INFORMATION ETHICS:
AN APPLIED STUDY OF UNITED STATES FOREIGN INTELLIGENCE SURVEILLANCE UNDER PRESIDENT GEORGE W. BUSH

Michelle Louise Atkin

School of Information Studies McGill University, Montreal

January 2011

A thesis submitted to McGill University in partial fulfillment of the requirements of the degree of
Doctor of Philosophy

Table of Contents

Abstract

This dissertation examines the philosophical foundations of information ethics and their potential for application to contemporary problems in U.S. foreign intelligence surveillance. Questions concerning the limits of government intrusion on protected Fourth Amendment rights are addressed by analyzing the post-9/11 changes to the U.S. foreign intelligence surveillance law and policy in terms of the traditional ethical theories commonly used to support or discount these changes, namely utilitarian and contractarian ethical theories. This research combines both theoretical elements, through its use of analytic philosophy, and qualitative research methods, through its use of legislation, court cases, news media, and scholarship surrounding U.S. foreign intelligence surveillance. Using the *U.S.A. PATRIOT Act*, the *Foreign Intelligence Surveillance Act (FISA*) and the Terrorist Surveillance Program as case examples, the author develops and applies a normative ethical framework based on a legal proportionality test that can be applied to future cases involving U.S. foreign intelligence surveillance.

The proportionality test developed in this research, which is based on a modified version of the Canadian *Oakes Test*, seeks to balance legitimate concerns about collective security against the rights of the individual. As a new synthesis of utilitarian and contractarian ethical principles, the proportionality test laid out in this dissertation has potential for application beyond U.S. foreign intelligence surveillance. It could act as a guide to future research in other applied areas in information policy research where there is a clear tension between individual civil liberties and the collective good of society. Problems such as passenger screening, racial and ethnic profiling, data mining, and access to information could be examined using the framework developed in this study.

Résumé

Cette thèse porte sur les fondements philosophiques de l'éthique de l'information et sur leur potentiel d'application aux problèmes contemporains en matière de surveillance du renseignement étranger aux États-Unis. On aborde des questions relatives aux limites de l'intrusion du gouvernement sur les droits protégés par le quatrième amendement en analysant les changements post-9/11 aux lois et aux politiques en matière de surveillance du renseignement étranger en termes de théories éthiques traditionnelles couramment utilisées pour discuter de ces changements, à savoir l'utilitarianisme et les théories de contractualisme. Cette étude combine à la fois des éléments théoriques, par son utilisation de la philosophie analytique, et les méthodes de recherche qualitative, à travers son utilisation de la législation, la jurisprudence, les médias et les recherches au sujet de la surveillance du renseignement étranger. Utilisant comme exemples la *U.S.A. PATRIOT Act*, la *Foreign Intelligence Surveillance Act (FISA)* et le *Programme de surveillance des terroristes,* l'auteur élabore et applique un cadre d` éthique normative fondé sur un test de proportionnalité, un cadre que l'on peut appliquer à d'autres cas impliquant la surveillance du renseignement étranger.

Le test de proportionnalité développé dans cette recherche, qui est basé sur une version modifiée du célèbre *Oakes test* de la Cour supr**ê**me du Canada, cherche à contrebalancer les préoccupations légitimes concernant la sécurité collective et les droits individuels. Comme synthèse des principes utilitairistes et contractualistes, le test de proportionnalité énoncé dans la présente thèse a un potentiel d'application au-delà de la surveillance du renseignement étranger aux États-Unis. Il pourrait servir de guide pour des recherches dans d'autres domaines appliqués

où il y a une tension évidente entre les libertés individuelles et le bien collectif de la société. Des problèmes tels que le contrôle des passagers, le profilage racial et ethnique, l'exploration de données, et l'accès à l'information pourrait être examiné en utilisant le cadre élaboré dans cette étude.

Acknowledgements

I would like to take this opportunity to thank my supervisor, Dr. Andrew Large for his continued support and guidance throughout this project. It has been an honour and a pleasure to work with him.

In addition, I would like to thank the members of my Advisory Committee: Professor Philip Buckley (Department of Philosophy), Professor Peter McNally (School of Information Studies), and Professor Mary Maguire (Department of Integrated Studies in Education) for all their insightful and helpful comments and suggestions.

I would also like to thank my colleagues at Carleton University (past and present) who have supported me throughout this journey. A special thank you to: Martin Foss, Margaret Haines, Elizabeth Knight, and Frances Montgomery of the MacOdrum Library, and Professor Peter Swan and Professor David Elliott of the Law Department.

And last but not least, a thank you to my family and my lovely Elizabeth.

Abbreviations

ACLU = American Civil Liberties Union

AG = Attorney General

AUMF = Authorization for Use of Military Force

CAPPS = Computer-Assisted Passenger Prescreening System

DNI = Director of National Intelligence

DOD = Department of Defense

DOJ = Department of Justice

ECPA = Electronic Communications Privacy Act

EFF = Electronic Frontier Foundation

FAA = FISA Amendments Act of 2008

FCRA = Fair Credit Reporting Act

FERPA = Family Education Rights and Privacy Act

FISA = Foreign Intelligence Surveillance Act of 1978

FISC = Foreign Intelligence Surveillance Court

ISP = Internet Service Provider

NSL = National Security Letter

NSA = National Security Agency

PAA = Protect America Act of 2007

Patriot Act = U.S.A. PATRIOT Act of 2001

Patriot Reauthorization Act = U.S.A. PATRIOT Improvement and Reauthorization Act of 2005

PSP = President's Surveillance Program

RFPA = Right to Financial Privacy Act

TSA = Transportation Security Administration

TSP = Terrorist Surveillance Program

Glossary of Terms

Analytic Philosophy: the broad philosophical tradition dominant in various regions, most notably Great Britain and the United States, since the early twentieth century,[1] characterized by close argument aimed at achieving clarity, and respect for the natural sciences.

Applied Ethics: the application of ethical theories to particular practical domains such as medical ethics, business ethics, legal ethics, environmental ethics, computer ethics, and most recently, information ethics.

Consequentialism: moral theories which judge an action to be moral or immoral on the basis of its final consequences or outcome. One who subscribes to such moral thinking would be referred to as a Consequentialist.

Contractarianism: a rights-based approach to morality and ethics that takes into account the differing types of rights, both positive and negative, and the roles and responsibilities of citizens and governments to uphold and protect those rights. This relationship between citizens and their government takes the form of a social contract.

Communitarianism: a teleological approach to morality that attaches an ethical importance to community values and bonds, the importance of which has not been adequately captured by deontological theories, specifically those focused on social contract. Communitarians argue that

[1] See Aaron Preston's definition for 'Analytic Philosophy' provided in the Internet Encyclopaedia of Philosophy: A Peer-Reviewed Academic Resource. March 25, 2006. <http://www.iep.utm.edu/analytic/> for additional information on the historical roots of the tradition.

such contracts do not capture the full importance of the community, both in terms of tradition and cultural understanding.

Ethics: the philosophical study of morality: that is, of right conduct, obligation, responsibility, and social justice.

Information Ethics: the application of traditional ethical theories to issues regarding the collection, classification, and dissemination of information. Information ethics includes standards of professional practice, codes of conduct, and aspects of information law and public policy.

Meta-ethics: the philosophical study of the nature of moral judgment and ethical norms. It is concerned with foundational issues, such as the meaning of terms like "right" and "wrong," or the objectivity (or lack thereof) of moral judgments. Meta-ethical theories are in general purely descriptive and do not aim to have prescriptive implications for human action.

Morality: a code of right conduct. This code may be the result of social or religious norms or the product of rational thought.

Negative Rights: a negative right is the right to freedom from outside interference in a specified domain. The rights to intellectual freedom, freedom of speech, and of privacy are examples of negative rights, as they assert the right of the individual to think, speak and keep some part of her life outside the public realm without interference from forces that would try to subvert those

rights.

Normative Ethics: unlike meta-ethics which concerns itself with the nature of norms, normative ethical theories are prescriptive. Normative ethics sets out norms or rules related to action. Normative ethics have traditionally been broken down into two groups: teleological, which are theories of the good; and deontological theories, which are theories of duty

Positive rights: unlike a negative right, which set out a boundary protecting the individual against outside interference, a positive right is the right to a specified good considered necessary for individuals to fully express their freedom within the community. That is, a positive right establishes an obligation on the part of the community to provide that good, without which the individual could not be considered fully free. For example, the right to health care and the right to education would be positive rights.

Proportionality test: a judicial test for determining whether or not a constitutionally protected right can be reasonably limited under the law.

Teleological Theories: from the Greek word 'telos' meaning end, fulfillment, completion, goal or aim. Teleological theories in normative ethics take a conception of the good to be primary; the theory is then framed in such a way as to lay out the means to be used in order to maximize the good. The value of any particular action, policy of action, or even of a law, is judged by the degree to which it has maximized the good.

Deontological Theories: normative ethical theories which hold adherence to rules (laws, norms) to be primary, and consequences secondary in judging the morality of an action or policy. Typically, moral evaluations within such theories hold adherence to the moral law to be necessary but not sufficient; an action must be motivated by respect for the moral law (rather than to achieve some desired outcome) to count as moral. Deontological theorists have based the high degree of respect due the moral law on, variously, the law's divine provenance, its rootedness in human nature, or the basis of the concept of morality in pure practical reason.

Utilitarianism: a form of consequentialism, first expounded by Jeremy Bentham that views pleasure as being unquestionably good and pain and suffering as unquestionably bad. The rightness or wrongness of an action, law or policy depends upon its ability to maximize pleasure and/or minimize suffering.

PART I:

INFORMATION ETHICS IN THE POST 9/11 PERIOD

Chapter 1:

Overview of the Research Design

Following the terrorist attacks on the Twin Towers and the Pentagon that took place on September 11, 2001, the U.S. Government under the Bush Administration took unprecedented measures in an effort to apprehend and punish the perpetrators of those attacks and to prevent future attempts against the American homeland. Law enforcement agencies were given the right to access database information concerning individuals held by any U.S. based organization (including library patron information) through the use of National Security Letters (NSLs). They were also given the right to intercept phone calls, and to engage in other forms of warrantless surveillance as deemed necessary in the 'War on Terror.' Eventually, additional legislation was passed to ensure that such warrantless activities, if not initially legal, were at least retroactively so. These new measures have had far-reaching political and ethical implications. The aim of this study is to examine how the general implications of these new policies in the U.S. play out in the domain of information ethics. Only time will tell whether or not the Obama Administration (or future administrations) will look to reverse the legislative and administrative policy trends set by the previous government. In the meantime, studying the ethical impact of the decisions taken in the eight years of the Bush Administration may prove insightful to the study of information ethics, law and policy.

As this research is an applied study in information ethics, it will be useful to lay out the terms of reference right from the start. Ethics is the philosophical study of morality: that is, of right conduct, obligation, responsibility, and social justice. Information ethics, narrowly construed, is

the application of traditional ethical theories, such as utilitarianism or contractarianism, to issues regarding the collection, classification, and dissemination of information. More broadly construed, information ethics includes standards of professional practice, codes of conduct, and aspects of information law, public policy and so forth.

In this research I set out a plan for first, exploring the philosophical foundations of information ethics, and second, combining this foundation with an applied study in information ethics with a focus on U. S. foreign intelligence surveillance. My aim in this study is partly theoretical (or abstract), and partly practical (or concrete). That is to say, that I am interested in both the development and application of a normative ethical framework that can be applied to cases involving U.S. foreign intelligence surveillance. By seeking to combine foundational ethical theory in a way that is flexible enough to deal with real world problems (transforming ethical theory to ethical practice in the form of applied ethics) this research falls squarely in line with that of prominent recent work in social and political philosophy. The American philosopher, Martha Nussbaum, for example, offers the following by way of a description of the central goals of her most recent book: Frontiers of Justice: Disability, Nationality, Species Membership:

> Theories of justice should be abstract. They should, that is, have a generality and theoretical power that enables them to reach beyond the political conflicts of their time, even if they have their origins in such conflicts. [...] On the other hand, theories of social justice must also be responsive to the world and its most urgent problems, and must be open to changes in their formulations and even in their structures in response to a new problem or to an old one that has been

culpably ignored.[2]

Research Question

The overarching question addressed in this dissertation is:

What are the boundaries limiting government intrusion on privacy rights and how are such boundaries drawn?

This is a more complex question than might be suggested by the simple response that freedom must be traded for security in a dangerous world. Any such justification of the limitation of civil liberties turns on the nature and the severity of the threat posed by terrorism, and the effectiveness of the measures in question in countering that threat. Even if it is granted, for the sake of argument, that legislative measures such as those provided by the *U.S.A. Patriot Act*, the Presidential authorization of the Terrorist Surveillance Program, and the recent changes to the *Foreign Intelligence Surveillance Act*, do enhance public security in the face of a serious, ongoing threat, there remain deeper issues with respect to justifying the sacrifice of such rights for security. The U.S. is a liberal democracy founded on a rights-based constitution. The fundamental claim to legitimacy advanced by such a constitution is not the achievement of common goods through binding together in a community (e.g., the welfare of security of its citizens), but rather the preservation of the rights to which citizens are entitled and from which they derive their dignity as equal members of the community. This dissertation seeks to address whether there can be a coherent justification for trading constitutionally protected civil liberties

[2] Nussbaum, Martha. Frontiers of Justice: Disability, Nationality, Species Membership. Cambridge, MA: Harvard University Press, 2006, p. 1.

in exchange for security in insecure times.

In order to address these questions I will analyze a variety of different sources: primary texts in philosophy; and primary and secondary sources related to government legislation, court decisions, committee reports, policy documents; position statements of government departments and non-governmental organizations. If a justification emerges that coheres with the core principles of American democracy that underlie the U.S. Constitution, then new legislative and policy measures may be seen as just another step in the continuous evolution of the scope and limits of rights and liberties in that country. If no such justification is forthcoming – that is if security and common good take precedence over civil liberties in any justification that can be offered – these new changes must be seen to represent an attempt at rethinking the fundamental principles upon which the most powerful liberal democracy in the world was founded. If so, then "everything" has indeed "changed."

Methodology

To address in any concrete sense the question of where the boundaries on government intrusion upon privacy rights lie, the use of case examples is essential. Although I am using real cases, that is to say that I am focused on actual historical events rather than purely hypothetical thought experiments, my approach is in many respects closer to one an analytic philosopher might use when testing out a theory or principle in humanities research. In that sense my use of the term 'case' is different from how the term 'case' might be used in much of the social sciences. The cases I set out are descriptive, that is, they outline the events as they were portrayed in the media, through government reports, committee meetings, and debates, through various court challenges,

and in the relevant scholarly literature. The benefit of using real cases when dealing with ethical questions is that they illustrate the need for critical ethical theory and research to address real world problems in the area of information ethics.

