantless wiretapping, the government's collusion with the telecommunications industry to obtain private records, and the surreptitious no-fly lists. *The New York Times*, *Wall Street Journal* and the *Washington Post* have all reported on aspects of the illegal wiretapping program, though the complete picture is still considered classified for national security reasons. What was once the Total Information Awareness program, a data mining project conducted at the Pentagon, is now a classified program, which sifts through vast databases of personal information looking for "suspicious patterns" (Gorman, 2008). The real extent of the threat to American's privacy rights is hidden, as long as the information about such programs remains secretive. Appropriate channels for citizens to find redress by such invasions of their privacy is less than obvious, and their ability to understand what information about themselves is collected, for what purposes, and by whom, is relatively non-existent.

Privacy Protections and Electronic Information

The government is not the only entity collecting, storing, and sifting through personal information. Corporations collect, buy, sell, and trade personal information they accumulate through transactions with consumers at all levels. Signing up for newsletters, magazines, credit cards, newspapers, special offers, contests, or general information allows a company to collect, store, and later sell individual's information. Most retail and services companies have special customer incentives to release personal information, such as access to special discounts, advance

sales notifications, and generally cheaper goods and services. Lengthy and highly legalistic privacy policy notifications accompany such registration, and oftentimes the consumer has little awareness that their information will be stored, shared, sold, or traded, and they are rarely informed to whom such information is sold. As a result, canceling one subscription does not necessarily negate the flow of information between the affiliated parties who have already purchased or received it.

Information is also collected through the internet, where online companies compile information about your purchase history, search terms, browsing habits, and personal tastes. Search engines like Google, Yahoo, and MSN maintain user search histories for over a year before anonymizing the data ("Search Engines Defend Your Privacy (To Target You Better)", 2007). Meaning every search conducted is indexed and personally identifiable. “In April [2007], Google launched its Web History service, which monitors all the sites someone visits if they use the Google toolbar” ("Search Engines Defend Your Privacy (To Target You Better)", 2007). This information is used to create behavioral profiles of users in order to target advertising or products at the individual level. Where privacy advocates find the most fault is that these profiles are maintained over a long period of time, and the companies reserve the right to use them how they see fit, even supplying them to the government upon request. Google, Microsoft’s MSN, Yahoo and AOL received subpoenas for a random sampling of millions of internet addresses cataloged in their databases, as well as for records for potentially billions of searches made over a one-week period. Only Google refused to comply (Godoy, 2006). Google cited privacy concerns for its users in its challenge of the subpoena. Privacy advocates applaud Google for resisting, but note that the information is still collected and maintained, which should be considered.

While internet privacy remains a huge concern, a more pervasive type of technology raises questions about corporate privacy standards. Radio Frequency Identification tags (RFID) "consists of a small integrated circuit attached to a tiny radio antenna, which can receive and transmit a radio signal" (van den Hoven, 2006). RFID tags can be embedded in just about anything, from clothing, personal accessories, ID badges, credit cards, passports, electronics, vehicles, animals, and even people.

> "RFID works by using a tag to transmit the identity and other properties of anything to which it is attached to a reader via radio frequency signals, allowing further information to be accessed in a computer database. This overcomes most physical barriers and can be accomplished almost invisibly" (McKee, 2006).

Useful applications for this technology abound – tracking and controlling manufacturing and supply chain logistics to minimize losses and theft, in-store theft prevention, tagging of wildlife for research, domestic animal tagging, etc. However, most items containing tags are not labeled as such. Consumers may be unaware that they are purchasing RFID tagged items, and may not be told if and when such items have transmitted information about the purchase. In the near future RFID "will be embedded in virtually everything you buy, wear, drive and read, allowing retailers and law enforcement to track consumer items - and, by extension, consumers - wherever they go, from a distance" (Lewan, 2008). Once purchases are linked to credit card or banking information, corporations then have the ability to identify purchasers and track consumers based on the products they buy. Walking into retail space becomes less than anonymous as RFID tags embedded in clothing, accessories, wallets, and credit cards transmit information about what an individual has purchased previously, what they are wearing, and what they are carrying. This kind of information could be used to ease the flow of transactions, but this "commodification of personal information can also have negative results for certain low-volume or otherwise undesirable customers. It might lead businesses to single out customers in order to discourage

their patronage" (Schwartz, 2004). If a consumer was felt this behavior was invading their privacy, would there be a way to 'opt-out' of participating in such scans? If not, will products containing RFID tags be properly labeled, will the tags be identifiable and removable? Such issues should be considered as this technology becomes more prevalent.

There are also voluntary methods of storing personal information using RFID technology. Schwartz (2004) identifies VeriChip and wOznet as two such technologies, identification devices that store, track, and monitor persons and personal information. The VeriChip is an implantable device that "stores six lines of text, which function as a personal ID number, and emits a 125-kilohertz radio signal to a special receiver that can read the text" (Schwartz, 2004). The accessible database holds personal information like age, name, address, medical history, and could potentially be used as a verification system for banking, financial transactions, passports, and travel.

Surveillance Society?

> *"My anxiety is that we don't sleepwalk into a surveillance society where much more information is collected about people, accessible to far more people shared across many more boundaries than British society would feel comfortable with.." – Richard Thomas, Information Commission, United Kingdom (Ford, 2004, p. 1)*

As Richard Thomas fears, it is entirely possible for both the US and UK to sleepwalk into a surveillance society, if they have not already. This reasonably assumes that liberal democratic societies value individual liberty over security to a certain extent, and that a true surveillance society would violate those fundamental values. Maintaining individual privacy is key to maintaining the ability of individuals to choose their own religion, hold minority political views, express unpopular opinions, and participate in activities outside mainstream society. "Government protection of privacy rights is a measure of society's commitment to liberty"

however, “the existence of political community requires the relinquishment of certain rights, prerogatives, and freedoms” (Krotoszynski, 1990, p. 1398). Finding a balance between these opposing forces has been the bedrock of liberal democratic societies. Leaning too heavily in favor of government power and control over the individual verges on tyranny, and leaves the government room to commit abuses of its power, which democratic societies have sought to avoid.

Government surveillance is only one facet of the complex issue of individual privacy. Technological advances in the internet, the proliferation of online purchasing, and RFID tags have allowed corporations to collect and store a vast amount of consumer data quietly, and the protection and uses of such data are often less than transparent. Every business that collects personal information has a privacy policy where they outline what information they collect, who they distribute it to, and generally provide a section where an individual can decide whether or not they wish to have their information shared. They are hardly ever decipherable without a legal degree, written in obtuse language, and tend to be unnecessarily long and complicated. Consumers’ ability to read and understand these policies are limited at best, leaving corporations room to collect, store, and distribute more information than consumers may be aware. Do these states acknowledge the potential for abuse from corporations, and what protections are available for citizens under their laws? The current trend in both states is that government is asking for increased access to consumer information, and in the case of internet service providers (ISPs), increased retention of personal digital records including search terms, purchase histories, and emails. Since governments are demanding help from corporations to track individuals, it would be reasonable to assume that they are benefiting from the increased information gathering of corporations.

As far as privacy rights are concerned in the digital age, carefully constructed data management and security, qualified and competent oversight, and a transparent surveillance system are necessary to keep abuses of power in check. Do either the U.S. or the U.K. present a clear and reasoned acknowledgement of the dangers of abusing personal information, and are there protections against invasion of privacy for citizens? Do they consider the pace at which technological development will alter the ease at which such information is collected, and what do they intend to do to protect individual privacy rights? It is not to suggest that technological advancements should in any way be shunned or avoided, and technology cannot be blamed for the harm perpetrated in its name. However, thinking about the future requires an understanding of how technology is progressing, and how to deal with the challenges new systems will present to existing legislatures. Can these states adapt to such changes in technology in a timely and appropriate manner, or will technological advancements outstrip the ability of the government to successfully keep up?

The goal of this thesis is to compare the privacy protection regimes in the United States and the United Kingdom in order to explore the above questions. While both states are democratic, there are many differences between both government structure and institutional arrangements, and these variations may explain important differences in the manner in which privacy policies are implemented.

CHAPTER 3: THEORETICAL FRAMEWORK

Veto Points Literature

Before 2000, the U.S. had been expanding the privacy rights regime and incorporating technological developments into existing views regarding what information and actions should be protected under existing laws. The U.K., albeit slowly, had advanced a more limited privacy rights agenda, although it was starting to move more in line with the European Convention on Human Rights (ECHR). After the attacks on September 11, 2001, however, there was a dramatic shift in attitudes about personal privacy in both states. Safety and the prevention of violence became the focal point of national discourse, and the security apparatus of the state was given precedence. In this thesis I examine the institutional determinants of individual privacy protection policy in the U.S. and the U.K. In other words, is there a relationship between the institutional structure and privacy protection? How do the institutional arrangements shape the way privacy policies are formed and implemented? Using the events of September 11 as a starting point, this thesis analyzes how the institutional structure of the U.S. or the U.K. affected the levels of privacy protection available for citizens.