My research is different from that of social scientists like Robert E. Stake, Robert K. Yin, Pamela Baxter and Susan Jack, among others, who use case studies as an instrument for developing a constructivist paradigm. In this paradigm the claim is that "truth is relative and that it is dependent on one's perspective."[3] Case studies in this sense examine the social construction of reality through participant narratives. The study of these narratives is what allows researchers the ability to gain a better understanding of a participant's actions. My main concern with this work is not why individual actors behaved the way they did (which raises more complicated social and political questions related to the aftermath of the 9/11 attacks), but rather what the limitations on government should be with respect to privacy. That is to say, I am concerned with the underlying ethical questions. Given the nature of the questions I am addressing, and the philosophical tradition from which I am approaching them, the use of constructivist paradigm is problematic because it is inconsistent with the fundamental premise of analytic philosophy: that analytical reasoning can help us make more prudent ethical choices by establishing the implications and consequences of alternative ethical approaches. If I were to point to a particular theorist who exemplifies the tradition in which I am working, I would most likely look to John Rawls who brought political philosophy back into the analytic tradition. That being said, this is not a Rawlsian dissertation (I do not subscribe to a completely contractarian approach to

[3] Baxter, Pamela, and Susan Jack. "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers." The Qualitative Report 13.4 (2008): 544.

ethics), but the influence of this type of analytic reasoning will likely become apparent to the reader as the dissertation unfolds.

The methodology used in this dissertation involves both an abstract or theoretical component as well as a concrete or applied component. The former will amount to a conceptual exploration of foundational ethical issues – specifically an examination of the conceptual coherence and plausibility of central insights of ethical theories from a broadly 'a priori' point of view. The latter will involve the discovery and discussion of qualitative empirical data about information practices in the post 9/11 period through the use of case examples, which will highlight the concrete, practical issues to be evaluated in the light of the theoretical results.

Initially my choice of subject matter was limited to my own personal interest in the ethical issues associated with the *U.S.A. PATRIOT Act (Patriot Act)* as it was being covered in the press in 2001, particularly the use of National Security Letters (NSLs) and their potential chilling effect on freedom of expression and intellectual freedom. In the immediate aftermath of the September 11th attacks, the use (and possible misuse) of such letters provided researchers with the first glimpse of a possible shift in American information policy in the post 9/11 period. Questions about whether or not the use of such letters was constitutional or a possible violation of the Fourth Amendment which protects against unlawful search and seizure, were to my mind not only of interest to strictly legal or political scholars but also of interest to those in philosophy and information studies because they represented an intersection between all four disciplines – that is to say, they raised legal, political, ethical and policy questions for all four disciplines.

As previously stated, my initial PhD proposal was to focus entirely on the *Patriot Act*, and was supposed to be a case study of this Act. Over time, and with the revelations of warrantless surveillance by the U.S. Government, this research expanded to include two additional case studies: one on the Terrorist Surveillance Program, and the other on the subsequent amendments to the *Foreign Intelligence Surveillance Act*. The reason I chose to expand the study was simple, I wanted to see if the ethical principles that arose from the examination of my overarching research question could equally be applied in my examination of all three cases given their similar national security concerns as related to foreign intelligence surveillance.

The case examples used in this dissertation are specific to the post 9/11 period of the U.S. and are limited to the two terms of the George W. Bush presidency (2001 – 2009). These case examples were selected on the basis of their moral justifications (something which came through clearly in the public accounts of each case through various media, court cases, government documents, etc.) and provide a modern example for testing more theoretical ethical approaches in an applied setting.

Research Design

Following an overview of my research approach and statement of my research questions provided in Chapter 1, Chapter 2 presents a review of the literature in the field. Although there is a great deal that has been written about the constitutional issues associated with the reforms that were instituted in the post 9/11 period, the review demonstrates that there is a gap in the literature when examining deeper ethical questions related to issues which go beyond the purely legal or political consequences of these reforms – something this dissertation seeks to address.

Chapter 3 examines the ethical dimension of the U.S. Constitution and of American law making. Engaging in a discussion of ethical principles in light of the constitutional principles is itself loosely meta-ethical because it assumes that the rights a constitution protects exist prior to the constitution - they would have to if they are deemed inalienable. The U.S. Constitution and the various legislative reforms discussed throughout the rest of the dissertation shape a discussion of meta-ethical, normative and applied ethics in the context of constitutionally protected rights, specifically Fourth Amendment rights. As this chapter points out, the majority of the post 9/11 legislative reforms and executive orders have looked to utilitarian arguments for support. Less attention has been paid to the other, contrasting approach that has consumed much of recent American legal and political thought, that of rights-based ethics. In this section, I examine both of these important branches of applied ethics and use them to analyze the development of moral values and ethical conflicts in the information field. In assessing these ethical theories, I consider the extent to which they are compatible with the fundamental principles of the U.S. Constitution. My objective is to formulate a third way forward that allows for a balance of both the right and the good. Chapter 3 concludes with a discussion of the application that information ethics can and should have in any discussion involving the myriad events and trends which have arisen in post – 9/11 America.

Chapters 4 – 6 examine various ethical issues with regard to privacy and access to information, in particular those relating to information collection, classification and dissemination, asking to what degree limitations in access to information may be justified in a liberal, democratic society. Chapter 4 begins with a discussion of the legislative response to the September 11th attacks, namely, the implementation of the *U.S.A. PATRIOT Act (Patriot Act).* This chapter also

provides an assessment of the tools now available to U.S. law enforcement in the "War on Terror," asking not only whether these measures are indeed effective, but also if they are compatible with the values put forth in the U.S. Constitution. Chapter 5 examines the use of warrantless surveillance in the U.S. which was been deemed by the George W. Bush Administration to be a constitutionally sound practice and a logical extension of the President's war-time powers. Chapter 6 concludes with a discussion of the liability for both the companies who complied with warrantless surveillance requests under the Terrorist Surveillance Program and the government officials who orchestrated the secret program. This chapter examines a major shift in American law making as witnessed by the *Protect America Act (PAA)* and the *FISA Amendments Act of 2008 (FAA)'s* immunity provisions, and the impact that such legislation will have on the future of American lawmaking.

Chapter 7 discusses the prospects for privacy in post 9/11 America. The work of authors such as Christopher Slobogin,[4] K.A. Taipale,[5] and Stephanie Cooper Blum[6] inform the discussion of balancing liberty and security in terms of electronic surveillance. This chapter attempts to provide a compromise between utilitarian and contractarian arguments through the use of tests which foster proportionality and minimization of harm to the right being infringed – that being, the Fourth Amendment. The U.S. Terry Stop test and the Canadian Oakes test are discussed in this chapter, with the latter test forming the basis for a new standard in measuring proportionality that goes beyond that proposed by Slobogin, Taipale, and Cooper Blum. By incorporating the

[4] Slobogin, Christopher. Privacy at Risk: The New Government Surveillance and the Fourth Amendment. Chicago: University of Chicago Press., 2007.

[5] Taipale, K. A. "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance." Yale Journal of Law and Technology 9 (2007): 128

[6] Blum, Stephanie Cooper. "What really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." Boston University Public Interest Law Journal 18 (2008): 269.

underlying principles of the Canadian Oakes Test, a judicial test for determining whether or not a protected right can be limited under the Canadian Constitution, into the discussion surrounding the limitations of government intrusion upon privacy rights, it is possible to address the concerns for a third way forward that combines both the utilitarian and contractarian concerns raised in the 'liberty versus security' debate. Chapter 8 concludes with an examination of the tension between civil liberties and national security. It focuses on the need for achieving a balance of these rights (Fourth Amendment rights in particular) and their corresponding responsibilities (the protection of national security) in the post 9/11 period.

Overview of Main Research Findings

This study involves highly political legislative and policy actions that took place during the Bush Administration in the post 9/11 period. Although the case examples studied indicate the political nature of these actions, the final analysis of these events focuses on the ethical dimensions. This research broadly examines the main ethical theories that were used to shape the ethical debate surrounding the issues: those being utilitarian and contractarian. Analysis of the three case examples revealed that the main tensions inherent in each case were part of the public 'liberty versus security' debate. This debate was framed by the Administration, civil liberties groups, politicians, and academics in largely utilitarian and contractarian terms. This study finds that the traditional ethical theories of utilitarianism and contractarianism are not sufficient to the task of dealing with contemporary ethical problems as they relate to information ethics. Rather than viewing utilitarian and contractarian approaches as being adversarial, this research looks to combine these approaches in the form of a proportionality test that Courts can apply to cases involving Fourth Amendment rights as related to foreign intelligence surveillance in the U.S.

By providing a model of proportionality that goes beyond the Terry Stop test, a court test for determining the limits of a lawful search and seizure, as presented in the American scholarly literature on the issue, this research is adding something new to the literature on this topic.

Implications

The events of 9/11 will no doubt be marked as a major turning point in American history, not only because of the event itself, but because of the dramatic shift in government policy they caused. The creation of far-reaching legislation such as the *Patriot Act*, the admission by the Administration that it had been conducting warrantless surveillance on Americans for four years (2001 – 2005) through the Terrorist Surveillance Program in an attempt to thwart terrorist efforts, and the subsequent passage of retroactive legislation to limit the legal liability for the telecom companies that cooperated with the Government's requests for information, have all raised questions as to what degree civil liberties, or human rights in general, can be set aside in the interest of national security. This study will be of interest to those in Information Studies, Philosophy, Political Science and Legal Studies.

Chapter 2:

Literature Review

Introduction

In the U.S. the discussion of rights and responsibilities has become largely a discussion about the balancing of individual rights with such things as the right to privacy against any government intrusions on such rights in the name of national security. The September 11, 2001 terrorist attacks on the U.S. required action by the Federal Government in order to protect the security of the nation. Issues related to the collection of specific types of personal information as well as barriers to information sharing among different government agencies were immediately highlighted as key problems in preventing the attacks. The passage of the *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act*[7] (*U.S.A. PATRIOT Act* or *Patriot Act* for short) was the initial legislative response to the events of September 11th. This Act, in combination with the National Security Agency's (NSA) program of warrantless surveillance, and subsequent amendments to the *Foreign Intelligence Surveillance Act of 1978* (*FISA*)[8] through the *Protect America Act of 2007 (PAA),*[9] and the *FISA Amendments of 2008 (FAA),*[10] has been subject to a great deal of controversy among civil liberties groups who argue that such measures have served to reduce civil liberties in

[7] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT) Act of 2001.* Public Law 107-56, § 214(a)(1), 115 Stat. 272, 286 (Amending 50 U.S.C. § 1842(a)(1) (2000)).

[8] *Foreign Intelligence Surveillance Act of 1978*, Public Law 95-511, 92 Stat. 1783, 50 U.S.C. ch. 36 s. 1566.

[9] *Protect America Act of 2007*, Public Law 110-55.

[10] *FISA Amendments Act of 2008*, Public Law110-261.

America.

Although one of the crucial responsibilities for any government is the provision of national security for its people, the potential for gross abuses of governmental power in instances where certain individual rights may be waived is something that requires further investigation. The following literature review examines a broad selection of scholarly articles relating to three broad questions:

What ethical, legal or political considerations should be taken into account with regard to the collection, classification, and dissemination of citizens' personal information by government departments and agencies?

Where do Fourth Amendment rights fit into foreign intelligence investigations?

Are there exceptional circumstances under which the right to privacy can be waived in the interest of national security?

In order to address these questions I have identified and synthesized a variety of scholarly articles. The articles selected are multidisciplinary, drawing from Law, Political Science and Philosophy. Specifically these articles look at the impact of the *Patriot Act* upon due process and judicial oversight, and the impact of the warrantless surveillance program conducted by the NSA and the retroactive immunity provisions added to *FISA* on Fourth Amendment rights, as well as a number of other civil liberties and human rights issues that have arisen in the post-

September 11th period.

Broad Ethical, Legal and Political Considerations

What ethical, legal or political considerations should be taken into account with regard to the collection, classification, and dissemination of citizens' personal information by government departments and agencies?

Information Gathering

The *Patriot Act* was the initial legislative response to September 11th 2001. The Act passed less than six weeks after the terrorist attacks on the World Trade Center and the Pentagon, amid pressures for government reaction to these horrific events. The objectives of the Act, according to Christopher P. Banks, were as follows:

1. to improve information sharing between law enforcement and foreign intelligence agencies;
2. to gather anti-terrorism intelligence through the use of the flexible warrant requirement of the Foreign intelligence Surveillance Act (FISA);
3. to expand wiretap authority over electronic communication;
4. to seize funds utilized for terrorist activities; and
5. to impose mandatory detention and deportation of non-U.S. citizens suspected of having links to terrorist organizations[11]

[11] Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004, p. 30.

As a means for fulfilling these objectives a number of important pieces of legislation were modified including the *Foreign Intelligence Surveillance Act* (*FISA*), the *Family Education Rights and Privacy Act* (*FERPA*), the *Right to Financial Privacy Act*, the *Electronic Communications Privacy Act*, the *Cable Communications Policy Act*, the *Federal Wiretap Statute*, the *Federal Pen Register and Trap and Trace Statute*, as well as many other statutes.[12]

Effects of Legislative Changes on Information Collection

The impact of the changes to the statutes identified by Banks, are reviewed sector-by-sector by Priscilla M. Regan in her article, "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." Here Regan examines various sectors currently affected by a reduction in privacy protection as a result of the *Patriot Act*. This act "amends virtually every information privacy statute to facilitate access, increase data collection, and reduce the due process and privacy protections for record subjects."[13] According to Regan, these changes represent a reduction in privacy protections across a variety of different sectors and are a clear expansion of government authority. In particular, Regan examines how the financial, educational, library, internet communications and transportation sectors are being affected by these changes.

Sector by Sector Impact

I. Financial

One aim of the *Patriot Act* is to bolster federal efforts to combat money laundering. It does so through the use of more stringent record keeping, disclosure and information sharing

[12] Statutes as cited in Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99, p. 100.