The veto points literature offers a framework through which to analyze how institutional structure affects policy-making. The literature defines a veto point as an institution that can affect the decision making process. O'Reilly finds that "a more *fragmented* state has more veto points within it, which increases the difficulty of altering levels of" policy change (O'Reilly, 2005, p. 653). Additionally, the literature identifies a veto player as an actor or collective actor who can affect the decision making process. "Generally, the literature of veto players asserts that particular constitutional configurations shape aggregate policy outcomes" (Minnich, 2005, p. 304). Tsebelis identifies two dimensions that affect policy changes, the number of veto points

and players, and the ideological proximity of veto players (Tsebelis, 1995, 1999, 2000). Institutional arrangements such as parliamentary or presidential systems, unicameral or bicameral houses, federalism, and partisan politics contribute to how policy is created, altered, compromised, rejected, or passed. To begin,

> "Fundamental to the theory of veto points is that, the more of them that exist, the more difficult it is to change policy, or in Tsebelis's (1999) useful definition, 'a veto player is an individual or collective actor whose agreement is necessary for a change of the status quo'" (Crepaz, 2004, p. 261).

The more veto points in a system decrease the likelihood that a state can engage in dramatic policy reversals, or put differently "the more power is diffused among many actors, the more difficult it should be to affect policy change" (Crepaz, 2004, p. 261). Henisz and Mansfield examine the effect that fragmentation, measured by the number of veto points present in a country, has on commercial openness. They argue that "to the extent that the preferences of actors with veto power differ, institutional structures with more veto points limit the range of feasible trade policy choices" (Henisz, 2006, p. 191). They find that "holding macroeconomic conditions constant, the trade regime changes less within democracies as the number of veto points increases" (Henisz, 2006, p. 208). O'Reilly also analyzes the effects of veto points on international trade policy, specifically tariffs, and "the findings here suggest that fragmentation may have a considerable effect on the abilities of states to cooperate with each other in the issue area of foreign economic policy" (O'Reilly, 2005, pp. 667-668). These studies support the idea that policy changes will be affected by the institutional structure of a state.

The U.S. is a federal, constitutional, and presidential system, and the power of government is decentralized so that no one branch or party can dictate policy for the entire nation. In the U.S., veto points are identified as the both houses of Congress, the President, and the Supreme Court, and the veto players as the Democratic and Republican parties. Ultimately,

the U.S. president's veto power can be overridden by a two-thirds majority in the Congress, but it's a difficult majority to obtain and allows the president's veto to remain effective. The constitutional system of checks and balances in the U.S. implies that there will be more oversight in the policy making process than there would be in the parliamentary system as two branches of government must approve of legislation before it can become binding law, and the Supreme Court is the final arbiter if and when such laws are challenged. Each branch of government potentially has veto power over the next, creating a system where the branches essentially compete for power with each other, thereby reducing the chance that one branch will be able to completely control the government.

On the other hand, the U.K. is a unitary, parliamentary system, with a highly centralized power structure. The party with the overall majority in elections forms a government, a cabinet, and selects a party member to the position of Prime Minister.

> "The British Parliament and its mechanism of fusion between executive and legislative power and parliamentary systems with single-member district electoral systems in general constitute only one veto point, because the prime minister emerges out of the majority party in Parliament reducing institutional competition" (Crepaz, 2004, p. 261).

Policy is created according to the party's goals, and opposition parties challenge those goals in open debate. Thus, as long as the controlling party wins an absolute majority and does not have to form a coalition government, it can create and implement policies without the support of the opposition parties, offering only one check on legislative power. There are a number of informal veto players in the U.K., however. Since the Prime Minister is selected by the majority party, (s)he depends on the support of the party, and if (s)he does not conform to the party's view a vote of no confidence can remove the Prime Minister from power. In addition, while the opposition party and the House of Lords hold very little power to stop legislation from being

passed, their dissenting opinions are signals to the public that certain courses of action are not unanimously approved.

Even taking informal veto players into context, the U.K. still has comparatively fewer veto points and players than the U.S., and I would expect that the British government should be able to more quickly create and change policies in response to the new security environment, and could be prone to changes in privacy policy due to less constraints on power. In other words, a larger (smaller) number of veto points and veto players would be associated with less (greater) policy change in response to the changing security environment after 9/11.

However, in addition to analyzing how fragmentation influences policy choices, the partisan preferences of the actors involved in policy making should be taken into account. The institutional literature is also concerned with the ideological identification of the different veto players, and "as the ideological distance among veto players increases, policy stability increases" (Tsebelis, 2000, p. 448). If veto points are controlled by the different political parties (veto players), the theory predicts policy stability, as changes to the status quo become harder to obtain. However, when the veto points are controlled by partisan players with similar interests "there is a condition of congruence among the institutions, and the relevant veto player is the party that controls the institutions" (O'Reilly, 2005, p. 657). Thus, the effective number of veto players can vary as the majority in the houses of Congress and control of the executive branch vary after elections. Hammond, finds that "as a general rule, then, policy choices by a system must be seen as the product of an interaction between the policy-making rules and the preferences of the actors in the system" (Krause, 2003, p. 102). Even if the veto players have different partisan identities, it doesn't necessarily mean their preferences will automatically diverge. If there is widespread support for a particular policy outcome, i.e. increased security

after the events of 9/11, policy preferences may converge, despite the number of veto players. Thus, when attempting to analyze the affect of institutional structure on privacy protection, this research must take into account not only the institutional veto points, but also the preferences of the actors involved in the policy-making process.

> "Institutional veto players are usually determined in the constitution of a country, and while partisan veto players can change number, the overall picture is one of relative stability. For example, in the UK there is always one veto player, in the United States always three (although their ideological distance from each other may vary)" (Tsebelis, 2000, p. 469).

However, some findings have shown that the preferences of actors in presidential and parliamentarian systems can be predicted as similar, depending upon the alignment of veto points.

> "Instead, differences in policy stability between two different kinds of systems depend on the *interaction* between the number of veto points and the distribution of preferences…of the elected officials populating the veto points in the two kinds of systems. In fact, it was demonstrated that for some preference profiles presidential and parliamentary systems should be expected to select similar policies and exhibit similar patterns of policy change, despite the systems' institutional differences" (Krause, 2003, p. 76).

This is not to say that presidential and parliamentary systems will always behave in the same way, but that there are certain 'preference profiles' that will allow these systems to behave in the same manner. Policy choices are made by actors with differing preferences, and usually result in compromises. A preference profile is the set of policy choices a particular actor will be willing to accept (Krause, 2003). Similar ideological backgrounds, such as party affiliations, identify what an actor's preference profile will generally be. The colored sections of the graphic below represent the varying policy compromises each of the actors would be willing to accept. Figure 1 represents actors with farther distance between their policy preferences than the actors in Figure 2.

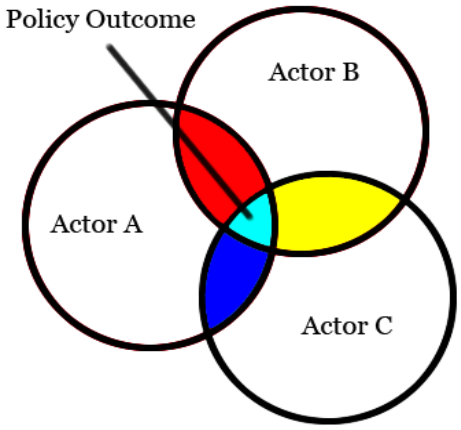

Figure 1: Policy outcomes, dissimilar ideological preferences[4]

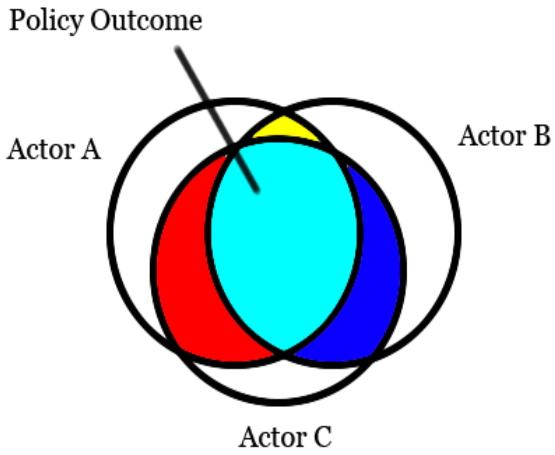

Figure 2: Policy outcome, similar ideological preferences

As actors' policy preferences converge, the set of policy outcomes they would be willing to accept grows, and the possibility of policy change increases. As actors' preferences diverge, the set of acceptable policy outcomes shrinks, translating into increased policy stability, in most cases.

[4] Figures 1 and 2 adapted from Tsebelis (1999).

Therefore, despite the fact that the U.S. government has a system of checks and balances, due to a convergence of veto player preferences following 9/11, the Bush administration was able to push through a significant amount of legislation governing surveillance and intelligence gathering laws, and amass power in the presidential office, essentially circumventing oversight by keeping surveillance programs secretive and under bureaucratic control. Furthermore, when Congress eventually demanded information about surveillance programs, the Bush administration claimed expanded powers under the War Powers clause. Oversight, checks and balances, and restraints on power only function properly if policies and laws are created within the established policy-making system. Circumventing the veto points essentially negates their effect.

The expectation is that when the veto players with similar policy preferences or ideological convergence, there is a greater potential for policy change, and specific to this research, a greater possibility of change in privacy protections in response to security threats. With this in mind, the policy change in the U.S. and U.K may be more similar than different as both countries experience periods of time where veto players have closer proximity. During the time period from 2000 until the 2003 invasion of Iraq, the U.K. experienced a strong preference convergence due to popularity of the Blair administration and the Labor Party. In the U.S., following the attacks on 9/11 until after the 2004 elections, there is also a strong preference convergence. Both countries should be able to accomplish desired policy changes with little resistance during these time periods, as veto players are ideologically aligned. If policy preferences of these administrations include enhancing law enforcement capabilities to enhance security domestically, and thereby reduce privacy rights, then it is expected that these goals will be accomplished.

A strong argument could be made that any sweeping policy changes during the time period could be attributed to partisan politics in the U.S. From the 2002 to the 2006 election cycles, Republicans held majorities in both houses of Congress and the presidency. During that period, it is entirely possible that partisan politics could account for policy choices, although this is still consistent with Krause's argument that the distribution of preferences among actors determines policy outcomes. Since these U.S. institutional veto points are controlled by a single party, it would be expected to act similarly to a parliamentary system, despite institutional variations. Interestingly, the most widespread change to government intelligence gathering and law enforcement activity in the U.S. is the USA PATRIOT Act of 2001. The PATRIOT Act expanded the government's surveillance and intelligence gathering powers by augmenting existing laws, and passed an evenly divided Senate with an overwhelming majority of 96-1, and the House, with a modest Republican majority, passed the bill 356-66. While partisan politics cannot account for this, the overwhelming support the PATRIOT Act received could be attributed to the "the fog of uncertainty, emotions such as urgency and visceral fear, and the tendency of legislators and the public to 'rally 'round the flag'" after 9/11 (Vermeule, 2008, p. 1155). A surge in nationalism and the 'rally' effect would also produce a convergence of player preferences, and explain the policy outcomes regardless of ideological affiliations.

Research Design

The goal of this research is to analyze how variation in the institutional arrangements across the U.S. and U.K. allowed for more or less protection of privacy rights for citizens. The veto points literature provides the framework for institutional comparison, and suggests that the number of veto points and ideological proximity of veto players have an effect on the formulation of policy. This leaves two important questions about measuring policy change. 1.

How to measure which country has more privacy protections for its citizens?, and 2. How to measure more (or less) privacy protection for its citizens over time? In order to answer the first question, it is necessary to devise a reasonably consistent and objective system to catalog the existing privacy protections in each country at a specified time. Subsequently, a later date must be set in order to measure if and how the protections have changed. For the purposes of this thesis, the time period over which changes in privacy protections are to be estimated is from the year 2000-2006.

Privacy is an ambiguous term, and laws governing privacy have situational components, therefore I conduct a qualitative study to examine what protections exist under the laws of the country to protect citizens from intrusive searches, seizures, and surveillance. The government regulates the investigation of suspected criminal activity, terrorist activity, and espionage, and provides guidelines for law enforcement organizations to follow when they conduct investigations and authorize surveillance activities. Comparing qualitatively across countries is appropriate here since the countries treat similar investigations differently, and different levels of surveillance are authorized based on the type of investigation. For example, the investigation of criminal activity has an extra component in the U.K., as some crimes are considered regular criminal activity and some are considered serious criminal activity, a designation reserved for crimes like narcotics or human trafficking and homicide.

The comparative case study will analyze the activities authorized by the government as they pertain to privacy protections, and list the relevant laws. Two tables provide a listing of the relevant legislation dealing with law enforcement capabilities and privacy protections. Table 1 provides the relevant legislation up to 2000, and Table 2 from 2001 to 2006. A discussion of the specific laws and procedures follows each set of tables, so an overall view of the laws regulating

law enforcement agencies' capabilities in each country can be measured. By discussing each aspect of these laws independently, privacy protections can be inferred from the presence (absence) of expansions in law enforcement capabilities. The research can then determine if there has been an increase or decrease in privacy protections based upon this assessment.

Searches, seizures and surveillance are regulated by a complex system of laws, therefore, it is possible for the activities sanctioned by the government to broaden in one area, such as wiretapping, but contract in another, such as email interception. It would be difficult to objectively determine if the expansion of government power in one area should be considered more intrusive than expansion in another. For example, assume that use of closed-circuit television cameras (CCTV) in public areas expands and that wiretapping laws become less strict. It is impossible to gauge which action causes a loss of more privacy, and that type of evaluation may not even be desirable. Where one individual would find increased audio surveillance more intrusive, another may determine that video surveillance is more so. However, it is reasonable to assume that since government powers of surveillance increase in both situations, that there is a net loss to privacy.

Once changes in privacy protections over time have been determined, it is then possible to evaluate if the variation in institutional arrangement and the ideological proximity of veto players have affected policy outcomes. Government transparency, or the lack thereof, creates a certain amount of difficulty in truly establishing a measure of privacy protection. Programs that operate in secrecy or without oversight may infringe on privacy rights otherwise afforded to citizens, and if possible, should be included in the overall analysis. Where possible, such programs are discussed.

CHAPTER 4: COMPARATIVE CASE STUDIES AND RESULTS

Surveillance, Data Protection and Law Enforcement Regulations

Technological developments in the late 1980's and early 1990's began transforming the surveillance landscape. Personal computers, the internet, and the widespread use of cell phones increased information sharing capacities for individuals and governments alike. Technological advances in communications technology made it easier to share information across great distances rapidly and cheaply, and the internet allowed these activities to be anonymous information exchanges. Such developments also precipitated an increased capacity to record and retain information, and created a "broader network of surveillance activities that now assumes a remarkable array of forms, including sensors, bureaucratic documentation, x-rays, satellites, and computerized databases" (Haggerty, 2005, p. 170). Closed-circuit TV (CCTV) security systems monitor public places, businesses, roadways, and residential areas 24 hours a day, some have facial recognition technology, internet traffic and emails can be monitored by law enforcement agencies, and sophisticated databases have been built to track DNA, fingerprints, and spending and travel patterns. How this information is gathered, processed and used is governed by a complicated series of statutes, laws, and policies in both the U.S. and U.K.

Tables 1 and 2 in the following section provide lists of the major laws governing these surveillance activities in the U.S. and U.K. A discussion of the laws follows, including the *de facto* range of search, seizure, and surveillance activities the governments were participating in both inside and outside the scope of the legislation. For example, while a warrant is legally required in order to conduct covert interception of communications, the U.S. and U.K. were conducting communications intercept activities in the 1990's through controversial programs such as ECHELON (Bedan, 2007). The ECHELON program was a joint effort between the U.S.,

U.K., and other countries, to actively intercept satellite communications signals in order to gather intelligence about national security threats. ECHELON works by capturing communications signals and combing through the data for keywords that could be consistent with criminal or terrorist activity (Wallace, 2000). Programs like ECHELON, which operate secretly and with little noticeable impact on the general public, complicate the measurement of privacy protections because they conduct their activities on such a large scale and in the classified realm of national security. Classified programs complicate measurement on two levels. The first being that the programs are not transparent, and there is no way to gauge if they are breaking existing privacy laws if their actions are not documented or available for oversight. Secondly, the scope of such programs is often unknown. Nonetheless, it has been rumored that the capabilities of ECHELON include collecting "as many as 3 billion communications a day, and sift[ing] through 90% of all Internet traffic" (Nabbali, 2004, p. 92). Even if such estimates cannot be independently verified due to the classified nature of the program, they cannot be completely ignored. However, the aim of this research is not to examine the full implementation of privacy protection protocols, but rather to discuss policy changes over time. Where it is appropriate, classified programs are discussed, despite the uncertainty surrounding their capabilities, scope, and legality.

Privacy Protections and Government Regulations in 2000

Table 1 provides a list of the laws governing surveillance, data protection, and law enforcement activities up to and including the year 2000 in the U.S. and U.K. These statutes provide the standards which law enforcement and government agencies must adhere to during investigations, and through their limits, define the areas where citizens can expect their privacy to be protected. By examining these laws and then comparing any changes over time, it becomes possible to gauge if the amount of personal information, actions, and communications the

government has access to increases or decreases. For example, the U.S. Cable Communications Privacy Act of 1986 (CCPA) states that cable companies cannot divulge consumers' personal information without

> "a court order only if…(1) such entity offers clear and convincing evidence that the subject of the information is reasonably suspected of engaging in criminal activity and that the information sought would be material evidence in the case; and (2) the subject of the information is afforded the opportunity to appear and contest such entity's claim" ("Cable Communications Policy Act of 1984 (Cable Act)", 1986).

If a law passed that does not require the requesting agency to provide evidence that the subject is suspected of criminal activity in order to obtain a court order, or the agency can access the information without a court order, it is reasonable to assume that privacy protections have decreased.