[13] Regan, Priscilla M. "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." Government Information Quarterly 21.4 (2004): 481.

requirements, and the imposition of new crimes and penalties.[14] For the financial sector, being able to track the flow of money is seen as critical in helping to identify and prevent future terrorist attacks. Changes to existing laws and practices have been implemented in an effort to make it easier for law enforcement and intelligence officials to access financial records. However, the changes have been an "implementation nightmare" [15] requiring banks to move from a "compliance focus to a more comprehensive, risk-based strategy to detect and report potential money laundering."[16] These changes have created the need for a whole host of identity verification and data transaction analysis products and services for the financial service industry as companies try to meet these new requirements. In a sense the "banks have been deputized as federal law enforcement agencies." In creating such an enormous mountain of financial information, the problem remains as to how the Government will be able to manage this information in a way that is sense-making, that will find the relevant items of information that may be carried along in the flood of reporting provided by financial institutions.

II. Educational Institutions

Among the various acts amended by the *Patriot Act* stands the *Family Educational Rights and Privacy Act (FERPA)*. Previously this act (*FERPA*) required student consent for the release of academic records; however, as it now stands pursuant to a court order, educational institutions are required to disclose student records to federal law enforcement authorities in conjunction

[14] Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004.
[15] Regan, Priscilla M. "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." Government Information Quarterly 21.4 (2004): 481, p. 485.
[16] Ibid. p. 485.

with a terrorism investigation.[17] In addition, the Immigration and Naturalization Service powers have been broadened with respect to the collection of information on foreign students. Under the *Patriot Act* educational institutions are required to collect and maintain passport and visa information. As Regan notes, "part of the difficulty is that educational institutions now maintain a plethora of records on students, faculty, and staff from traditional academic and personnel records to purchases with ID-based accounts and communications transactions, including Internet and e-mail records."[18]

III. Libraries

The library community has long protected the confidentiality of patrons' records. Section 215 of the *Patriot Act* in its amendments to the *FISA* has broadened the access of law enforcement agencies to "business records" and "all tangible things." In the library this could include access to patron library records and records of online activities. Patron records, until now, were only accessible with a warrant that was issued with probable cause; now law enforcement officials only require that foreign intelligence be a "significant purpose" of the investigation.[19] As Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure note, librarians must face the fact that any of the records they keep on patrons could be covered by a *FISA* warrant[20] issued by the Foreign Intelligence Surveillance Court (FISC) – and such a warrant does not require probable cause.

---

17 Ibid. p. 486.
18 Ibid. p. 486.
19 Ibid. p. 489.
20 Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99, p. 100.

IV. Internet and Communications Companies

A wide range of communications records have long been viewed as an integral part of any intelligence gathering investigations. These records can contain vast amounts of information on voice and data transactions such as the time that the communication took place, its length, the parties involved, as well as historical information on the frequency and patterns of communications. Given the vast amount of information that can be gleaned from these records, policies to protect an individual's "reasonable expectation of privacy" were incorporated in Title III of the *Omnibus Crime Control and Safe Streets Act* of 1968, the *Foreign Intelligence Surveillance Act* of 1978, and the *Electronic Communications Act* of 1986.[21] The *Patriot Act* has served to change many of these privacy expectations, particularly through the use of National Security Letters (NSLs).

V. Transportation

Given the means used by terrorists in the September 11th attacks, there should be little surprise that a great deal of attention has focused on airport security. The Department of Homeland Security has initiated several passenger screening systems as a way to ensure that the use of airplanes as weapons does not happen again. That said, how these systems maintain the records that they keep on passengers and their effect on privacy is something that needs to be examined more closely.

Following 9/11, the Government's use of the Computer-Assisted Passenger Prescreening System (CAPPS), resulted in a number of innocent Americans being unable to board their flights

[21] Regan, Priscilla M. "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." Government Information Quarterly 21.4 (2004): 481, p. 487.

because the screening criteria in CAPPS had produced false positives – individuals being wrongly matched to names on terrorist watch lists. Perhaps most famously, Senator Ted Kennedy was repeatedly subject to secondary screening because of criteria identified by CAPPS.[22]

If the CAPPS results were controversial, the Transportation Security Administration's (TSA) slated replacement for CAPPS, CAPPS II, was even more so. Under this new scheme, "data, including name, phone number, itinerary, and method of payment"[23] was to be transmitted by the individual airlines to CAPPS II. The system upon receiving this information would then request identity authentication from the airlines, who in turn, would send CAPPS II an identity authentication score. [24] Using this score, the proposed CAPPS II would then "use government databases, including classified and intelligence data, to conduct a risk assessment score, which would be transmitted to the check-in counter." [25]

Civil liberties groups such as the Electronic Frontier Foundation (EFF), among others were particularly concerned about the risk of false positives and they warned the public that:

> Based on your assigned color/score, you could be detained, interrogated or made subject to additional searches. If you are tagged with the wrong color/score, you could be prohibited from flying.[26]

---

[22] Henry, Ed and Ahlers, Mike. "Kennedy: Airline security risk? Senator tells of Screening Stops at Airport." CNN. August 19, 2004. <http://www.cnn.com/2004/ALLPOLITICS/08/19/kennedy.airlines/index.html>.
[23] Ibid. p. 487.
[24] Ibid. p. 487.
[25] Ibid. p. 487.
[26] Electronic Frontier Foundation. "CAPPS II: Government Surveillance via Passenger Profiling"

After a wave of opposition from both civil liberties groups and a number of politicians (Kennedy among them) the proposed CAPPS II was soon replaced by a new screening program called Secure Flight. According to the Department of Homeland Security, this new program:

> …shifts pre-departure watch list matching responsibilities from individual aircraft operators to the Transportation Security Administration (TSA) and carries out a key recommendation of the 9/11 Commission. By bringing watch list matching responsibilities in-house, TSA can better remedy possible misidentifications when a traveler's name is similar to one found on a watch list.[27]

Despite this reassurance from the TSA, the American Civil Liberties Union (ACLU) remains concerned about the "lack of adequate redress for individuals who are mistakenly matched to the secret government watch lists."[28]

Purpose of the Information Collection

Following 9/11 numerous statutory changes were implemented that resulted in a reduction in privacy protection for a variety of sectors including: the financial, educational, library, internet

---

<http://w2.eff.org/Privacy/cappsii/>.

[27] Homeland Security Press Release. "TSA to Assume Watch List Vetting with Secure Flight Program" October 22, 2008. <http://www.dhs.gov/xnews/releases/pr_1224686539438.shtm>.

[28] American Civil Liberties Union. "Secure Flight Re-Engineering Welcomed but Watchlist Problems Remain Unaddressed." October 22, 2008. <http://www.aclu.org/technology-and-liberty/secure-flight-re-engineering-welcomed-watchlist-problems-remain-unaddressed>.

communications and transportation sectors. One of the forces driving these changes, according to Barbara Ann Stolz, was 'symbolic politics.' Symbolic politics is a theory which looks at the political actions of individuals or political actors as symbols aimed at influencing a particular audience. Stolz uses this theory as a mechanism for explaining the actions of political actors in the post 9/11 period. Stolz uses the following four functions: reassurance, moral-educative, educative, and enhancement of Office-holder popularity as a guide to understanding symbolic politics. [29]

I. Reassurance

The first function in Stolz's model addresses the need to reassure the public through legislation that the Government was acting by giving law enforcement officials the tools they needed to prevent future terrorist attacks. Certainly the passage of the *Patriot Act* six weeks after the September 11th attacks was an attempt to reassure the public that the Government was acting and it was acting swiftly to prevent any future attacks. However, as Stoltz acknowledges, the new legislation did not reassure all groups, particularly those afraid of civil liberties violations similar to those which occurred in the Watergate-era.[30]

II. Moral-Educative: Line Drawing

The second function, moral-educative, refers to the traditional line that is drawn between law-abiding and non law-abiding citizen behaviour in the criminal justice system. Criminal law punishes the law breakers and in effect praises the law abiders.[31] In Stoltz's model, the changes

[29] Stolz, Barbara Ann. "The Foreign Intelligence Surveillance Act of 1978: The Role of Symbolic Politics." Law & Policy 24.3 (2002): 269.
[30] Ibid. p. 288.
[31] Ibid. p. 271.

to FISA (which changed the intelligence gathering requirements for intelligence investigations from one of "primary purpose" to "significant purpose")[32] involved a form of moral educative line drawing because it drew the line between the external enemy terrorist and the law abiding citizen. The symbolic narrative of the new law according to Stoltz points to the future: it is a future in which there is a continued threat of terrorist attack by an evil enemy against a virtuous law-abiding nation, the United States.[33]

III. Educative Function: Simplification through Symbolization

The third function, educative, in Stoltz's model, refers to the need for some public education with regards to *FISA* given the number of amendments to that Act by the *Patriot Act*; however, the approach was to simplify the response to these questions (i.e. "by fixing the 'gaps' in *FISA*, the threat of terrorism would be reduced, because the tools for "combating the enemy" had been strengthened").[34] The result is therefore a kind of oversimplification of the impact of these legislative changes. A nervous public may feel so reassured by the simplified response that they don't question any potential negative impacts (say for example any impact upon civil liberties) of the new law.

IV. Enhancement of Office-holder Popularity

And lastly, Stoltz's fourth function involves the enhancement of the Office-holder's popularity. Here the Office-holder's popularity is increased on the basis that he/she is seen to act. Questioning or not supporting a particular piece of legislation that is popular could be damaging

[32] Ibid. p. 289.
[33] Ibid, p. 289.
[34] Ibid, p. 290.

to the Office-holder's popularity and future career if they are viewed as not acting. In this sense towing the line in order to maintain popularity is problematic not just in terms of the motivation of the individual's actions, but also in terms of the law and policy such action produces.

The use of symbolic politics as a framework that may be used to study criminal justice policymaking is interesting, but even Stolz herself acknowledges that there are limitations. The framework does not explain all aspects of the policymaking process or provision of a particular legislative proposal, nor does it consider other sociological influences on law and lawmaking such as class conflict or globalization. The theoretical framework that she presents does not touch on normative issues (i.e. those associated with rights). That said, the application of this framework to specific case studies does provide insight into the policymaking process underlying the legislation. Factors such as the importance of public perception of the particular policies and the policymaking process do have an impact on the legislative process. In addition, the ability to compare legislative proposals at different points in time (as she does with *FISA*, looking at various amendments over a period of more than twenty years) is insightful and contributes to our understanding of the criminal justice policymaking process.[35]

Constitutional Considerations

Where do Fourth Amendment rights fit in foreign intelligence investigations?

The above question is one that all of the authors covered in this literature review acknowledge in

[35] Ibid, p. 296.

their work. However, the degree to which each author felt that citizens should have access to the information collected about them by the Government varied significantly. For authors such as Rebecca A. Copeland, in her article "War on terrorism or war on constitutional rights? Blurring the lines of intelligence gathering in post-September 11 America,"[36] it is clear that recent legislative changes have had a negative impact on constitutional rights. Copeland acknowledges the need of the Government to conduct secret electronic surveillance in order to prevent future terrorist attacks; however, she argues that this government power must not be used in such a way as to deprive citizens of their fundamental constitutional rights.

Ava Barbour in her article "Ready…aim…FOIA! A Survey of the *Freedom of Information Act* in the Post-9/11 United States,"[37] is also worried about the potential for the Government to use the increased powers that it has acquired as a result of post-September 11th legislation, to ignore civil liberties. In her article, Barbour looks to the *Freedom of Information Act* as essential to preventing potential abuses, the kind that can arise as a result of overreaching and excessive government secrecy. Barbour points to the lessons of history, citing the Vietnam and Watergate eras that prompted the U.S. Congress to institute measures to strengthen the Freedom of Information Act. As she notes, Vietnam and Watergate "led to public distrust, and eventually apathy, with our government and our political system. Following the tragedy of September 11th, distrust and apathy are the last things America needs."[38] Barbour suggests that in order to "defend our freedom and our security,"[39] the public must be vigilant about participating in the

[36] Copeland, Rebecca A. "War on Terrorism Or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America." Texas Tech Law Review 35.1 (2004): 1.
[37] Barbour, Ava. "Ready…aim…FOIA! A Survey of the *Freedom of Information Act* in the Post-9/11 United States." The Boston Public Interest Law Journal 13 (2004): 203.
[38] Ibid, p. 226.
[39] Ibid, p. 226.

democratic process. For Barbour it is clear that the *Freedom of Information Act* must be preserved intact in the post-September 11th legislation, in order to ensure that government remains accountable to the people.

For Michael V. Hayden, it is clear that there must be a balance between security and liberty. The issue of privacy protection is one which even the 9/11 Commission has acknowledged requires effective oversight.[40] As Hayden argues, the application of set rules, along with an effective oversight structure that includes the executive, legislative, and judicial branches, would strengthen security without diminishing the constitutional liberties of the American people.[41] Hayden points to the amendments to the *FISA* which have allowed for increased sharing of information between agencies and the FISC which provides a judicial safeguard as an example of both rules and effective oversight which serve to protect rights (both *FISA* and the FISC Court are described in more detail below).

Although there is a judicial safeguard in place, the executive branch has not been immune from criticism from the Department of Justice's Office of the Solicitor General and Office of Legal Counsel, the principal constitutional interpreters for the executive branch when it comes to the *Patriot Act*. One of the safeguards put in place by Congress to prevent potential abuses under the *Patriot Act*, according to Cornelia T.L. Pillard in her article, "The unfulfilled promise of the Constitution in the Executive hands,"[42] was to include in the Act a provision charging the Inspector General in the Department of Justice to investigate and report on claims of civil rights

---

[40] Hayden, Michael V. "Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence." Notre Dame Journal of Law, Ethics & Public Policy 19 (2005): 247, p. 260.

[41] Ibid, p. 260.