Table 1: Laws governing surveillance and privacy to 2000

United States	United Kingdom
Federal Intelligence Surveillance Act (FISA) Privacy Protection Act of 1980 (PPA) Cable Communications Policy Act of 1984 (CCPA) The Electronic Communications Privacy Act of 1986 (ECPA) Video Privacy Protection Act of 1988 (VPPA)	European Convention on Human Rights (ECHR) Data Protection Act of 1998 Regulation of Investigatory Powers Act 2000 (RIPA) The Terrorism Act 2000
Communications Assistance for Law Enforcement Act of 1994 (CALEA)	

Two major pieces of legislation govern law enforcement activities in the United States in 2000, the Fourth Amendment and the Federal Intelligence Surveillance Act (FISA). Fourth Amendment protections have been recorded into the U.S. Code under Title 18: Crimes and Criminal Procedures, Parts I and II, and Title 47: Interception of Digital and Other Communications. U.S. Code, under these sections, state that only authorized government agents or law enforcement agencies with a court order (or warrant) may intercept oral or electronic communications, install wiretaps, pen registers, and/or trap and trace devices, access stored communications data, and access personal information from telecommunications providers. A specific person has to be identified in order for a warrant to be issued, and specific conversations

are targeted. The only exception to these requirements is if the authorized government agent or law enforcement agency is conducting these activities under FISA provisions. FISA allows for warrantless searches, seizures, and communications interceptions when the subject is a foreign power, but does require a FISA court order in order to conduct such activities on a U.S. person ("The Foreign Intelligence Surveillance Act", 1978). Neither law enforcement nor authorized government agents can intercept the communications of or surveil U.S. persons without a court order or warrant. Law enforcement agencies can conduct legal search and seizures if probable cause can be established, such as searching the car of a person who fails a sobriety test for more drugs or alcohol. The Cable Communications Policy Act of 1984 (CCPA) and the Video Privacy Protection Act of 1988 (VPPA) protect consumers from having their personal information divulged to any requesting parties without a court order. For example, cable providers and video rental outlets cannot divulge rental or subscription preferences, histories, or records to third parties without a court order, and when requesting a court order, the law enforcement agency must submit evidence to the court that the information sought is relevant to suspected criminal activities ("Cable Communications Policy Act of 1984 (Cable Act)", 1986; , "Video Privacy Protection Act", 1988).

Another piece of legislation with implications for privacy protections is the Communications Assistance for Law Enforcement Act of 1994 (CALEA), which requires “that digitally switched telephone networks be designed and built with wiretap capabilities and that service providers assist [Law Enforcement Agencies] in obtaining the desired surveillance” (Guhl, 2008, p. 110). Part of the provisions of CALEA is that neither the targeted party nor the telecom provider should be aware of surveillance conducted on the line. These backdoors built into the digital system were to allow law enforcement agencies easy access to all forms of

communication if the need to access them arose (Guhl, 2008). These built in protocols are worrisome because of their anonymity. If neither the provider nor the subject is able to detect the surveillance, the burden of trust is on law enforcement agencies not to misuse the technology. While a warrant is required for law enforcement agencies to access the backdoors, and misuse of the technology clearly falls under implementation of the law, it is still important to note the possibility exists for abuse of the system.

The above laws state that the government cannot conduct domestic surveillance or investigations without obtaining a warrant, either through a traditional court, or through the FISA court. However, as Bedan points out "U.S. Constitutional law has always recognized a distinction between intelligence gathering and intelligence sharing. The central difference between the two is that intelligence gathering…is typically limited by statutory and constitutional requirements, where intelligence sharing typically is not" (Bedan, 2007, p. 441). This difference is what makes programs such as ECHELON disturbing. Any of the other countries participating in the program could conceivably conduct investigations of U.S. citizens and voluntarily turn the information over to U.S. authorities without being subject to Fourth Amendment or FISA requirements. Since ECHELON was a classified program conducted by the National Security Agency (NSA) with little or no public oversight, the extent of such information sharing activities is not known. However, does circumventing Fourth Amendment and FISA provisions effectively negate their ability to protect the privacy rights of citizens? The answer is not always. U.S. courts are still afforded the opportunity to determine whether or not the evidence obtained through such methods is admissible in court, and offer the subjects of such surveillance the opportunity to argue against the permissibility of such evidence.

Privacy protections are far less obvious in the U.S. concerning CCTV camera operation. There is surprisingly little mentioned in U.S. federal law about CCTV camera usage, regulations, or requirements, other than laws against video voyeurism and covert audio capabilities. CCTV cameras capturing sound are subject to U.S. wiretap laws, and unauthorized recordings are illegal based on U.S. Code, Title 18:

> “any person who – intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when—(i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication…shall be punished as provided in subsection (4) or shall be subject to suit as provided in subsection (5)” ("U.S.C. Title 18, Part I, Chapter 119").

In another section of Title 18, the government makes illegal any action by a person “to capture an image of a private area of an individual without their consent, and knowingly does so under circumstances in which the individual has a reasonable expectation of privacy” ("U.S.C. Title 18, Part I, Chapter 88"). Beyond these two statutes, there are no regulations governing the implementation of CCTV cameras at the federal level. This is particularly problematic as access to CCTV technologies reaches the mainstream, and video capture technology becomes more prevalent.

In the U.K., the warrant requirements under the Regulation of Investigatory Powers Act of 2000 (RIPA) specifiy that

> “an interception warrant must name or describe either— (a) one person as the interception subject; or (b) a single set of premises as the premises in relation to which the interception to which the warrant relates is to take place” ("Regulation of Investigatory Powers Act", 2000).

By identifying a location or a set of locations, as viable subjects, RIPA authorizes surveillance of all persons communicating from those places, which could include monitoring or recording the conversations of innocent people. In addition, RIPA warrants

> "shall be taken to include—(a) all such conduct (*including the interception of communications not identified by the warrant*) as it is necessary to undertake in order to do what is expressly authorised or required by the warrant; (b) conduct for obtaining related communications data" ("Regulation of Investigatory Powers Act", 2000, emphasis added).

Unlike U.S. warrant requirements, which state specific conversations must be targeted, RIPA expands the interception to include even those communications not targeted by the warrant. Furthermore, "related communications data" is not clarified, leaving the warrant open to intercept an indefinite amount of information. Another section of RIPA requires that if intercepted communications are found to be password protected or encrypted, internet service providers and/or the subject of the investigation must provide password and decryption information.

> "It is highly unrealistic to expect people and ISP's to remember all such information. It becomes a serious problem when a fine can be imposed or indeed a prison sentence can be imposed for what in some circumstances is mere forgetfulness and absent-mindedness as opposed to criminal intent" (Reid, 2001, p. 190).

In 2000, the U.K. was already employing CCTV cameras in major cities, shopping centers, and residential areas, and the government encouraged their spread through funding and public statements. CCTV operation generally covers public spaces, although personal CCTV cameras can capture images on private property and in residential areas, and is covered by the Data Protection Act of 1998 (DPA) ("Data Protection Act (c. 29)", 1998). There is no warrant requirement for conducting CCTV surveillance, and anyone can purchase and install a surveillance camera on their property, including municipalities. Operators must register their CCTV system with the Information Commissioner, and when doing so, are provided with a list

of regulations concerning their operation. The Data Protection Act identifies recorded images as personal data or sensitive person data, and requires that:

> "A person must not knowingly or recklessly, without the consent of the data controller—(a) obtain or disclose personal data or the information contained in personal data, or (b) procure the disclosure to another person of the information contained in personal data" ("Data Protection Act (c. 29)", 1998).

Once a CCTV operator records personal information, they would be violating the Data Protection Act by distributing it to a third party, with the exception that disclosure of the information would prevent or expose criminal activity. With an ever expanding number of CCTV cameras in the millions in operation, enforcement of these regulations is probably quite lax. Widespread use of CCTV Nonetheless, the U.K. outlines legal behavior and provides a regulatory structure to CCTV usage where the U.S. does not. How these policies are implemented and the scope of such programs may differ greatly, however, and it outside the realm of this research.

The Terrorism Act of 2000 contains language that allows "any constable in uniform" to stop any vehicle or pedestrian and "search the vehicle; the driver of the vehicle; a passenger in the vehicle; anything in or on the vehicle or carried by the driver or a passenger;…the pedestrian; anything carried by him" as long as (s)he "considers it expedient for the prevention of acts of terrorism" ("The Terrorism Act 2000 (c. 11)", 2000, s. 44). This clause essentially provides law enforcement with blanket search and seizure capabilities, as terrorism is broadly defined and includes acts of "serious violence against a person; [or] involves serious damage to property" ("The Terrorism Act 2000 (c. 11)", 2000). Furthermore, "Under the new measure, a suspected terrorist can be arrested without a warrant and detained for up to a week without charge" (CNN.com, 2001). With such a broad definition of terrorism, and suspension of due process, the act leaves room for misinterpretation and abuse.

Privacy Protections and Government Regulations in 2006

Several new bills regulating surveillance activities were passed in the U.S. and U.K. between 2000 and 2006, and are listed in the table below. Following the 9/11 attacks, both the U.S. and U.K. sought to strengthen internal security by creating or modifying anti-terrorism laws. The actions authorized under these newer laws will be compared to what was authorized in the previous section, and the change in privacy protections over time will be evaluated.

Table 2: Laws governing surveillance and privacy 2001-2006

United States	United Kingdom
Authorization for Use of Military Force Against Terrorists 2001	Anti-terrorism, Crime and Security Act 2001
USA PATRIOT Act 2001	Serious Organised Crime and Police Act 2005 (SOCPA)
Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)	Identity Cards Act 2006
USA PATRIOT and Terrorism Prevention Reauthorization Act of 2006	Terrorism Act 2006

A week after 9/11 the House and Senate passed the Authorization for Use of Military Force Against Terrorists (AUMF) which provided the president with the "authority under the Constitution to take action to deter and prevent acts of international terrorism against the United States" ("Authorization for Use of Military Force Against Terrorists", 2001). While the act does appear to affect privacy rights, the AUMF was cited by the Bush Administration as the authorization to conduct warrantless wiretapping of terrorist suspects. "[T]he Bush administration's argument is that the Authorization for Use of Military Force allows wiretapping of suspected terrorists without FISA court approval" (Wolly, 2006). Warrantless wiretapping completely sidesteps FISA laws, and all other relevant privacy protections. This is an ambiguous issue of both implementation and policy. The Bush administration argued that warrantless wiretapping was permissible under AUMF since the Act authorizes the president to conduct any actions he deems necessary to protect the U.S. from terrorism. Congress finds serious fault with this broad assumption of executive power and completely denies that warrantless wiretapping is

authorized by AUMF (Wolly, 2006). Regardless, warrantless wiretapping was conducted by the NSA, authorized by Bush administration officials under this act for a number of years following the 9/11 attacks. As with ECHELON program, the true scope of the warrantless wiretapping issue is hard to assess while it remains classified, but it would be unwise to completely ignore it as the privacy of citizens is affected.

The second major piece of legislation passed in the U.S. after 9/11 was the USA PATRIOT Act. The PATRIOT Act modified sections of the Foreign Intelligence Surveillance Act (FISA), the Privacy Protection Act of 1980 (PPA), the Cable Communications Policy Act of 1984 (CCPA), The Electronic Communications Privacy Act of 1986 (ECPA), and the Video Privacy Protection Act of 1988 (VPPA). One of the most sweeping modifications to these acts is found in Section 215, the ability of investigating government agencies to obtain information without a warrant about personal purchases, library records, video rental records, business records, and a host of other records without having to disclose that the information was sought. The government agencies used National Security Letters (NSLs) to obtain the information and inform the organization that they were also not allowed to disclose to anyone what information was provided to the government. The text from this section is provided below:

> “An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a). No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section. A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production” ("USA PATRIOT Act", 2001, s. 215).

In addition to stripping the previous privacy protections of the CCPA, ECPA, VPPA, and FISA, section 215 does not require the investigating agency to apply for a warrant or show probably cause that the subject under investigation has committed or intends to commit a crime, or inform

the subject that his or her records have been obtained. This clause also seems to run contrary to the Fourth Amendment warrant requirement, however deciding the constitutionality of the Act is outside the scope of this paper. Nonetheless, it seems to disregard even Fourth Amendment protections, and should be considered a reduction in overall privacy protections.

In addition, the PATRIOT Act expands government investigatory powers to incorporate what it terms “domestic terrorism” including “activities that involve acts dangerous to human life that are a violation of the criminal laws of the United States” ("USA PATRIOT Act", 2001, s. 802). Suspects of broadly defined domestic terrorism could then be subject to searches and seizures without a warrant. Searches conducted without warrants, and with delayed notification, could expand the scope of what is actually searched, as previous laws require warrants to be targeted at specific items or locations. For these above reasons, the PATRIOT Act significantly expands the government’s investigatory powers beyond the scope of what was authorized in 2000.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) also modifies an important definition of FISA. FISA authorizes broader surveillance of agents of a foreign power than it does U.S. citizens. A person is considered an agent of a foreign power under FISA when evidence supports they are working for a foreign power ("The Foreign Intelligence Surveillance Act", 1978). Title VI of IRTPA modifies this FISA requirement by authorizing surveillance of ‘lone wolf’ terrorists, whose connections to a foreign power cannot be established. This definition leaves open the possibility that the suspected terrorist could be a U.S. citizen, who cannot be tied to a foreign power, yet receives the same protections as foreign agent under FISA ("IRTPA", 2004). This expansion further lowers the wall between foreign and domestic intelligence gathering activities, and reduces privacy protections under FISA.

In March of 2006, Congress reauthorized most sections of the PATRIOT Act. The reauthorization did repeal some of the above provisions, including the gag order surrounding national security letters (NSLs), and the 'roving wiretap' provision that allowed the government to wiretap any phone an individual had access to (CNN.com, 2006). It also granted further oversight by requiring that the FBI report to Congress the ways in which the PATRIOT Act's powers were being used. President Bush issued a signing statement after the reauthorization in which he declared the Executive branch free to act under AUMF and "his constitutional authority to bypass a law" he deemed prohibitive of his ability to secure the nation against terrorist activity (Savage, 2006). So while Congress authorized a redacted a modest amount of investigatory powers, the Bush administration asserted that such protections may not apply to executive actions. Again, this may fall under implementation of the law, and not the actual policy changes. However, if the president authorized cabinet levels agencies such as the FBI to ignore even the slight amount of privacy protections Congress provided under the reauthorization, this would have an impact on overall privacy protections. Regardless, the reauthorization of the PATRIOT Act still included most of the provisions of the 2001 bill which decreased overall privacy protections since 2000.

The U.K. also passed major legislation following the attacks on 9/11 which expanded law enforcement capabilities. The Anti-Terrorism, Crime and Security Act 2001 authorized law enforcement to obtain fingerprints, search, and photograph a person detained as a suspected terrorist if it "will facilitate the ascertainment of that person's identity; and that person has refused to identify himself or the officer has reasonable grounds for suspecting that that person is not who he claims to be" ("Anti-Terrorism, Crime and Security Act 2001 (c. 24)", 2001, Part 10). The Act further permits law enforcement to stop and search any person or vehicle at any

time they feel “incidents involving serious violence may take place” and seize any item “he has reasonable grounds for suspecting to be an offensive weapon” even without charging the detainee with a crime ("Anti-Terrorism, Crime and Security Act 2001 (c. 24)", 2001, Part 10). This goes beyond previous privacy protections as the detainee does not actually have to be charged with a crime in order to be fingerprinted, photographed or searched, or a warrant provided to search and seize items.

In addition, Part 11 of the Act requires telecommunications providers to retain all communications data for a period of two years “for the purpose of safeguarding national security; or for the purposes of prevention or detection of crime or the prosecution of offenders which may relate directly or indirectly to national security” ("Anti-Terrorism, Crime and Security Act 2001 (c. 24)", 2001, Part 11). Such communications data would then be available for the government if and when an investigation took place. By requiring that telecommunications providers retain personal communications data, the government is basically authorizing pen register devices on all communications devices in the event that they *may* be needed at an unspecified time. This is clearly an expansion over the investigatory powers allowed in 2000, and decreases privacy protections covering communications within the U.K.

In 2005, the parliament passed the Serious Organised Crime and Police Act (SOCPA), which gave law enforcement new capabilities to arrest, detain and remove persons suspected of offenses, and new powers to search multiple premises, possibly an unlimited number of times. Law enforcement gained the ability to:

> “arrest without a warrant— anyone who is about to commit an offence; anyone who is in the act of committing an offence; anyone whom he has reasonable grounds for suspecting to be about to commit an offence; anyone whom he has reasonable grounds for suspecting to be committing an offence” ("Serious Organised Crime and Police Act", 2005, Part 3).

SOCPA also allows law enforcement to remove people from any “place if [law enforcement] believes, on reasonable grounds, that the person is in the place at a time when he would be prohibited from entering it” ("Serious Organised Crime and Police Act", 2005). Exclusionary zones were implemented around public buildings, including parliament, and peaceful protesters were forcibly removed, thereby curtailing their ability to congregate, and subjecting them to the other powers authorized under SOCPA if they refused. Furthermore, under the Act law enforcement is only required to obtain one warrant to search multiple premises the subject of the search may be affiliated with and if the warrant “authorises multiple entries, the number of entries authorised may be unlimited, or limited to a maximum” ("Serious Organised Crime and Police Act", 2005, Part 3). Previously, British law required that search warrants specify a person or premises to be searched, but under SOCPA, a warrant may be issued to search multiple premises an unlimited number of times.

SOCPA also expands powers authorized in the Anti-Terrorism and Security Act by allowing detainees suspected of criminal offenses, not necessarily terrorist offenses, to be fingerprinted, photographed, and adds that detainees can now have an “impression taken of [their] footwear” even if they are not charged with a crime ("Serious Organised Crime and Police Act", 2005, Part 3). SOCPA powers decrease privacy protections against unwarranted searches, seizures, and detentions, and expand the scope of warranted searches and seizures over 2000 levels.

In 2006, parliament passed the Identity Cards Act which established “a register of individuals (to be known as “the National Identity Register”)” ("Identity Cards Act", 2006). The purpose of the National Identity Register is to maintain a database of personal information including:

> “the address of every other place in the United Kingdom or elsewhere where he has a place of residence; where in the United Kingdom and elsewhere he has previously been resident; the times at which he was resident at different places in the United Kingdom or elsewhere; his current residential status; residential statuses previously held by him; information about numbers allocated to him for identification purposes and about the documents to which they relate; information about occasions on which information recorded about him in the Register has been provided to any person; and information recorded in the Register at his request; his full name; other names by which he is or has previously been known; his gender; his date and place of birth and, if he has died, the date of his death; and external characteristics of his that are capable of being used for identifying him; his nationality; his entitlement to remain in the United Kingdom; and where that entitlement derives from a grant of leave to enter or remain in the United Kingdom, the terms and conditions of that leave” ("Identity Cards Act", 2006, 1).