[42] Pillard, Cornelia T. L. "The Unfulfilled Promise of the Constitution in the Executive Hands." Michigan Law Review 103 (2005): 676, p. 756.

or civil liberties violations by Department of Justice employees. The Inspector General has filed semi-annual reports identifying over two thousand civil rights or civil liberties complaints. Of these complaints the Inspector General deemed several dozen as credible after investigation.[43] In a special report issued in June 2003, the Inspector General listed practices regarding classification of arrestees and detainees, information sharing among agencies, processing and clearing detainees, and treatment of detainees during their confinement, as being problem areas. The Inspector General used this opportunity to offer 21 recommendations for reforming Executive practices to minimize incursions on civil rights and civil liberties. At that time the Executive had "not announced refinements or elaborations of its relevant constitutional views on individual rights that respond to the range of problems" identified by the Inspector General.[44] This is something which Pillard says underscored the "lack of more general, active constitutional self-monitoring and reflection" within the executive branch. [45]

Understanding FISA

In order to understand the significance of the *Patriot Act* with regards to intelligence surveillance, Alison A. Bradley notes that you first need to have a good understanding of the history behind one of the key acts which it amends, the *FISA*. In her article Bradley looks in depth at the events that led to the creation of *FISA* and the Foreign Intelligence Surveillance Court (FISC), and the various amendments which have facilitated an increase in surveillance for national security purposes up to the present. The creation of both *FISA* and FISC, Bradley notes, are rooted in the political revelations of the Nixon administration. During this administration electronic surveillance was used to monitor so-called "subversive groups" – such groups were

[43] Ibid, p. 756.
[44] Ibid, p. 757.
[45] Ibid, p. 757.

domestic and therefore lacked the requisite foreign nexus. Revelations that the administration had gone so far as to monitor the Democratic Party during the 1972 Presidential campaign were what led to the Watergate scandal and the eventual downfall of the Nixon administration.[46]

At the time of the Nixon administration, the core legislation governing the use of wiretapping for criminal law enforcement purposes was contained in *The Omnibus Crime Control and Safe Street Act* which authorized the use of electronic surveillance for specific classes of crimes. Although the use of surveillance as outlined in this statute was subject to significant limitations, and required a court order on the basis of probable cause, nowhere was there a restriction on the administration's use of surveillance involving matters of national security. The act thus confirmed presidential authority to conduct warrantless electronic surveillance.[47]

The solution to this problem was deemed to be the creation of the *Foreign Intelligence Surveillance Act* (*FISA*). After "six years of debate, compromise, and negotiation between the administration and federal agencies" *FISA* was enacted in 1978.[48] As Bradley notes, the initial idea behind *FISA* was that it would provide a balance between protecting the constitutional rights of citizens while at the same time allowing the Administration to provide for national security. Under *FISA,* a separate court called The Foreign Intelligence Surveillance Court (FISC) was established. It is through this court that government agents are granted the ability to surveil targets if there is probable cause that the subject of the search is a foreign power or agent of a

[46] Bradley, Alison A. "Extremism in the Defense of Liberty? the Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT Act." Tulane Law Review 77 (2002): 465, p. 469.
[47] Ibid, p. 472.
[48] Ibid, p. 473.

foreign power.[49] This is contrary to the regular legal system that requires that there must be probable cause that a crime has been committed before a warrant will be issued.[50] Under section 215 of the *Patriot Act*, *FISA* was substantially altered by expanding the term "record" to include "any tangible item that contains information."[51] The result of this change was that it essentially opened up the use of *FISA* warrants as a means by which law enforcement agencies could conduct fishing expeditions through their collection of personal information from electronic communications, voice mail, and any physical or electronic record.

Changes to FISA pre 2007

Joseph G. Poluka, in his article "The Patriot Act: Indispensable tool against terror,"[52] on the other hand, argues that the criticisms directed at the *Patriot Act* are unfounded. The primary purpose of the Act, he asserts, was to remove the barrier between traditional law enforcement officials and counterintelligence agents (whose duty it is to protect national security) in their sharing of information. Prior to the passage of the *Patriot Act*, law enforcement officials could not share information with FBI counterintelligence agents, and vice versa. The *Patriot Act* has amended *FISA* in order to allow the use of *FISA* whenever foreign intelligence is a "significant purpose," rather than "the purpose," of an investigation. This change has allowed law enforcement agents and prosecutors to "determine if there is a basis for bringing criminal

[49] Breglio, Nola K. "Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance." Yale Law Journal 113 (2003): 179.
[50] Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004, p. 35.
[51] Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99, p. 104.
[52] Poluka, Joseph G., "The Patriot Act: Indispensable tool against Terror." Pennsylvania Bar Association Quarterly 76 (2005):33, p. 35.

charges against the targets of a foreign intelligence investigation."[53] Here it is important to note that the individual must be a target of a foreign intelligence investigation. Poluka is quick to dismiss worries about ordinary citizens having their rights violated through the use of *FISA* warrants since individuals are protected in three ways. First, a *FISA* court order is required in order for the FBI agent to obtain records. Second, section 215 can only be used for matters involving "international terrorism and clandestine intelligence activities or to obtain foreign intelligence information not concerning a United States person" – it cannot be used to investigate domestic terrorism or ordinary crimes. Third, it cannot be used be used to conduct investigations "solely on the basis of activities protected by the First Amendment"[54] which protects freedom of religion, speech, press, assembly, and the right to petition the Government.

In her article "Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques," Solveig Singleton suggests that the "power grab" theory advanced by civil libertarians may be tempting but underestimates the possibility that there might actually be valid law enforcement arguments.[55] Although it is true that the *Patriot Act* cannot be used to investigate domestic terrorism or ordinary crimes, there are times where it "will often be difficult, if not impossible, for investigators just starting an investigation of some kind of odd or suspicious conduct to know in advance whether they are investigating terrorism or 'ordinary' crime."[56] The potential for errors in requesting a set of powers that is either "too much" or "too little," Singleton argues could prove to be disastrous for an investigation. She gives two examples of how this could play out: in one the prosecutor is finally in a position to lay charges,

---

53 Ibid, p. 36.
54 Ibid, p. 38.
55 Singleton, Solveig. "Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques." Ohio Northern University Law Review 30 (2004): 417, p. 418.
56 Ibid, p. 430.

but the evidence has to be excluded (because the set of powers requested was ultimately determined to be "too much"); in the other, there is a mass disaster because the set of powers requested was "not enough."[57] It is clear from Singleton's article that questions concerning the potential for infringement of one's civil liberties have to be weighed and balanced against the national security concern.

In a similar vein, Katherine Coolidge believes that the controversy concerning the potential violation of the rights of ordinary citizens by the Department of Justice is overblown. Coolidge outlines the process for obtaining *FISA* warrants, and is of the opinion that this process has sufficient oversight. As she notes, the Foreign Intelligence Surveillance Court (FISC) consists of eleven federal district court judges who have been appointed to the FISC for a limited term (maximum seven years). These judges have years of experience on the federal bench, and according to Coolidge, it would be an outrage to assume that once a judge has been appointed to the FISC that "suddenly their standards of professional conduct and respect for the integrity of the legal profession dissipate."[58]

For Poluka, Singleton and Coolidge the suggestion seems to be that, unless you are conducting activities related to terrorism, you need not worry as there are protections built into the legislation which will prevent its use against ordinary citizens. However, for authors such as Paul T. Jaeger, John Carlo Bertot, and Charles R. McClure, concern over the amendments to the *FISA* by the *Patriot Act* should not be so quickly brushed aside. The changes to *FISA* have, as

---

[57] Ibid, p. 430.

[58] Coolidge, Katherine K. "Baseless Hysteria: The Controversy between the Department of Justice and the American Library Association Over the USA PATRIOT Act." American Association of Law Libraries Law Library Journal 97 (Winter 2005): 7, p. 11.

they say, dramatically altered the ability of the Government to collect and analyze personal information. The authors state that the "the ways in which the *Patriot Act* modifies *FISA* are clearer at this point than the impacts of these alterations over time."[59] These changes have significantly modified the original scope and intent of *FISA*, which make their final impact on American information policy hard to discern given the level of secrecy surrounding the *U.S.A. Patriot Act* which amends it. The problem that Jaeger and his colleagues acknowledge is that one is not in a position to adequately judge whether or not law enforcement agencies are respecting the constraints on the use of FISA because of the high level of secrecy surrounding how the Act is used, secrecy which the Government claims is essential to the proper functioning of the Act itself.[60]

Oddly enough, the initial amendments to *FISA* under the *Patriot Act* were something which Nola K. Breglio took issue with as early as 2003, but for a very different reason than that of Jaeger, Bertot, and McClure. Breglio then charged that the changes brought about by the *Patriot Act* had damaged the usefulness and the legitimacy of *FISA* and the FISC. In her article "Leaving *FISA* Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance," Breglio made a case for the abolition of *FISA* and argues that warrantless searches should be held as the standard in foreign intelligence cases. As Breglio stated, her intention was not to give the Department of Justice a "blank check to investigate anyone, anytime, anywhere; such a regime would cause the kind of backlash that prompted the passage of *FISA* in the first place."[61] Rather, her intention

---

[59] Ibid.

[60] Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99, p. 108.

[61] Breglio, Nola K. "Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance." Yale Law Journal 113 (2003): 179, p. 181.

was for the creation of a system in which the executive and legislative branch would be subject to strict internal review procedures to ensure accountability and to prevent the kind of abuses that *FISA* was intended to prevent in the first place.

Prosecutors in Breglio's model would have to give targets of warrantless operations notice at the conclusion of such investigations. This would allow targets of such a surveillance operation to contest the surveillance in court. This change, she argued, would benefit all parties involved as it would allow the Department of Justice greater flexibility in conducting investigations, "as it would not have to procure judicial warrants and could act rapidly to investigate time-sensitive threats." In addition, the level of openness about investigations at their close would increase as they would be removed from the "super secret domain of the FISC."[62] This change would make the Attorney General publicly accountable for his orders, and would allow persons subject to investigation an opportunity to challenge the basis of their investigation in court. Here also, courts could investigate the constitutionality of such warrantless searches. By the end of December 2005, it became widely known that the Government had actually been conducting warrantless surveillance outside the domain of FISA and the FISC, although unlike Breglio's suggestion here, no notice of past warrantless searches was ever communicated to the target of such a search.

Still others, such as Jennifer L. Sullivan, in her legal note, "From 'the purpose' to 'a significant purpose': Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment," argue that the Government is justified in overriding individual liberties in

[62] Ibid, p. 181.

the interest of national security.[63] Sullivan, in her commentary on the state of foreign intelligence surveillance for national security purposes in the post-September 11th period, notes that September 11th "dramatically highlighted the startling inadequacies of prior legislation that had been enacted to address the problem of domestic and international terrorism."[64] The recent changes to *FISA* have become a rallying cry for civil libertarians who argue that the new amendments allow law enforcement officials to bypass the traditional warrant requirements of the Fourth Amendment. This claim, according to Sullivan, is unsubstantiated since the *Patriot Act*, via the language set forth in section 218 of the act, clearly satisfies both the Warrant Clause and the Reasonableness Clause of the Fourth Amendment.[65] Although *FISA* warrants require a reduced probable cause standard than is required for other types of warrants, this is something that Sullivan notes has consistently been held to be within the bounds of the Constitution.

National Security Considerations

Are there exceptional circumstances under which the right to privacy can be waived in the interest of national security?

Authors such as Laura Taylor Swain point out that a wartime context does transform the threshold question concerning civil liberties:

> The Constitution grants unique powers to the political branches with respect to the

[63] Sullivan, Jennifer L. "From 'the Purpose' to 'a Significant Purpose': Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment." Notre Dame Journal of Law, Ethics & Public Policy 19 (2005): 379.
[64] Ibid, p. 412.
[65] Ibid, p. 382.

> conduct of war and foreign policy; the courts continue to have the responsibility to determine, in the context of particular cases of which they have jurisdiction, whether particular actions are within the scope of those powers and other relevant Constitutional limits as a legal and factual matter.[66]

The courts, according to Swain, have a responsibility to discern whether the authority exercised by the executive has been outside the bounds of the Constitution.[67] Liberty is not to be trampled on in an effort to protect national security interests here. That said, it must be placed in proper balance so as to protect the rights of the individual and the public good.

All of the articles covered in this literature review acknowledge that a fine balance must be struck so that national security needs can be met while at the same time respecting constitutionally protected civil liberties. Whether or not the initial legislative changes that took place through the *Patriot Act* provide such a balance is open to debate. For authors such as Jeff Breinholt and Michael F. Dowley, the Act does provide such a balance. Breinholt, in his article "How About A Little Perspective: The *U.S.A. PATRIOT Act* and the Uses and Abuses of History,"[68] points out that those who oppose the *Patriot Act* have tended to look to the lessons of history to base their objections to the Act – that is to say that they have looked to instances where civil liberties abuses have been carried out in the name of protecting national security only later be have been found excessive. The argument put forth by those who object to the Act, according to Breinholt, is that the Act allows for similar excessive violations of civil liberties under the

---

66 Swain, Laura Taylor. "Liberty in the Balance: The Role of the Third Branch in a Time of Insecurity." Suffolk University Law Review 37 (2004): 51, p. 77.

67 Ibid, p.77.

68 Breinholt, Jeff. "How about A Little Perspective: The USA PATRIOT Act and the Uses and Abuses of History." Texas Review of Law & Politics 9 (2004): 17.

guise of protecting national security. What these critics fail to do, Breinholt argues, is acknowledge the series of massive reforms and limitations on law-enforcement operations that arose out of those excesses.[69] To make the argument that the *Patriot Act* is part of a pattern of abuses is absurd, given the legal protections offered by past reforms – ones which the *Patriot Act* works in accordance with. Breinholt goes further to say that even if it were possible that such violations could occur, the present laws provide the necessary additional check; thus there is no excuse to label this as part of an historical pattern given the existence of recourse through the courts.[70] This last point is particularly interesting given the number of civil liberties groups currently pursuing court action in regards to this Act, which seems to suggest that they do not agree with Breinholt's summation of this Act, but are willing to take him up on the offer to test the checks and balances.

Michael F. Dowley is in agreement with Jeff Breinholt that the *Patriot Act* strikes a reasonable balance, but he offers different reasons for this assessment. Dowley, in his article, "Government Surveillance Powers Under the *U.S.A. PATRIOT Act*: Is it Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War," notes that the "drafters of the Constitution provided government with the necessary authority to protect this country during times of war and times of significant national security threats."[71] The idea that "in every conflict between liberty and governmental-imposed order concerning issues of national security, liberty should not always prevail"[72] is not particularly new, but the justification that Dowley

---

[69] Ibid, p. 19.
[70] Ibid, p. 59.
[71] Dowley, Michael F. "Government Surveillance Powers Under the USA PATRIOT Act: Is it Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War." Suffolk University Law Review 36 (2002): 165, p. 174.
[72] Ibid, p. 174.

presents to support this position seems a bit misplaced. He points to instances where the Government, in order to protect national security, has extinguished "civil liberties without regard for constitutional constraints."[73] His list of historical events includes the *Alien and Sedition Acts* in 1798, the Civil War suspension of the writ of habeas corpus, the curtailment of antiwar speech during World War I, the treatment of Japanese-Americans during World War II, and the Cold War persecution of communists. According to Dowley, it was not until the 1960s and 1970s that Americans really began to witness greater protection of civil liberties. During that time the Supreme Court took on a more active role in protecting these liberties. Dowley seems to imply that this increase in protection was correlated to a lack of significant threats to America's national security. Given the events of September 11th, he believes that the expectations regarding civil liberties have changed forever.