Additionally, a person with an ID card must “allow his fingerprints, and other biometric information about himself, to be taken and recorded; to allow himself to be photographed” ("Identity Cards Act", 2006). Such a broad amount of information would be stored on every person in the U.K. and kept in a centralized database, and registration in the National ID Card Registry is compulsory. Implications for privacy protection are substantial, however. Innocent citizens required to give detailed residency histories, biometric information, and other sensitive personal information on one card face revealing these details about themselves to not only the government, but also potential employers, schools, doctors, insurance agencies, telecommunications providers, banks, libraries, and other organizations which require ID cards in order to process applications, loans, or services.

Following the July 7th, 2005 attacks on the subway and transportation system in London, parliament enacted the Terrorism Act in March 2006. The Terrorism Act further augmented law enforcement capabilities by criminalizing encouragement of terrorism, the dissemination of terrorist publications, training for terrorism, and by allowing the detention of terrorist suspects for up to 90 days without a charge ("The Terrorism Act", 2006). The 90 day detention was reduced to 28 days after the bill had initially passed, during one of the review sessions. The Act

also authorized “all premises warrants” which permit law enforcement the ability to search any and all premises occupied by a suspect without “specify[ing] in the application all the premises which the person so specified occupies or controls and which might need to be searched” ("The Terrorism Act", 2006, Part 2). Additionally, a warrant can be issued “to enter and search the premises; and to seize anything found there which the constable has reason to believe is” a terrorist publication ("The Terrorism Act", 2006, Part 2). Without clarification of what a terrorist publication entails, possessing controversial reading material could potentially be an offense capable of eliciting a search and seizure. Outside of issues concerning freedom of speech, this authorizes access to private residences based solely on reading the wrong books, articles or websites. Search and seizure capabilities are further extended to law enforcement to search any vehicle, the operator of any vehicle, and the crew located within the “‘internal waters’… in the United Kingdom that are not comprised in any police area” ("The Terrorism Act", 2006, Part 2).

While the U.S. and the U.K. both expanded search, seizure, and surveillance capabilities after the 9/11 attacks, the evidence above suggests that the U.K. was far more comprehensive in its expansion of law enforcement powers, and by consequence, less protective of privacy rights. Based on deviations from the status quo, the U.K. enacted legislation authorizing broader police powers. Again, both countries widened the scope of search and seizure provisions, and wiretap procedures, but the U.S. retracted two of the more controversial provisions of the PATRIOT Act legislation towards the end of the time period, the roving wiretap provision and the gag order surrounding NSLs. In comparison, the U.K. consecutively passed legislation expanding investigatory powers, with no revision in successive legislation[5]. This appears to be in accordance with the central hypothesis that the institutional structure affects policy outcomes,

[5] The reduction of the detention period did not require additional legislation, but was changed during a review of the legislation.

and specifically that a smaller (larger) number of veto points allows for more (less) deviations from the status quo.

Privacy Protection and Institutional Variations

The previous section analyzed the changes in privacy protections over time, evidenced by the deviations from the status quo, defined herein as the year 2000. Both the U.S. and U.K. created policies which modified and/or expanded the investigatory powers of law enforcement and government agencies. Do institutional variations across the U.S. and U.K. explain the policy outcomes evidenced in the previous section? The veto points literature argues that "the policy stability of a political system increases when the number of veto players increases, [and] when their congruence decreases" (Tsebelis, 1999, p. 322). It follows that policy change would increase when the number of veto players decreases, and when their preferences converge. Do the U.S. and U.K. exhibit these characteristics during the time period specified, and if so, is that evidentiary of a relationship between institutional structure and policy change. If not, what other possible explanations exist for the policy outcomes experienced in these countries? The following sections endeavor to thoroughly answer these questions.

Institutional Structure in the U.S.

The 2000 general election in the U.S. produced a Republican president, George W. Bush, a slight Republican majority in the House of Representatives, and an evenly split Senate. There was a substantial electoral crisis following the presidential election, which eventually led to Bush's certification as the 43rd President of the United States.

> "The way in which George W. Bush won the White House certainly makes it harder for him to deliver on his campaign promise to "be a uniter, not a divider." But even without that burden, any president would face a formidable challenge in trying to govern in harness with a Congress so evenly and sharply divided by party as the one elected in 2000, especially when the partisan divisions are so firmly rooted in the parties' respective electoral constituencies" (Jacobson, 2001, p. 25).

To add fuel to the partisan fire, in May of 2001, Senator James Jeffords (R) Vermont, switched his party affiliation to Independent and announced he would caucus with the Democrats, giving them a slim majority (Conniff, 2001). The 9/11 attacks placed these partisan sentiments on hold. The U.S. experienced a period of marked preference convergence following the attacks on 9/11. If the House and Senate had been bitterly and closely divided in August 2001, they were definitely not so following the attacks. The House and Senate voted to pass the AUMF 420-0 and 98-0, respectively, and the USA PATRIOT Act 357-66 and 98-1, respectively.

The sudden and dramatic shift in public and partisan sentiment has been attributed to the "'rally 'round the flag' phenomenon [which] is well documented in the political science literature, and Bush's surge in public opinion constitutes a quintessential rally" (Schubert, Stewart, & Curran, 2002, p. 559). A profound convergence in veto player preferences such as this would create an opportunity for policy changes, and passage of the PATRIOT Act. As far as the institutional literature is concerned, whether or not this convergence was the result of the rally effect, or some other variable, the result would still be a preference profile likely to consent to policy change, which it ultimately did.

The U.S. experienced another convergence in preferences during the 2002 mid-term elections when the Republicans gained majority control in both houses of Congress. The Republican electoral victory and subsequent control of Congress and the Presidency presents another situation where veto points are controlled by veto players with similar preferences and internal cohesion. These sentiments continued during the 2004 re-election of Bush, the solidifying of the Republican majority in the House, and the slim majority of Republicans in the Senate. Preference convergence was never as high as immediately following 9/11; however it appears to still be significant. The Intelligence Reform and Terrorism Prevention Act of 2004

passed with wide bi-partisan support, passing the House 336-75, and the Senate 89-2. Interestingly, a bi-partisan effort successfully derailed the reauthorization of the PATRIOT Act with a threatened filibuster in 2005, even though the veto points in the U.S. were still majority controlled by the Republican Party (Stolberg, 2006).

> "In a letter Thursday, a bipartisan group of six senators said the tentative deal had caused them "deep concern" because it did not go far enough in "making reasonable changes to the original law to protect innocent people from unnecessary and intrusive government surveillance." The group called for tighter restrictions on the government's ability to demand records and its use of so-called "sneak and peak" warrants to conduct secret searches without immediately informing the target, among other measures" (Lichtblau, 2005).

Instead of making all provisions of the Patriot Act permanent, the Senators argued they should sunset in four years, allowing for additional review by the legislation. Once these revisions were implemented, the bill passed a resounding 89-10 in the Senate, and 280-138 in the House (Bacon, 2006). It appears that on issues of national security, acceptable policy outcome preferences remained quite similar across parties. Given the devastating nature of the 9/11 attacks, and the subsequent expansion of the security apparatus of the state, it is not surprising that issues of national security, including law enforcement capabilities, would result in veto player preference convergences, even among previously bitterly divided partisan actors. It would be interesting to analyze if the preference convergence noted on these national security issues extended to other issues, or if it is simply a product of heightened security concerns.

Institutional Structure in the U.K.

The U.K. government during this time period was controlled by Prime Minister Tony Blair and the Labour Party, which he brought to a resounding victory in 1997. Blair swept the Labour Party into power with bold initiatives, promises of reform and enjoyed an above average popularity with the British people, at least until the invasion of Iraq in 2003 ("The great

performer leaves the stage." 2007). With a singular veto point the institutional literature predicts that policy changes are quite likely. Due to Blair's landslide victory and the widespread popularity of the Labour Party, the effects of the informal veto points were weakened. Based on evidence from the previous section, over the 2000 to 2006 time period, the U.K. did produce several major pieces of legislation that deviated from the status quo.

Under the Labour Party and Tony Blair, the U.K. passed four major successive pieces of legislation affecting privacy protections. While all of the measures were opposed by members of the opposition parties and the House of Lords, the Acts were still passed, albeit sometimes with minor concessions (Millar, 2002; , "Terror detention law 'must go'", 2004; Travis, 2004; Ward, 2002). The Iraqi invasion in 2003 dramatically weakened Blair's position, within his party and in public opinion of his leadership. Blair's popularity waned following Britain's cooperation in the Iraq war, and he faced a growing backbench rebellion, culminating in MPs calling for his departure in 2006. Despite these factors, the Labour Party was still capable of passing the Terrorism Act of 2006 ("Backbench mood darkens over Blair's departure", 2006). Of all the Acts passed since RIPA, the Terrorism Act of 2006 broadens the most government search and seizure capabilities, and introduces criminal charges for broadly defined terrorist publications. While the House of Commons eventually reduced the amount of time a terrorist suspect could be held without charge from 90 days to 28 days, this minor compromise does not seem to reflect the inner turmoil over party leadership.