Dowley acknowledges that:

> …[a]lthough provisions of the Act may inadvertently infringe on precious civil liberties vital to this nation's survival, its implementation may ensure America's continued existence by allowing government agents to keep pace with technological advancements and monitor elusive terror networks within this country's borders. Future judicial review may more neatly tailor the Act to satisfy the Government's interests without infringing on civil liberties with such severity.[74]

Dowley believes that, as enacted, the *Patriot Act* provides a reasonable and constitutional

[73] Ibid, p. 174.
[74] Ibid, p. 178.

balance between upholding civil liberties and protecting national security.

On the contrary, authors such as Timothy Edgar, Witold Walczak, Emanuel Gross and Philip B. Heymann hold that this hardly seems an acceptable balance. Edgar and Walczak in their article "Perspectives on the U.S.A. PATRIOT Act: We can be both Safe and Free: How the PATRIOT Act Threatens Civil Liberties," make the argument that the *Patriot Act* has placed civil liberties in a precarious position.[75] They see the Act as a direct threat to privacy rights and point to the newly expanded powers which have enabled the Government to increase its ability to monitor everything from an individual's internet use, to sensitive educational, banking, credit, consumer, communications and even library records through the use of National Security Letters (NSLs).[76] As the authors state, such "letters can be issued for any documents – or even whole databases – the FBI believes are relevant to an investigation to protect against terrorism" and do not require a court order. This is a shift from previous requirement that such letters "only be issued in cases where there exist 'specific and articulable facts' that the records concern a terrorist, spy, or other foreign agent."[77]

As Emanuel Gross has pointed out in his article, "The Struggle of a Democracy Against Terrorism – Protection of Human Rights: The Right to Privacy Versus the National Interest - the Proper Balance," the *Patriot Act* significantly expands the power of the FBI to demand "not only records but also "any tangible things," from any body or person (such as a book shop or internet service provider), and not only in cases where there is reason to believe that the subject of the

[75] Edgar, Timothy, and Witold Walczak. "Perspectives on the USA PATRIOT Act: We can be both Safe and Free: How the PATRIOT Act Threatens Civil Liberties." Pennsylvania Bar Association Quarterly 76 (2005): 21.
[76] Ibid, p. 22.
[77] Ibid. p. 27.

information request is a foreign agent, but where any person is involved."[78] Gross notes that once a body or person has handed over this information, they are prohibited from telling anyone that this handover took place by a gag order built into the law.[79] This leaves open the potential for cases in which no security justification for secrecy exists but individual privacy rights are infringed. Only the person or body contacted to give the information will know that the search took place, but they will not be able to challenge the legality of the search. It is because of the removal of this prior restraint on the use of such letters to obtain such information that these authors, unlike Breinholt, see parallels between the civil liberties abuses by governments of the past and the potential for modern day abuses.

Philip B. Heymann, in his article, "Civil liberties and Human Rights in the Aftermath of September 11,"[80] claims that the risks to civil liberties will depend upon how the Government responds to the following three objectives: prevention, consequence management, and punishment of terrorists. As Heymann describes it, the issue at hand is not one of new legislation, but rather the discretion of the executive branch of government in its use of newly defined powers. These issues involve "matters of life or death, torture, detention without trial, trial without juries, and basic freedoms to dissent."[81] How the executive branch chooses to come to terms with the threat of terrorism both within its borders and abroad will impact civil liberties within the country and could have potentially harmful consequences for human rights abroad. If there is a perception of anything less than equal citizenship and equal protection under the law

[78] Gross, Emanuel. "The Struggle of a Democracy Against Terrorism – Protection of Human Rights: The Right to Privacy Versus the National Interest - the Proper Balance." Cornell International Law Journal 37 (2004): 27, p. 74.
[79] Ibid, p. 74.
[80] Heymann, Philip B. "Civil Liberties and Human Rights in the Aftermath of September 11." Harvard Journal of Law & Public Policy 25.2 (2002): 441.
[81] Ibid, p. 441.

for citizens – i.e. if the Government in its efforts to prevent terrorism chooses to focuses only on limited ethnic identities - then there is a high risk that innocent members of society may be subjected to investigation. If these false positives are large enough in number, then there is the risk that those who belong to those groups but do not support terrorist activities might themselves become sympathetic to the organization if they feel themselves to be less than full citizens.

With regards to consequence management, Heymann acknowledges the complexity of dealing with modern terrorist threats. As he notes, at the heart of the problem of consequence management is preparation:

> …getting into place the committed physical and human resources, skills and advance training, plans, understandings as to cooperation across functional and jurisdictional lines, and legal authority that we would want if and when a plausible threat or actual use took place.[82]

If the U.S. is to be prepared to deal with any possible threat of a major terrorist attack, according to Heymann, it will need to have the resources, training, and authority firmly in place to cope with a variety of different scenarios.

Conclusion

In compiling this literature review, I chose to draw upon articles which related to three central

[82] Ibid, p. 450.

research questions, namely:

What ethical, legal or political considerations should be taken into account with regard to the collection, classification, and dissemination of citizens' personal information by government departments and agencies?

Where do Fourth Amendment rights fit into foreign intelligence investigations?

Are there exceptional circumstances under which the right to privacy can be waived in the interest of national security?

In synthesizing these articles, I found that the majority focused on issues regarding the encroachment upon civil liberties. In addition, there has been a great deal of discussion about whether or not such limitations on civil liberties are reasonable given the new threat of terrorism in the U.S. Although there is a vast amount of scholarship concerning the legal and political situation with regards to collection and use of information in the post-September 11th environment, I found it striking that there were relatively few articles which dealt with ethical constraints underlying limitations on the collection, classification and dissemination of information. All of the articles looked at civil liberties from either a political or legal angle, but none explicitly addressed the nature of such liberties and why they are in and of themselves important. Failing to address foundational issues makes it difficult to judge in a conclusive way when or if civil liberties may legitimately be curtailed. In instances where civil liberties could arguably be traded off to purchase additional security, I think it is important that we address the

root issues.

PART II:

TOWARDS AN ETHICAL FRAMEWORK

Chapter 3:

Philosophic Approaches to Information Ethics

Should Internet Service Providers be compelled to give out customer search and email records to government agencies?

Should airlines be required to turn over all passenger data to the government?

Should Library patron records, including online searches, downloads, and book records, be turned over to government agencies?

Should data mining programs that search emails for use of terrorism-related keywords be used as part of the war on terror?

Any attempt to answer questions such as the ones I have posed above will require that some sort of judgment be made regarding the acceptable level of government intrusion into the private sphere. Responding to these kinds of questions will require a moral judgment – that is a judgment about what is the right course of action to be taken. This chapter provides a brief introduction / overview to the branches of ethics (more generally), and then to some of the ethical theories (more specifically) which have had an influence on the shaping of legislation and policy in the U.S. The chapter concludes with a discussion of whether or not the recent shifts in American lawmaking regarding security and privacy are the result of a greater underlying shift in the ethical preferences of lawmakers, one that possibly favours consequentialist arguments over

rights-based ones.

Moral Reasoning

Ethics is the philosophical study of morality, that is, of right conduct, obligation, responsibility, and social justice. Philosophers who specialize in ethics attempt to provide general, systematic, reasoned theories of the right answers to moral questions, rather than merely describing the various answers individuals and societies have in fact given to such questions and explaining how they arrived at them.

Ethics as a discipline can be broken down into the following three branches:

- *Meta-ethics*
- *Normative Ethics*
- *Applied Ethics*

Meta-ethics

The first branch, meta-ethics, can be defined as the philosophical study of the nature of moral judgment. As the name would suggest, meta-ethics is concerned with foundational issues, for instance, with the meaning of moral terms such as "right" and "wrong," with the objectivity (or lack thereof) of moral judgments, and so forth. Questions of this kind are in some sense logically prior to moral judgments themselves, but they are distinct from them, and most meta-ethicists hold that they have little direct bearing on such judgments. The fact that a rights-based constitution deems the rights within it to be inalienable is interesting from a meta-ethical point of view. The principles which the constitution lays out themselves contain ethical principles – that

is they set out the rights which the constitution protects. By doing so in this fashion, it assumes that the rights a constitution protects exist prior to the constitution - they would have to if they are deemed inalienable. If we accept this as our starting point, then we can say that the constitution emerges from an ethical framework. Although foundational issues of this kind are outside the scope of this study, the fact that inalienable rights would require some kind of meta-ethical grounding within the constitution itself presents an interesting philosophical question about the foundation for any rights-based constitution.

Normative Ethics

Normative ethics, on the other hand, sets out norms or rules related to action. Meta-ethics concerns itself with the nature of norms, while normative ethics aims to delineate norms and grounds of judgments themselves. Normative ethics have traditionally been broken down into two groups: teleological, which are theories of the good; and deontological theories, which are theories of duty. This latter group is typically broken into two separate categories: duty-based and rights-based ethics.

Applied Ethics

Applied ethics is, simply put, the application of ethical theories (i.e. utilitarianism, contractarianism, etc.) to particular practical domains. Applied Ethics is varied in its areas of specialization, with each area having its own centres for research and teaching, specialized journals, and a rapidly growing literature. The areas of specialization are vast and include medical ethics, business ethics, legal ethics, environmental ethics, computer ethics, and most recently, information ethics.

Information Ethics

The focus of this dissertation is on these last two branches of ethics: normative and applied ethics. Exploration of the former will be necessary in order to apply ethical theory to and create a framework for the applied area of specialization: information ethics. Questions concerning the development and resolution of ethical conflicts in the information field will be the primary focus of this work. For the purposes of this dissertation, the term *information ethics* as narrowly construed is the application of normative ethical theories, to issues regarding information and it use. More broadly construed, information ethics includes standards of professional practice, codes of conduct, and aspects of information law, public policy and so forth. This definition of 'information ethics' should be distinguished from some of the existing uses of the phrase in information studies literature. For example, Toni Samek's Librarianship and Human Rights stresses the importance of information ethics for those engaged in the information professions, but does so in a way that is resolutely intercultural and seen "through the lens of individuals, institutions and societies."[83] One of the key goals of this study is to establish a more stable definition and foundation for information ethics.

From Theory to Practice: Normative Theories and Applied Information Ethics

Ethical theories come in many forms, each with their unique merits and shortcomings. In this section I explore a few of the main normative approaches to ethics and discuss their potential application to information ethics broadly, but more specifically to the problems associated with government intrusion into the private sphere in insecure times. This section examines two distinct types of normative ethics, namely, teleology and deontology, and the potential

[83] Samek, Toni. Librarianship and Human Rights: A Twenty-First Century Guide. Oxford: Chandos, 2007, p. 10.

application of such theories in our given context.

Teleological Theories: Utilitarianism

"Telos" is the ancient Greek term for an end, fulfillment, completion, goal or aim: it is the root of the modern word "teleology." As the name of the view would suggest, teleological theories in normative ethics begin with a conception of the good; the theory is then framed in such a way as to lay out the means to be used in order to maximize the good (or, as occurs in pluralist versions of this approach, the goods). Hence, the value of any particular action, policy of action, or even of a law, is judged by the degree to which it has maximized the good.

Although the teleological approach in ethics has a long history and has yielded many versions, the most prominent current version, *utilitarianism,* was first expounded by Jeremy Bentham (b. 1748 – d.1832) in his work *Introduction to the Principles of Morals and Legislation*.[84] Bentham's original motivation in developing utilitarianism was largely legal. His project was to render the legal domain – and by a straightforward and natural extension, the moral domain – more rational and more humane. Bentham began with the assumption that pleasure is unquestionably good and pain is unquestionably bad.[85] The rightness or wrongness of a law, policy, or an act was then to be judged on whether it in fact had a tendency to maximize pleasure and/or minimize suffering. Bentham supposed that judgments of this kind could be straightforwardly calculated, taking the pleasure and pain of each person affected by said law, policy, or act to count equally in the calculation.[86] As critics were quick to point out, it is rather

[84] Edgar, Stacey L. Morality and Machines: Perspectives on Computer Ethics. Sudbury, Mass: Jones and Bartlett Publishers, 2002, p. 58 - 59
[85] Ibid. p. 58 – 59.
[86] Ibid, p. 58.

less straightforward than Bentham supposed to apply such a calculus, as the practical problems involved in providing an objective quantitative measure of subjective, qualitative sensations such as pleasure and pain were (and remain) insurmountable.

Nonetheless, the basic structure of utilitarianism survived Bentham with the ambitious notion of a calculus replaced with the more modest claim that the results of alternative courses of action could at least be compared. The directly "hedonistic"[87] tenor of Bentham's utilitarianism is also attenuated in the version of the theory advanced by the most renowned of his successors, John Stuart Mill (b. 1806 – d.1873). According to Mill,

> The creed which accepts as the foundation of morals, utility, or the greatest happiness principle, holds that all actions are right in proportion as they tend to promote happiness, wrong as they tend to produce the reverse of happiness. [88]

While Mill nominally accepts an identification of happiness with pleasure, in reality he seeks to enforce a qualitative distinction between "a beast's pleasures" and the "pleasures" associated with the employment of the "more elevated" human faculties. Whatever the merits of Mill's efforts at making such a distinction, the practical effect on his and subsequent versions of utilitarianism is that the project of calculating the good quantitatively has been largely sidelined[89] in favour of qualitative comparison.

---

87 Ibid, p. 59.

88 Mill, John Suart. Utilitarianism. Buffalo, N.Y.: Prometheus Books, 1987, *§2*.

89 It has been sidelined almost entirely in serious discussions of ethics outside economics, where the problem is conveniently surmounted by measuring value entirely in monetary terms.

Two notable features of the utilitarianism espoused by Bentham, Mill, and their successors are: first, the premium these theories place on prudential reasoning, on the way we think about the means we can employ to reach a desirable end; and secondly, a refusal to accord any moral principle absolute, unquestioning respect. The former feature of utilitarianism allows that whatever they may be, the most efficacious means of maximizing the good are legitimate. Disputes within utilitarianism tend to centre on alternative means; for example, whether a paternalist political order or a liberal one will better promote human happiness (Mill famously argued for liberty). Evidently, the kinds of arguments employed in order to settle such disputes must depend on a viable account of how the world, and especially the human part of it, works – hence the tendency of utilitarians to see their view as hard-headed, empirical, and above all, *practical*.

The second above-mentioned feature of utilitarianism also exhibits a certain hard-headedness. Any particular action, but more especially any claimant to the status of moral principle, must withstand scrutiny against the principle of utility. The claimant that cannot be justified in terms of its tendency to maximize happiness is to be summarily rejected, however longstanding the principle may be, or how deeply it may be entrenched in the common understanding of morality. In fact, even those principles otherwise endorsable in accordance with the principle of utility may be trumped by the advantages of a course of action that violates the principle, where the advantages of doing so outweigh the costs of such a violation. To think otherwise would not be consistent with the principle of utility, and would be, as one particularly hard-headed utilitarian puts it, "a form of superstitious rule-worship."[90]

[90] Smart, J. J. C. "Extreme and Restricted Utilitarianism." Theories of Ethics. Ed. Philippa Foot. Oxford: Oxford University Press, 1967, p. 180.

Teleological Theories: Communitariansim

Communitarianism is a term that has been applied to thinkers such as Michael Sandel, Michael Walzer, and Amitai Etzioni among others. The basic tenant of communitarian discourse is that there is an ethical importance to belonging to part of a community which matters in a way that has not been adequately captured by deontological theories, specifically those focused on social contract. The argument is that such contracts do not capture the full importance of the community, both in terms of tradition and cultural understanding.

In his work, Rights and the Common Good: The Communitarian Perspective, Amitai Etzioni, describes the communitarian agenda simply as being the rebuilding of communities. Specifically Etzioni focuses on two core communitarian issues: "the balance between individual rights and social responsibilities, and the roles of social institutions that foster moral values within communities."[91] Although the first of these agenda items could be easily taken up as part of a contract model – the second agenda item is a bit more complex because it looks to community values which might not always be compatible with a rights-based ethical model.

In his later work, How Patriotic is the Patriot Act, Etzioni distinguishes the type of communitarian branch that he is a proponent of, that being responsive communitarianism:

> A key tenet of responsive communitarianism is that a good society is based on a carefully crafted balance between liberty and social order, and a combination of particularistic (communal) and society wide values and bonds. This school stresses the responsibilities

[91] Etzioni, A. Rights and the Common Good: The Communitarian Perspective. New York: St. Martin's Press., 1995, p. iii.

> that people have to their families, kin, communities, and societies. These exist above and beyond the universal rights that all individuals command, which is a main focus of liberalism. [92]

This later refinement of his original communitarian position makes it clear that this theory, although perhaps mindful of human rights, is not a slave to them. For example, if the community values collective security over the individual rights of minorities, it would seem that a responsive communitarian model could collapse into a tyranny of the community in the same way that utilitarianism can collapse into a tyranny of the majority if sufficient checks are not built into the system. The reason for this is that both theories favour the good over the right as their starting point and so the definition of the ultimate good will have an impact on individual rights. Unless the ultimate good is seen as the protection of individual rights of minorities, it is hard to imagine that such a theory would protect these rights in times of emergency.

Deontology: Duty-based Ethics

Whereas teleological theories take as their starting point some conception of the good, the starting point for deontological theories in normative ethics is some conception of obligation. That is to say, the guiding conception for moral behavior is not maximization of the good, but rather respect for moral obligations. As it is sometimes put in deontological theories, right is prior to the good. Hence, the moral evaluation of any action or policy to act in a certain way depends not on the result of that course of action, but rather on the basis of that action in a motive to respect (or disrespect) one's moral obligation.

---

[92] Etzioni, A. How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism. New York: Routledge, 2004, p. 4.

The deontological approach also has a long and varied history, including for example, divine command accounts of moral obligation and accounts of moral obligation based in natural law. But in any account of duty-based ethics, the central figure should be Immanuel Kant (b. 1724 – d. 1804). Kant's theory exhibits the logic of the deontological approach clearly and uncompromisingly.

Against teleological approaches to morality Kant argues that nothing is unconditionally good except for a good will.[93] As Kant points out, even those ends that seem unquestionably good may, under certain circumstances, fall considerably short of deserving the title. For example, Bentham's end in itself – pleasure – is only perversely described as good when it is the pleasure that a sadist takes in inflicting suffering. By way of contrast, a good will is not the objective of an action or policy, but is rather a characteristic of human beings that is ordered in such a way as to respect the moral law.

Kant accepts just as much as any utilitarian that human actions each have an end and that it is the role of practical reasoning to choose the means to arrive at that end. As he puts it, practical reason yields hypothetical imperatives, counsels that reason gives itself regarding a policy to follow in order to achieve a given end – for example, if you want to be healthy, then eat right and exercise. However, given that no objective of an action can be absolutely and unquestionably good, and that the ends pursued by individuals can vary quite radically, hypothetical imperatives cannot be genuinely moral imperatives. Rather, practical reason should seek an imperative that is unconditional, that includes reference to no particular, subjective end – that is, a categorical

[93] Gregor, Mary, ed. Groundwork of the Metaphysics of Morals / Immanuel Kant. Cambridge: Cambridge University Press, 1998, p. 8.

imperative.

Kant claims that just such an imperative can be derived from the very notion of moral obligation; in fact, he manages to derive several formulations of what he maintains is one and the same principle. The best known formulation is:

> Act only in accordance with that maxim through which you can at the same time will that it become a universal law. [94]

However, the most intuitively clear formulation is:

> Act so that you treat humanity, both in your own person and in that of another, always as an end and never merely as a means.[95]

Note the reference to the "maxim" of an action in the first formulation: in Kant's view, for every action the will gives itself a rule (viz., maxim) and then behaves accordingly. This may be a hypothetical imperative where there is an objective to be achieved. But where the question of the rightness or wrongness of an action arises, the rule, or as it might be more colloquially put, the *motive* of that action is to be tested against the categorical imperative. As Kant sees it, the good will, the will that seeks to do right, gives itself a rule for testing motives. This rule for rules, the categorical imperative, is universal because it follows logically from the common concept of moral obligation that everyone pre-theoretically understands; it is binding as a rule the

[94] Gregor, Mary, ed. Groundwork of the Metaphysics of Morals / Immanuel Kant. Cambridge: Cambridge University Press, 1998, p. 31.
[95] Ibid, p. xxii.

rational mind imposes on itself, and it is absolute, in that no end, however apparently desirable, could justify violating it.

While there have been doubts from the beginning about the logical underpinnings of Kant's derivation of the categorical imperative, it is undeniable that his theory introduces and strongly emphasizes notions that remain central to our conception of morality today. For example, our fellow moral agents deserve respect just because they are, like us, moral agents; hence they must never be treated as mere means to achieving some objective of our own. And our dignity as moral agents depends on our autonomy – that is, the fact that we are self governing, that the laws we are governed by are the laws we give ourselves, including the categorical imperative.

The greatest source of discomfort for Kant's critics, however, is the absoluteness of his moral imperatives. There seems to be no room at all for consideration of consequences in his theory. In Kant's life time, Benjamin Constant took him to task for his absolute prohibition on lying, asking what one was to do if a murderous, axe wielding madman were to come knocking on one's door, asking after the neighbor one is hiding in the house. Constant's objection to Kantian absolutism remains a serious concern since a moral theory that entirely refuses to take consequences into account risks permitting, or perhaps even committing, monstrosities in the name of morality.[96]

[96] Benton, Robert J. "Political Expediency and Lying: Kant vs Benjamin Constant." Journal of the History of Ideas . 43.1 (Jan. - Mar., 1982), 135, p. 138.

Deontology: Contractarian Ethics

Rights-based ethics places an emphasis on actions that uphold an individual's human or legal rights. Rights can be broken down into positive and negative rights. Negative rights refer to freedom from outside interference. For example, the right to intellectual freedom, freedom of speech, liberty and privacy, are negative rights because they represent freedom from forces that would try to subvert those rights. Positive rights, on the other hand, represent rights that are necessary to the pursuit of freedom. The right to health care, education and the like are examples of such rights.

In its modern form, contractarianism is a rights-based approach to morality and ethics that takes into account these differing types of rights, both positive and negative, and the roles and responsibilities of citizens and governments to uphold and protect those rights. This relationship between citizens and their government takes the form of a social contract. The idea of a social contract is basically this:

> What makes some particular system of collectively enforced social arrangements legitimate is that it is the object of an agreement for the people who are subject to it.[97]

Here contractarianism is not intended as an account of the historical origins of current social arrangements, but rather a framework for answering questions about legitimacy and obligation.

Contractarianism refers to a type of morality that is based on the social contact between a

[97] D'Agostino, Fred. "Contemporary Approaches to the Social Contract." Stanford Encyclopedia of Philosophy. September 5 2008. <http://plato.stanford.edu.proxy.library.carleton.ca/entries/contractarianism-contemporary/>.

government and its citizens. In this arrangement citizens have given their consent to be ruled by a government, which is said to possess legitimate authority. But how was such consent obtained? Here we need to discuss the very idea of consent. In the context of government, John Locke argued that a government was legitimate only if its citizens had consented to it. Where it is obvious that not everyone has consented to the government under which they live, Locke proposed the idea of tacit consent, claiming that anyone who accepts the benefits of a government has tacitly consented to the burdens that government imposes on them. Thus, accepting the benefits of society imposes certain obligations on individuals. Locke is quite clear on this point stating in Two Treatises of Government that:

> [E]very man, that hath any Possession, or Enjoyment, of any part of the Dominions of any Government, doth thereby give his tacit Consent, and is as far forth obliged to Obedience to the laws of that government, during such enjoyment, as any one under it.[98]

Thus, if one receives benefits, one incurs obligations.

In A Theory of Justice, John Rawls makes an argument that is similar to Locke's. For Rawls the question is not simply whether or not one would consent to a government explicitly or tacitly, but whether or not the consent to this form of government would be from a fair, original position. The *original position of equality* is something that Rawls says corresponds to the state of nature in traditional social contract theory. This condition is not an actual historical condition, but a primitive condition of culture. In the original position, principles of justice are chosen behind a

[98] Locke : Political Essays. Ed. Mark Goldie. Cambridge: Cambridge University Press, 1997.

veil of ignorance, which "ensures that no one is advantaged or disadvantaged in the choice of principles."[99] Rawls demonstrates through the original position the importance of fairness in consent theory and this is an important addition to our modern understanding of social contract theory.

The restrictions that Rawls refers to as the "constraints of the concept of right"[100] are restrictions that he says hold true for all ethical principles and not just those of justice. According to Rawls' theory, an ethical principle must satisfy the following five requirements:

1. The principle should be general;
2. Principles are to be universal in application;
3. Parties assume that they are choosing principles for a public conception of that principle;
4. The conception of right must impose an ordering of conflicting claims;
5. The parties are to assess the system of principles as the final court of appeal in practical reasoning.[101]

Rawls'posits that:

> …[t]aken together, then, these conditions on conceptions of right come to this: a conception of right is a set of principles general in form and universal in application, that is to be publicly recognized as a final court of appeal for ordering conflicting claims of moral

[99] Rawls, John. A Theory of Justice. Cambridge, Mass: Belknap Press, 2005 reprint of 1971 edition, p. 130.
[100] Ibid, p. 135.
[101] Ibid, p. 135.

persons. [102]

Rawls' constraints of the concept of right provide us with a basis for the development of moral norms. Of note in his theory is the fact that the conception of right must impose an ordering of conflicting claims.[103] It is precisely this sort of problem that we see in Kant's moral imperative (the difficulty in dealing with competing claims), and in utilitarianism (the inherent desire to appeal to utility on a case by case basis).

One of the main concerns with Rawl's theory is whether or not it can be applied in practice. That is to say, how would one apply such a contract? How would it work among real people? There is much beauty in a contract that appeals to rational lexical application of the principles outlined above, but the problem seems to be that as a tool for civic engagement, it appears to be an unworkable thought experiment for the average citizen, let alone the average politician.

Developing an Ethical Framework

Policy development and constitutional interpretation are informed by ethical reasoning. Much of the discourse regarding post-September 11th legislative and administrative reforms, particularly the *Patriot Act*, the National Security Agency's Terrorist Surveillance Program (TSP), and the *Foreign Intelligence Surveillance Amendment Act of 2008 (FAA)*, have focused on the constitutionality of such reforms. This study considers the constitutional and ethical issues surrounding these reforms; however I wish to address a shortcoming common to most work on the subject, namely that these discussions begin and end with the U.S. Constitution. Although

[102] Ibid, p. 135.
[103] Ibid, p. 134.

there is much to be said for this document, it need not be the last word on these issues. Nor in reality is it, as evidenced by frequent disputes over its interpretation at even the highest levels of American public life. As previously stated, the U.S. Constitution can be viewed itself as meta-ethical in that it sets out rights which it claims are in themselves inalienable. To make such a claim would suggest that these rights themselves must exist prior to Constitution. The purpose of the Constitution then is really to spell out the rights, which are particularly vulnerable to infringement, in such a way to make them legally enforceable. The reason we can engage in an ethical discussion about constitutional principles is because these principles themselves emerge from a prior ethical framework. That said, this dissertation does not set out to construct a meta-ethical framework for the U.S. Constitution (although presumably such a framework would be influenced by philosophers like John Locke among others[104]). What it does set out to do is provide a normative framework that can be used in an applied sense to real world political and legal problems involving foreign intelligence surveillance in the U.S. My guiding thought throughout this study will be that if one is going to make political and legal decisions one should have some moral basis for doing so.

This chapter has sought to provide a brief introduction to some of the main ethical theories which have informed the ethical debate over legislative measures like the *Patriot Act*, and the subsequent changes to the *Foreign Intelligence Surveillance Act (FISA).* For the most part this chapter has emphasized the utilitarian arguments and the contractarian arguments since these are the ethical arguments which have largely informed this debate.

[104] John Locke's *Two Treatises of Government* is widely understood to be one of the most influential texts in shaping the language of the right to revolution in the *Declaration of Independence* as well as the inalienable rights in the *Constitution of the United States of American*.