According to the veto points literature, conditions in both the U.S. and U.K. were favorable for policy changes to occur. In the U.S., policy outcomes during the time period when the House and Senate were controlled by different parties represent a dramatic preference convergence between to Democrats and Republicans which manifests itself in national security

issues post 9/11. It does not appear that the ideological proximity of actors greatly influenced policy outcomes, however. Democrats voted similarly to Republicans on all of the legislation expanding law enforcement powers, despite their ideological differences. The major pieces of legislation passed from 2001-2006 were all approved by bi-partisan majorities, with few Democrats opposing legislation. While partisan politics may have played a major role in other facets of government policy, where law enforcement capabilities and national security were concerned, ideological differences appear to have taken a back seat. Without a strong minority party, major party defections or a coalition government, the U.K. system remains open to policy changes as the Prime Minister and his/her party see fit. Strong reactions after the 9/11 attacks and 7/7 bombings most likely contributed to the ease of passage of the Anti-terrorism, Crime and Security Act as well as the Terrorism Act of 2006. However, the lack of meaningful checks on executive power in Britain appears to give the Prime Minister and his/her party a clear path to create and implement new legislation.

CHAPTER 5: CONCLUSIONS AND DISCUSSION

Terrorism as a method of violent expression became popular among domestic and international dissident groups in during nationalist, leftists, and anti-war movements of the 1960's. Both the U.K. and the U.S. reacted in the 60's by increasing surveillance and information gathering on dissident groups. There was a significant backlash in the 1970's as some of the methods of surveillance and covert operations were exposed, resulting in the improved privacy protection laws. However, terrorist events beginning in the 1990's and leading up to 9/11 created an environment where national security was seen as the most important issue facing the modern national state. As the focus of the state swings towards the security apparatus, it is important to understand how privacy protections and the police powers of the state expand and contract. This research thus far has shown that institutional variation across the U.S. and U.K affects privacy protections.

The cases of the United States and United Kingdom between 2000 and 2006 have been examined, finding that both countries expanded their law enforcement capabilities and reduced previously held privacy protections. In the case of the U.S., the September 11th attacks created an environment where there was clear bi-partisan support for increasing law enforcement capabilities, and the effect appears to last well into 2006, based on bi-partisan support for law enforcement enhancing legislation. Where partisan politics may have been an important factor in other legislative areas, it appears they did not significantly affect voting on the major bills approved post 9/11 that dealt with investigatory powers. In the case of the U.K., both the 9/11 and 7/7 terrorist attacks prompted increased state focus on security and law enforcement capabilities.

The institutional literature suggests that policy change is related to the number of veto points and preferences of veto players involved in policy making. The U.S. has a greater number of veto points than the U.K., and although national security threats produced preference convergence among the veto players, the policy changes reducing privacy protections were arguably narrower in scope than those in the case of the U.K. Tentatively, this is in line with the expectation that the U.K. would be able to push through more legislation affecting privacy protections. Evidently, while both states push through the same amount of legislation, the scope of the expansion of law enforcement powers is arguably greater in the U.K. In the U.K., policy changes decreased privacy protections against unwarranted searches, seizures, and detentions, and expanded the scope of warranted searches and seizures to include multiple locations and possible unlimited access. Furthermore, U.K. communications interception capabilities went beyond U.S. laws on two key points. Firstly, they require telecommunications providers to retain communications data for up to two years, and secondly they criminalize the act of not providing passwords or encryption keys to government agencies, even when such information is not withheld due to criminal intent.

Further investigation is needed post-2006, as after this time period both countries experienced a change in leadership. Tony Blair was replaced as Prime Minister following prominent backbench rebellions concerned with his competency to run the government, and in 2008 the U.S. electorate responded to the Bush administration's tenure by handing the Democrats a resounding victory and control of Congress and the presidency. With the U.K. still under Labour Party control, albeit with much reduced popularity, and the U.S. institutions controlled by ideologically similar actors, it would be interesting to investigate if there is a reversal of policies. A reversal could occur, if that is the intention of the new administrations.

The public opinion backlash in the U.S. represented by the overwhelming election of Democrats could signal that the expansion of law enforcement capabilities is no longer popular.

Obama's record is mixed on whether or not he would support increased privacy protections based on a controversial vote in the Senate "extending the power of the executive branch to authorize warrantless interception of international communications, and effectively granting retroactive amnesty to telecoms that participated in the extralegal surveillance program authorized by President George Bush after the attacks of 9/11" (Sanchez, 2008). In addition, the Supreme Court also signaled that widespread policy change is unlikely. In early 2008, the Court "turned down an appeal from the American Civil Liberties Union to let it pursue a lawsuit against the [warrantless wiretapping] program that began shortly after the Sept. 11 terror attacks" ("Supreme Court Rejects ACLU Challenge to Warrantless Surveillance Program", 2008). More recently, the Obama administration approved tighter restrictions on national security letters (NSLs) imposed by a federal appeals court, which "w[ould] force the FBI to justify to a judge the gag orders that it routinely slaps on the targets of NSLs" (Stokes, 2009). While strengthening some privacy protections, but not others, it remains unclear if the new administration will favor widespread policy change.

Prime Minister Gordon Brown's record is a bit more straightforward with regard to law enforcement capabilities. Brown has consistently defended the legislation passed under the Blair administration, of which he was a part. In a speech to the Institute for Public Policy Research in 2008

> "Brown accepted the proposals for an annual debate on the UK's surveillance apparatus – at least where it involves CCTV - the rest of [his] speech was a defence of CCTV and the other technologies which prompted the committee to consider whether the UK is indeed sleepwalking into being a surveillance society in the first place" (Fay, 2008).

Other reports suggest that Prime Minister Brown is considering expanding surveillance beyond the legislation authorized in 2006. In 2008,

> "British newspapers reported that Prime Minister Gordon Brown's government was working on a plan to monitor every phone call, Web-site visit, text message and email in the country, entering the information into a vast database that would be used to catch terrorists, pedophiles and scam artists" (Sullum, 2009, p. A15).

Given the institutional structure in the U.K., and the preferences of the executive to maintain or expand law enforcement powers, it is likely that the U.K. may experience a further reduction in privacy protections.

BIBLIOGRAPHY

Anti-Terrorism, Crime and Security Act 2001 (c. 24), Parliament of the United Kingdom(2001).

Authorization for Use of Military Force Against Terrorists(2001).

Backbench mood darkens over Blair's departure. (2006). *Guardian.co.uk: Politics* Retrieved July 2, 2009, from http://www.guardian.co.uk/uk/2006/sep/01/labourleadership.labour

Bacon, J., and Diamond, John. (2006). Anti-terror law passes: USA Today.

Bedan, M. (2007). Echelon's Effect: The Obsolescense of the U.S. Foreign Intelligence Legal Regime. *Federal Communications Law Journal, 59*(2), 425-444.

Berger v. New York, 388 U.S. 41 (U.S. Supreme Court 1967).

Cable Communications Policy Act of 1984 (Cable Act), §551 (1986).

CIA World FactBook: United Kingdom. (2008). United States of America, Central Intelligence Agency.

CNN.com. (2001, February 28). Britain lists terrorism act groups. Retrieved 06/05/2009, from http://archives.cnn.com/2001/WORLD/europe/UK/02/28/terrorist.law/

CNN.com. (2006). House approve Patriot Act renewal. *Politics* Retrieved July 1, 2009, from http://www.cnn.com/2006/POLITICS/03/07/patriot.act/

Conniff, R. (2001). Tipping Point in the Senate. *Progressive, 65*(7), 12.

The Constitution of the United States, Amendment IV, (1791).

Crepaz, M., and Moser, A.W. (2004). The Impact of Collective and Competitive Veto Points on Public Expenditures in the Global Age. *Comparative Political Studies, 37*(3), 259-285.

The Criminal Justice Act 2003 (c. 44), Parliament of the United Kingdom(2003).

Data Protection Act (c. 29), Parliament of the United Kingdom(1998).

Desai, A. C. (2007). Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy. *Stanford Law Review, 60*(2), 553-594.

Eggen, D. (2005, August 26). Library Challenges FBI Request. *Washington Post*, p. A11.

Etzioni, A. (2007). Are New Technologies the Enemy of Privacy? *Knowledge, Technology & Policy, 20*(2), 115-119.

The European Convention on Human Rights. (4 November 1950). Rome: Council of Europe.

Fay, J. (2008). Brown pledges annual commons debate on surveillance and says freedom auditors will protect our liberties. *The Register* Retrieved July 3, 2009, from http://www.theregister.co.uk/2008/06/17/brown_ippr_speech/

The Foreign Intelligence Surveillance Act, S. 1566 (1978).

Gadzheva, M. (2008). Privacy in the Age of Transparency: The New Vulnerability of the Individual. *Social Science Computer Review, 26*(1), 60-74.

Godoy, M. (2006). Google Records Subpeona Raises Privacy Fears [Electronic Version]. *NPR: Technology*. Retrieved April 27, 2008 from http://www.npr.org/templates/story/story.php?storyId=5165854.

Gore, A. (2006). Transcript: Former Vice President Gore's Speech on Constitutional Issues: The Washington Post.

Gorman, S. (2008, March 10). NSA's Domestic Spying Grows As Agency Sweeps Up Data. *The Wall Street Journal*.

The great performer leaves the stage. (2007, 5/12/2007). *Economist, 383*, 57-59.

Guhl, S. D., and Pendse, Ravi. (2008). Communications Assistance for Law Enforcement Act of 1994 (CALEA). *Information Security Journal: A Global Perspective, 17*, 110-113.

Haggerty, K. D., Gazso, A. (2005). Seeing Beyond the Ruins: Surveillance as a Response to Terrorist Threats. *Canadian Journal of Sociology, 30*(2), 169-187.
Henisz, W. J., and Mansfield, E.D. (2006). Votes and Vetoes: The Political Determinants of Commericial Openness. *International Studies Quarterly, 50*, 189-211.
Hentoff, N. (2008). Free Inquiry and the Unblinking Eye. *Free Inquiry, 28*(3), 22-23.
Identity Cards Act, Parliament of the United Kingdom(2006).
Intelligence Reform and Terrorism Prevention Act United States Senate, 108th Congress Sess.(2004).
Jacobson, G. C. (2001). A House and Senate Divided: The Clinton Legacy and the Congressional Elections of 2000. *Political Science Quarterly, 116*(1), 5.
Kastner, S. L., & Rector, C. (2003). International Regimes, Domestic Vetoâ€"Players, and Capital Controls Policy Stability. *International Studies Quarterly, 47*(1), 1.
Katz v. United States, 389 U.S. 347 (U.S. Supreme Court 1967).
Krause, G. A., and Meier, Kenneth J. (Ed.). (2003). *Politics, Policy, and Organizations: Frontiers in the Scientific Study of Bureaucracy*: University of Michigan Press.
Kyllo v. United States, 533 U.S. 27 (U.S. Supreme Court 2001).
Lewan, T. (2008). Companies map new uses for tracking chips, Critics concerned technology would compromise privacy [Electronic Version]. *Associated Press, San Francisco Chronicle*. Retrieved April 27, 2008 from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/02/03/MNM8UK3NH.DTL&hw=RFID&sn=001&sc=1000.
Lichtblau, E. (2005). Extension of Patriot Act Faces Threat of Filibuster. *The New York Times* Retrieved July 15, 2009, 2009, from http://www.nytimes.com/2005/11/18/national/18patriot.html
McKee, A. a. L., Vladamir. (2006). Ethical Considerations and Proposed Guidelines for the Use of Radio Frequency Identification: Especially Concerning Its Use for Promoting Public Safety and National Security. *Science & Engineering Ethics, 12*, 265-272.
Millar, S., and Lucy Ward. (2002). No 10 defends wider electronic surveillance. *The Guardian: Politics* Retrieved June 20, 2009, from http://www.guardian.co.uk/politics/2002/jun/12/security.humanrights
Mindle, G. B. (1989). Liberalism, Privacy, and Autonomy. *The Journal of Politics, 51*(3), 575-598.
Minnich, D. J. (2005). Veto players, electoral incentives and international commitments: The impact of domestic institutions on intergovernmental organization membership. *European Journal of Political Research, 44*, 295-325.
Nabbali, T., and Perry, Mark. (2004). Going for the throat: Carnivore in an ECHELON world - Part II. *Computer Law & Security Report, 20*(2), 84-97.
Noone, M. F., and Alexander, Yonah (Ed.). (1997). *Cases and Materials on Terrorism: Three Nations' Response*. The Hague, London, Boston: Kluwer Law International.
O'Reilly, R. F. (2005). Veto Points, Veto Players, and International Trade Policy. *Comparative Political Studies, 38*(6), 652-675.
Olmstead et al. v. United States, 277 U.S. 438 439 (U.S. Supreme Court 1928).
Peterman, L. (1993). Privacy's Background. *The Review of Politics, 55*(2), 217-246.
Porter, H. (2009). Jacqui Smith's tactical withdrawal. Retrieved April 25, 2009, from http://www.guardian.co.uk/commentisfree/libertycentral/2009/apr/17/ripa-jacqui-smith-councils
The Prevention of Terrorism Act 2005, Parliament of the United Kingdom(2005).

Protecting Privacy under the Fourth Amendment. (1981). *The Yale Law Journal, 91*(2), 313-343.
Rackow, S. H. (2002). How the USA Patriot Act Will Permit Governmental Infringement Upon the Privacy of Americans in the Name of 'Intelligence Investigations'. *University of Pennsylvania Law Review, 150*(5), 1651-1696.
Rayner, G., and Alleyne, Richard. (2008, April 14, 2008). Council spy cases 1,000 a month. *Telegraph.co.uk* Retrieved April 25, 2009
Regulation of Investigatory Powers Act, C. 23 (2000).
Reid, A. S., and Ryder, Nicholas. (2001). For Whose Eyes Only? A Critique of the United Kingdom's Regulation of Investigatory Powers Act 2000. *Information & Communication Technology Law, 10*(2), 179-201.
Sanchez, J. (2008). FISA compromise passes with Obama, Clinton on opposite sides. *Ars Technica: Law & Disorder* Retrieved July 3, 2009, from http://arstechnica.com/tech-policy/news/2008/07/fisa-compromise-passes-with-obama-clinton-on-opposite-sides.ars
Savage, C. (2006). Bush shuns Patriot Act requirement. Retrieved July 1, 2009, from http://www.boston.com/news/nation/articles/2006/03/24/bush_shuns_patriot_act_requirement/?page=2
Schubert, J. N., Stewart, P. A., & Curran, M. A. (2002). A Defining Presidential Moment: 9/11 and the Rally Effect. *Political Psychology, 23*(3), 559-583.
Schwartz, P. M. (2004). Property, Privacy, and Personal Data. *Harvard Law Review, 117*(7), 2056-2128.
Seamon, R. H., and Gardner, W.D. (2005). The Patriot Act and the Wall Between Foreign Intelligence and Law Enforcement. *Harvard Journal of Law & Public Policy, 28*(2), 319-463.
Search Engines Defend Your Privacy (To Target You Better). (2007). In A. Age (Ed.): Center for Digital Democracy.
Seipp, D. J. (1983). English Judicial Recognition of a Right to Privacy. *Oxford Journal of Legal Studies, 3*(3), 325-370.
Serious Organised Crime and Police Act, Parliament of the United Kingdom(2005).
Solove, D. J. (2002). Conceptualizing Privacy. *California Law Review, 90*(4), 1087-1155.
Stokes, J. (2009). Obama administration reins in FBI's NSL-related gag orders. *Ars Technica: Law & Disorder* Retrieved July 3, 2009, from http://arstechnica.com/tech-policy/news/2009/05/obama-admin-makes-fbi-submit-nsl-gag-orders-to-judicial-review.ars
Stolberg, S. G. (2006). Key Senators Reach Accord On Extending the Patriot Act. *New York Times*, 14.
Sullum, J. (2009, May 18, 2009). The State of Surveillance. *The Wall Street Journal (Eastern Edition)*, p. A15.
Supreme Court Rejects ACLU Challenge to Warrantless Surveillance Program. (2008). *Foxnews.com: Politics* Retrieved July 3, 2009, from http://www.foxnews.com/story/0,2933,331203,00.html
'Talking' CCTV scolds offenders [Electronic (2007). Version]. *BBC News*. Retrieved April 22, 2008 from http://news.bbc.co.uk/2/hi/uk_news/england/6524495.stm.
Terror detention law 'must go'. (2004). *BBC News* Retrieved June 20, 2009, from http://news.bbc.co.uk/2/hi/uk_news/politics/3534274.stm
The Terrorism Act, Parliament of the United Kingdom(2006).
The Terrorism Act 2000 (c. 11), Parliament of the United Kingdom(2000).

Travis, A. (2004). Home Office draws up tighter terrorism laws. *Guadian.co.uk* Retrieved June 20, 2009, from http://www.guardian.co.uk/uk/2004/aug/04/terrorism.september111/print

Tsebelis, G. (1995). Decision making in political systems: Veto players in Presidentialism, Parliamentarism. *British Journal of Political Science, 25*(3), 289.

Tsebelis, G. (1999). Veto players and law production in parliamentary democracies: An empirical analysis. *American Political Science Review, 93*(3), 591.

Tsebelis, G. (2000). Veto Players and Institutional Analysis. *Governance: An International Journal of Policy and Administration, 13*(4), 441-474.

U.S.C. Title 18, Part I, Chapter 88, S. 1801.

U.S.C. Title 18, Part I, Chapter 119, S. 2511.

United States v. United States District Court for the Eastern District of Michigan et al., 407 U.S. 297 70 (U.S. Supreme Court 1972).

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, 107th Congress, 1st Sess.(2001).

van den Hoven, J. (2006). Nanotechnology and Privacy: The Instructive Case of RFID. *International Journal of Applied Philosophy, 20*(2), 215-228.

Vermeule, A. (2008). Emergency Lawmaking after 9/11 and 7/7. *University of Chicago Law Review, 75*(3), 1155-1190.

Video Privacy Protection Act, S. 2710 (1988).

Wallace, B. (2000, May 2000). Top of the News: Who's Reading Your Mail? Feds Have Their Eye on You. *PC World, 18,* 66-67.

Ward, L., and Nicholas Watt. (2002). Home Office 'safeguards' on privacy leave critiques unconvinced. *The Guardian: Politics* Retrieved June 20, 2009, from http://www.guardian.co.uk/technology/2002/jun/18/security.politics

Warren, S., and Brandeis, L. (1890). The Right to Privacy. *Harvard Law Review, IV*(5), 193-220.

Wise, J. (2007). Civilian UAVs: No Pilot, No Problem [Electronic Version]. *Popular Mechanics*. Retrieved April 22, 2008 from http://www.popularmechanics.com/science/air_space/4213464.html?page=1.

Wolly, B. (2006). Wiretap Revelations Spur Presidential Powers Debate. *The Online NewsHour: Background Report* Retrieved June 25, 2009, from http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/questions.html