Chapters 4 - 6 of this dissertation provide the basis for this applied study in information ethics. By examining the *Patriot Act*, the Terrorist Surveillance Program (TSP), and the recent amendments to the *Foreign Intelligence Surveillance Act (FISA)* through the various ethical lenses described above, the following chapters take into consideration the utilitarian teleology of the good (as informed by the tradition of Bentham and Mill) and the contractarian rights-based deontology (as informed by the tradition of Rawls) which have been most commonly used to interpret these changes in an ethical context. It is my argument that these traditional utilitarian and contractarian frameworks are insufficient for dealing with contemporary problems surrounding foreign intelligence surveillance. Rather than viewing these two ethical theories as competing or conflicting frameworks, Chapter 7 seeks to blend these two normative theories so that they might best be applied in a practical sense to the contemporary problems of foreign intelligence surveillance in the U.S.

PART III:

CIVIL LIBERTIES IN INSECURE TIMES:

CASE STUDIES IN APPLIED ETHICS

Chapter 4.

U.S.A. PATRIOT Act: A Necessary Tool in the War on Terror?

Backgrounder: *The U.S.A. PATRIOT Act of 2001*

The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act* (*U.S.A. PATRIOT Act* or *Patriot Act* for short)[105] was the legislative response to September 11, 2001.[106] The first of the Act's objectives, as described by Banks, was the improvement of information sharing. Shortly after September 11th, both the U.S. Congress and Administration saw the lack of shared information as a one of the major failures in being able to prevent the September 11th attacks. The difficulties in accessing key information within the intelligence community meant that pertinent information, which was available shortly before the attacks, was not shared between the various agencies that had national security responsibility.[107] The terrorist attacks acted as an impetus for cooperation between law enforcement and intelligence agencies, as is reflected in the *Patriot Act*. According to the Department of Justice (DOJ), shortly after the passage of the *Patriot Act*, the Act had worked to increase the ability of law enforcement to share information in the following ways:

1. it establishe[d] secure information-sharing systems to enhance the ability of agencies to investigate or prosecute multi-jurisdiction terrorist activities;

---

[105] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT) Act of 2001. Public Law 107-56.

[106] See Appendix A of this dissertation on page 181 of this dissertation for a legislative summary of this Act.

[107] Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004, p. 30.

2. and it allow[ed] law-enforcement personnel to share grand-jury and wiretap information regarding foreign intelligence with various other federal officers without first obtaining a court order: facilitating the sharing of information from criminal investigations.[108]

In order to streamline bureaucratic reaction time, many of the judicial controls were removed by the *Patriot Act*. The idea was that a reduction in legal barriers would enhance the Federal Government's "potential to monitor, track, and capture messages exchanged between hostile forces in the United States and elsewhere."[109]

The second objective of the Act, which called for the use of flexible warrants under *FISA*, provided the Government with an increase in surveillance opportunities from which to gather anti-terrorism intelligence. These flexible warrants could be obtained through the Foreign Intelligence Surveillance Court (FISC), as mandated by *FISA.* Under a *FISA* warrant, government agents have the ability to surveil targets if there is probable cause that the subject of the search is a foreign power or agent of a foreign power. As such, FISA warrants are contrary to the regular court system which requires that there must be probable cause that a crime has been committed before a warrant will be issued. Federal law enforcement agencies under *FISA* could collect personal information from electronic communications, voice mail, and any physical or electronic record, the term 'record' having now been expanded by the *Patriot Act* to include "any

[108] "Department of Justice: Fact Sheet overview of information sharing initiative in the war on terrorism." Federation of American Scientists. 2002. <http://www.fas.org/irp/agency/doj/fs091902.html>.

[109] Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004, p. 35.

tangible item that contains information".[110] With such an all encompassing definition, the worry by many was that *FISA* warrants could easily be used to conduct "fishing expeditions".

Section 215 and Section 505 of the *Patriot Act*, among the most controversial provisions, were the focus of several important legal challenges. Under Section 215 of the Act, the FBI could obtain a Section 215 order (*FISA* warrant) which allowed it to gain unprecedented access to certain business records held by a third party (i.e. medical, library, internet and other private records) without a subpoena or a warrant based on probable cause. [111] A gag order in the law prevented anyone served with a Section 215 order (i.e. an Internet Service Provider, medical professional, librarian) from telling anyone else that the FBI demanded information. Equally controversial, Section 505 of the Act allowed the FBI to use National Security Letters (NSLs) to request telephone toll and transactional records. Like a Section 215 order, NSLs were also subject to non-disclosure provisions that prevented a recipient from disclosing to anyone that they had been served with an NSL. In order to issue an NSL the FBI needed only to "certify - without court review - that the records [were] "relevant" to an intelligence or terrorism investigation."[112] In response to these provisions, several lawsuits were launched against the Government. In particular, the case of *Doe v. Ashcroft* garnered a great deal of attention with regards to the constitutionality of NSLs. This case will be discussed later in the chapter on page 84.

---

[110] Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99, p. 104.

[111] American Civil Liberties Union. "ACLU Blasts Justice Department's Attempts to Manipulate Truth About PATRIOT Act Ruling." October 1, 2004. <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16631&c=282>.

[112] Ibid.

The third objective of the *Patriot Act*, the expansion of wiretap authority over electronic communication, was met through amendments to *FISA* which allow for the use of roving wiretaps (which have unlimited jurisdiction), pen registers, and trap and trace devices without probable cause of a crime having been committed. The Government, in such instances, needed only to certify that the information that was likely to be obtained through the use of the device was:

> foreign intelligence information concerning a U.S. person or [was] relevant to an ongoing investigation to protect against international terrorism or clandestine activities, provided that such an investigation of a U.S. person [was] not conducted solely upon the basis of activities protected by the First Amendment of the Constitution.[113]

That said, the trap and trace provision under Section 214 of the Act expanded an exception to the Fourth Amendment (which protects against unreasonable searches and seizures), in order to "collect 'addressing' information about the origin and destination of communications, as opposed to the content."[114]

The fourth objective, the seizing of funds utilized by terrorist activities, signaled the recognition by the Government of the overall influence that money played in the material operation of terrorism. The *Patriot Act* bolstered Federal efforts to combat money laundering through regulations, international cooperation, criminal sanctions, and forfeiture, through the use of more

---

[113] USA PATRIOT Act, Pub. L. No. 107-56, § 214(a)(1), 115 Stat. 272, 286 (amending 50 U.S.C. § 1842(a)(1) (2000)).

[114] American Civil Liberties Union. "Surveillance Under the USA PATRIOT Act." April 3, 2003. <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206>.

stringent record keeping, disclosure and information sharing requirements, and the imposition of new crimes and penalties. Prior to the *Patriot Act*, financial institutions were required to file a variety of reports detailing the particulars behind transactions exceeding certain amounts with the Department of the Treasury and the Internal Revenue Service (IRS), and to establish anti-money laundering programs. The *Patriot Act* thus expanded reporting and disclosure of information, previously limited to the Treasury Department or the IRS, to all relevant actors involved in national security and foreign intelligence.

In addition, the President now had the power to designate any organization or individual a terrorist and thereby freeze all their assets and criminalize all transactions with them. It was this power that the President used to shut down three of the largest Muslim charities in the country. The assets of two Chicago-based Muslim charities, the Global Relief Foundation and Benevolence International Foundation, were frozen pending a government investigation of their potential terrorist links. The third, the Holy Land Foundation, was designated a terrorist organization on the charge that it was connected to Hamas. According to David Cole, this charity "was given no notice or hearing prior to its designation, and when it filed suit after the fact, the district court denied it any opportunity to produce evidence supporting its innocence."[115]

The fifth and final objective of the *Patriot Act* called for mandatory detention and deportation of non-U.S. citizens suspected of having links to terrorist organizations. Here Section 412 of the Act allowed the Attorney General to detain any non-citizen suspected of terrorism for up to seven days. Under Section 412, the Attorney General had to certify that he had reasonable

[115] Cole, David. "Enemy Aliens and American Freedoms." September 5, 2005. <http://www.thenation.com/doc/20020923/cole>.

grounds to believe that the suspect was either engaged in "conduct [that] threatens the national security of the United States or [was] inadmissible or deportable on grounds of terrorism, espionage, sabotage, or sedition."[116] Within that seven day period the Attorney General had to initiate removal, criminal proceedings or release the alien. In the event that the suspect was held, the determination had to be "reexamined every six months to confirm that the alien's release would threaten national security or endanger some individual or the general public."[117]
By advancing the argument that non-citizens are not entitled to the same rights (due process, equal protection and the freedoms of speech and association) as citizens in the war on terror, by extension one could argue that citizens should be allowed to trade the liberties of non-citizens for additional security.[118] This is a very difficult position to defend as a constitutional matter, given that basic rights are not limited to citizens but apply to all "persons" within the U.S. or subject to U.S. authority. "These are human rights, not privileges of citizenship."[119]

Here I think the following statement by Human Rights Watch captures nicely why Section 412 is such a controversial provision in the *Patriot Act*:

> A fundamental corollary of the right to liberty is the right not to be held without charge. Article 9 of the International Covenant on Civil and Political Rights states, "anyone who is arrested shall be informed, at the time of the arrest, of the reasons for his arrest and shall be promptly informed of any charges against him." U.S. constitutional law similarly

---

116 Congressional Research Service. "CRS Report for Congress: The USA PATRIOT Act: A Legal Analysis." CRS Report for Congress. April 2002. <http://www.fas.org/irp/crs/RL31377.pdf>.
117 Ibid.
118 Cole, David. "Enemy Aliens and American Freedoms." September 5, 2005. <http://www.thenation.com/doc/20020923/cole>.
119 Ibid.

> recognizes that detention without charge violates the right to liberty protected by the due process clause of the fifth and fourteenth amendments.[120]

In liberal democratic societies, there is a need to talk not only of individual rights, but also of the common good. In the U.S. the discussion of rights and responsibilities is becoming largely a discussion about the balancing of individual rights to such things as access to information and the right to privacy, against the collective good, national security.

Patriot Act Reauthorizations

One of the features of the several provisions of the *Patriot Act* was the use of built in sunset clauses. Given the controversial nature of these provisions, the insertion of a four-year sunset clause was viewed as a compromise to ensure the Act's passage. With the most controversial sections of the original *Patriot Act*, Section 215 among them, set to expire on December 31, 2005, the Administration needed to persuade Congress that the Act could be amended in such a way that it would live up to its claim that it not only made America safer, but was indeed constitutional.

Section 215, by broadening the term "record" to include "all tangible things", was heavily criticized for being overbroad. Claims that this provision of the *Patriot Act* was being abused were vehemently denied by the Administration. In an online Op Ed. Piece for the Washington Post on December 14, 2005, Attorney General Alberto Gonzales (John Ashcroft's successor in February 2005), answered public questions regarding the *Patriot Act*. Gonzales wrote in his

[120] Human Rights Watch. "Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees." United States Report 14.4 (G). August 2002. <http://www.hrw.org/reports/2002/us911/USA0802.pdf>.

response to questions from the public about the great deal of misinformation about the *Patriot Act*, stating in one real time response:

> The *Patriot Act* incorporates important safeguards, including judicial review, congressional oversight, and audits by the Inspector General. You mention wiretaps. All wiretaps must be authorized by a federal judge. In addition, investigators must show probable cause and comply with other requirements before the court may authorize the wiretap. This has always been the case, and the *Patriot Act* did nothing to diminish these safeguards.[121]

These comments would soon prove false in the windstorm that followed only a couple of days later with the December 16, 2005 revelation in the New York Times that the FISC was in many instances being by-passed entirely through a program of warrantless surveillance which had been in operation under a secret presidential order signed in 2002.[122]

Despite all of the bad press, the Administration was able to get the necessary extensions to amend the legislation, sections 215 and 505 in particular. The *U.S.A. PATRIOT Improvement and Reauthorization Act of 2005(Patriot Reauthorization Act)* was finally approved in the Senate on March 2, 2006 and in the House on March 7, 2006.[123] Although the reauthorized section 215 now required agents to present the FISC with data "proving how the evidence sought will apply

---

[121] Online Transcript. "Gonzales Discusses Patriot Act: U.S. Attorney General Wrote Op-Ed in Today's Post." December 14, 2005. <http://www.washingtonpost.com/wp-dyn/content/discussion/2005/12/13/DI2005121301425.html>.

[122] Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." December 16, 2005. <http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089>.

[123] See Appendix B of this dissertation on page 183 of this dissertation for a legislative summary of this Act.

to the relevant investigation and affords greater protections for library, medical, and educational records,"[124] it did little to address the problem of warrantless surveillance. Indeed the Bush Administration further attempted to legitimize the NSA program through its use of wartime presidential power arguments. To provide additional legitimacy, the program was brought under the purview of the *FISA* law through the passage of the *Protect America Act of 2007 (PAA).*[125] This new law which was passed August 5, 2007 permitted "intelligence professionals to more effectively collect foreign intelligence information on targets in foreign lands, without first receiving court approval." [126] In addition, it protected third parties who provided information to the Government, such as internet service providers or telephone companies, from being subject to private lawsuits.[127] Given the class action suits which were filed against such companies alleging their participation in the NSA program, the six-month sunset attached to this act was not sufficient to quash those suits, but it did make it possible for the legislation to be amended and reinstituted – which is what happened with the passage of the *FISA Amendment Act of 2008 (FAA).*[128]

Like section 215, section 505, which provides for the expanded use of NSLs, has been criticized as being a tool with the potential for gross abuse. In the key case on the subject, *Doe v. Ashcroft,*[129] an unnamed Internet Service Provider (ISP) and the American Civil Liberties Union challenged the constitutionality of Section 505 of the *Patriot Act* which allows for the use of

---

124 Belt, Dave. "Domestic security: The homefront and the war on terror for." The NewsHour (PBS). March 27, 2006. <http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/patriotact.html>.

125 Protect America Act of 2007 Public Law No: 110-55

126 "Fact Sheet : The Protect America Act." White House. August 7, 2007. <http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html>.

127 See Appendix C of this dissertation on page 185 of this dissertation for a legislative summary of this Act.

128 See Appendix D of this dissertation on page 193 of this dissertation for a legislative summary of this Act.

129 Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

NSLs.[130] On September 28, 2004 the United States District Court, Southern District of New York, ruled that the provision granting the use of NSLs was unconstitutional. Judge Victor Marrero struck down the section on the grounds that it violated "free speech rights under the First Amendment as well as the right to be free from unreasonable searches under the *Fourth Amendment*."[131] The Government appealed this decision only to have the appeal declared moot and the case returned to the original district court for reconsideration in light of the recent revisions to the *Patriot Act*.[132] For a second time Marrero struck down the controversial NSL provision on September 6, 2007[133] declaring it unconstitutional despite so called assurances that the new legislation had corrected the lack of congressional oversight in the original.[134] As with his previous ruling, Justice Marrero stayed the ruling for ninety days pending government appeal. The Government did follow up with another appeal, but by the time of the next appeal they had withdrawn their original NSL from the ISP in question. As the NSL had been withdrawn, the only issue at hand was whether or not the ISP was still bound by the prohibition on disclosing receipt of the NSL.

Under the *Patriot Reauthorization Act* the non-disclosure obligations on NSL recipients were modified.[135] NSL recipients were still bound by non-disclosure obligations in cases where the

---

[130] Due to improper redacting of Court documents, the media first deduced that the ISP consisted of four librarians of the Library Connection, a consortium of libraries in Connecticut. Although the librarians were part of the suit, the original ISP, Calyx Internet Access, remained bound by a partial gag order and was not identified until August of 2010 when U.S. District Judge Victor Marrero partially removed the gag order on its President, Nicolas Merrill. See: Zetter, Kim. "'John Doe' Who Fought FBI Spying Freed From Gag Order After 6 Years" in Wired. August 10, 2010. <http://www.wired.com/threatlevel/2010/08/nsl-gag-order-lifted/#ixzz0wcPM40Dg >.

[131] American Civil Liberties Union "In ACLU Case, Federal Court Strikes Down PATRIOT Act Surveillance Power As Unconstitutional." September 29, 2004. <http://www.aclu.org/safefree/spying/18589prs20040929.html>.

[132] Patriot Act Reauthorization had just been passed when this decision was rendered.

[133] Doe v. Gonzales 500 F. Supp. 2d 379 (2007).

[134] Eggen, Dan. "Judge Invalidates PATRIOT Act Provisions: FBI Is Told to Halt Warrantless Tactic." The Washington Post. September 7, 2006. <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601438.html>.

[135] Department of Justice. Office of the Inspector General. Special Report. A Review of the Federal Bureau of

FBI Director or his designee had certified that harm might arise in an investigation if a disclosure occurred. Section 116 of the *Patriot Reauthorization Act* amended Section 505 *Patriot Act* to allow recipients of NSLs to obtain legal advice from an attorney[136] (something which they had not been able to do under the original provision) on the condition that they inform the FBI Director or his designee of the disclosure, and reveal the identities of the individuals to whom they disclosed the existence of the NSL.[137]

On December 15, 2008 the U.S. Court of Appeals (Second Circuit) decision[138] upheld the Marrero's decision, in part finding that "portions of the statute violated the First Amendment; specifically the sections that wrongly placed the burden on NSL recipients to challenge gag orders."[139] In addition, the Court was concerned about the absence of any time limits placed upon the gag order (as it stood the gag orders were indefinite), as well as the absence of any judicial review requiring the Government to demonstrate the burden of proof for maintaining the gag order. These concerns lead to the case being sent back to the U.S. District Court for the Southern District of New York, forcing the Government to justify the constitutionality of the gag order imposed.[140]

The *Patriot Reauthorization Act* now requires the Inspector General of the Department of Justice

---

Investigation's Use of National Security Letters (Unclassified). (March 2007) <http://www.justice.gov/oig/special/s0803b/final.pdf>, p. 118.

136 Ibid.

137 Ibid.

138 Doe v. Mukasey, 2008 U.S. App. LEXIS 25193 (2d Cir. N.Y., Dec. 15, 2008)

139 American Civil Liberties Union. "ACLU: National Security Letters." <http://www.aclu.org/safefree/nationalsecurityletters/index.html>.

140 Zetter, Kim. "'John Doe' Who Fought FBI Spying Freed From Gag Order After 6 Years" in Wired. August 10, 2010. <http://www.wired.com/threatlevel/2010/08/nsl-gag-order-lifted/#ixzz0wcPM40Dg >.

to review and report on the FBI's use of NSLs.[141] The Inspector General's 2007 report found that the FBI, which issued almost 200,000 NSLs between 2003 and 2006, had in many instances, abused its authority and misused NSLs.[142]

Ethical Concerns

> Those who criticize the Patriot Act must listen to those folks on the front line of defending America. The Patriot Act defends our liberty, is what it does, under the Constitution of the United States. (Applause).[143]
>
> -President George W. Bush

> …the essential act of the Party is to use conscious deception while retaining the firmness of purpose that goes with complete honesty.[144]
>
> -George Orwell, *Nineteen Eighty-four*

Defenders of the original *Patriot Act* (before its sunset provisions were reauthorized) used utilitarian arguments to frame the debate concerning individual rights and the collective good (national security). Limitations to individual liberties, so the argument went, were justified if they served to protect the ultimate collective greater good, that being national security. Through use of Mill's *liberty principle*, these defenders cited the "prevention of harm" as the *prima facie*

---

141 Congressional Research Service. "National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments" CRS Report for Congress. September 8, 2009. <http://www.fas.org/sgp/crs/intel/RS22406.pdf>.

142 Ibid.

143 Office of the Press Secretary. "President Bush: Information Sharing, PATRIOT Act Vital to Homeland Security." Remarks by the President in a Conversation on the USA Patriot Act, Kleinshans Music Hall, Buffalo, New York." April 20, 2004. <http://www.whitehouse.gov/news/releases/2004/04/20040420-2.html>.

144 Orwell, George. Nineteen Eighty-Four. New York: Harcourt, 1949, p. 215.

justification for the Act. Mill's principle states:

> … the sole end for which mankind are warranted, individually or collectively, in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others… [145]

The pro-*Patriot Act* response seemed to be that the only way to ensure the security of the majority was to curtail the freedom of some, or perhaps even all of the members of the community. That said, it was also possible to use the liberty principle against the Act, using a form of proportionality test. For example, if the outcomes of the Act resulted in (a) an excessive curtailment of liberty, relative to the threat it responded to, or (b) the curtailments of freedom involved in the Act were ineffective in protecting the community from genuine danger, one could use Mill's liberty principle to argue that the harms of the Act outweighed the (potential) benefits.

The utilitarian case, pro or con the original *Patriot Act*, was bound to be a frustrating exercise for the outsider, given the nature of the Act itself. With such a tight lid being kept on information about any actions taken under the Act, indeed, in *accordance* with the Act, it was almost impossible to make an informed judgment one way or another on these issues. Of course, the secrecy provisions of the Act were justified by its defenders as essential to its effectiveness. Not that this moved insiders to excessive scruples over appealing to "secret information" about

[145] Mill, John Suart. On Liberty. Ed. Alan S. Kahan. Boston: St. Martins, 2008.

terrorist threats interdicted, which unfortunately could not be shared, in defense of the Act and its provisions. Those opposed to the Act might have suspected that it was doing more harm than good, but they were prevented by the Act itself from putting together the evidence that this was so.

The case of the original Act demonstrated two problems with the utilitarian grounding of justice, the first a matter of principle, the other a matter of practice. The first problem is the often raised point that rights and freedoms are merely provisional if justified by utilitarian arguments. The ultimate utilitarian test for any policy is its effectiveness, whether or not the policy produces the greatest happiness of the greatest number. Mill's liberty principle was framed in response to the threat to freedom of thought and action posed by the state, and especially social paternalism. The argument of *On Liberty* is that, in the long run, freedom of thought and action are conducive to the greatest happiness of the greatest number. Implicit in the original Act, however, is the opposing view that freedom of thought, at least of some kinds, is not conducive to the greatest happiness of the greatest number. The issue between Mill and those who took this latter view was ultimately an empirical matter, to be tested by experience. For the consequentialist, there was no obstacle in principle to those who took this latter view.

This leads to the second problem, which is a particularly acute example of the epistemological problems with consequentialism. For the consequentialist, the rightness or wrongness of every action and every policy is judged on the basis of the contribution it makes to the general welfare. But every action and every policy is undertaken with limited knowledge of the consequences that will ensue. The world is a complicated place, and we are limited beings; however well-armed

with knowledge we may be, we cannot foretell with very great assurance what the outcome of any course of action we undertake might be. The secrecy involved in the case of the *Patriot Act* only exacerbates the epistemological problems already inherent in forming a judgment as to the potential effectiveness of any given policy. Using consequentialist arguments to defend the actions and policies of the Government becomes rather difficult, and our abilities to predict the long term consequences of legislation such as the *Patriot Act* falls more than a little short of perfection. Where relevant information, necessary for any serious analysis of the Act's consequences, potential or actual, is deliberately restricted, the problem is compounded.

The only really secure consequentialist judgments of the *Patriot Act* would have to be retrospective, made only when all the information becomes available. This is not to say that, as policy, the provisions of the *Patriot Act* were not justified from a utilitarian point of view. As the Act was framed, that was something for insiders to know, and the expectation was that citizens would simply have to accept their judgment on this matter. As a result, the *Patriot Act* presented an unsightly combination of a paternalism Mill would have deplored, founded in the very consequentialism he promulgated. Looking back at the remarks made in 2001 in defense of the original Act, by then Attorney General John Ashcroft, the term paternalism seems a fitting word, since there was no room left to even question the Act:

> To those who scare peace-loving people with phantoms of lost liberty, my message is this: your tactics only aid terrorists, for they erode our national unity and diminish our

resolve. They give ammunition to America's enemies, and pause to America's friends.

- John Ashcroft[146]

With the patriotism of those who questioned the Act's most controversial provisions being maligned, attempts to engage in any meaningful debate on the subject proved difficult. The most effective arguments against the *Patriot Act* were those based on a differently conceived conception of the foundations of rights and liberty. These arguments conceived the rights protected under the U.S. Constitution as human rights -- rights that were not beholden to the standard of utility. In contrast to utilitarianism, with its focus on the greater good, these contractarian arguments provided a means for examining a right-based critique of the Act. Even so, the contractarian approach was not so simple. Despite attempts to discredit those concerned about the impact that the legislation would have on civil liberties, in the manner of John Ashcroft above, a true social contract discussion would have to involve some discussion of rights and corresponding obligations (John Locke). It was not that Contractarians saw the rights infringed as necessarily absolute and uncompromising (although that was often the way they were portrayed in the debate), but rather that even for a Contractarian any attempt to establish some sort of ordering of competing rights claims in the 'liberty versus security' debate was equally frustrated by the lack of information needed in order to properly assess the true impact on the rights infringed. If the *Patriot Act* provided measurable benefits to security which outweighed any adverse effects on liberty, then there would be a reasonable expectation that the law was justifiable. Again though, given the veil of secrecy surrounding the Act, it was simply not possible to assess the actual trade-offs involved for the most controversial provisions.

[146] John Ashcroft: Testimony before the Senate Judiciary Committee, December 6, 2001. <http://www.justice.gov/archive/ag/testimony/2001/1206transcriptsenatejudiciarycommittee.htm>.

The fact that the very operation of the original *Patriot Act* depended on a high level of secret information outside of the normal checks and balances – made the act, I would argue, one of the most controversial pieces of legislation in American history. In its original state, the *Patriot Act* possessed no clear judicial oversight, and due to its nature, no public accountability (since that would have required public access to the information needed in order to question the effectiveness of the law under which it was governed – which it did not). This secrecy made it difficult to properly assess the Act from either a utilitarian or contractarian stance. These concerns led to considerable discussion in the U.S. regarding whether or not the Act's sunset provisions should be allowed to expire, or if saved somehow reformed to increase both judicial oversight and public accountability.

Despite the many legal setbacks facing the Bush Administration regarding reauthorization, the Administration was steadfast in its defence of the *Patriot Act* and its other Anti-terrorist measures. This defence was palpably utilitarian. Given the importance of the objective – protecting the U.S. against terrorism - the means necessary to achieve it were claimed to be legitimate. Seen in this light the Bush Administration's tendency to treat the Constitution as an impediment, rather than a genuine guide to action, becomes more comprehensible. However, there are multiple possible ways to dispute the Bush Administration's rationale on ethical grounds. For example a utilitarian might argue that the Administration had not chosen the optimal means to achieve its ends. Deeper criticism might proceed from the failure to respect the autonomy of U.S. citizens by that Administration. In the chapters that follow these issues will be explored in more depth with an aim of tying together a consistent ethical approach to dealing with such issues.

Chapter 5.

Warrantless Surveillance: An Extension of War Time Powers?

Backgrounder: The Terrorist Surveillance Program

James Risen and Eric Lichtblau broke the news of the National Security Agency (NSA)'s warrantless surveillance program on December 16th 2005 in the New York Times.[147] The program, which was later called the Terrorist Surveillance Program (TSP) by the Administration, allowed NSA to intercept "communications between individuals on American soil and individuals abroad, without judicial approval."[148] The 'program' was authorized by President Bush in October of 2001, through use of a secret presidential order, but would not become publicly known for another four years.

As Eric Lichtblau recounts in his book, Bush's Law: The Remaking of American Justice, the decision for the New York Times to go public with the news, was one the paper struggled with. The New York Times delayed publication for more than a year after intense lobbying by the White House on the grounds that publication of the story would jeopardize national security. Despite having a draft of the story in hand in 2004, the paper went to the Administration and heard out the White House's objections to its publication. According to Licthblau in an interview with *Democracy Now*, the fact that they were debating this before the election was a

147 Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." December 16, 2005. <http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089>.

148 Wong, Katherine. "The NSA Terrorist Surveillance Program." Harvard Journal of Law & Public Policy 43 (2006): 517.

"matter of happenstance."[149] Although the publication continued to be delayed, it was clear to the reporters involved that there were fierce anxieties about the legality of the program amongst a select few persons who were 'read into' or briefed about the program.

Immediately after the election, the paper continued to withhold publication of the story, but as time passed, it became clearer to the investigative reporters and their editors that many of the assertions made by the White House in defense of the continued secrecy surrounding the program were simply untrue. The legal safeguards which they had been assured were in place, and the insistence that there was no difference of opinion within the Department of Justice (DOJ) regarding the legality of the program by White House officials, became increasingly suspect. In particular, the repeated insistence by Attorney General Alberto Gonzales that there were no legal concerns about the program within the Administration and the DOJ were ultimately debunked by Lichtblau and Risen's investigation into the program.

Despite the White House's continued attempts to convince the paper to back off on publishing the story, it became clear that the story simply was not going to die. News of the secret program was likely to emerge in the book that Risen was working on, and the New York Times knew it. At this point it seemed really a matter of how and when the story would break. The paper received a tip that the Administration was considering using a legal court injunction to stop the paper from publishing, as had been the case with the Pentagon Papers in 1971 (a historical case of censorship where the Nixon Administration tried unsuccessfully to block the paper from

[149] Democracy Now. "Exclusive: Bush's Law: Eric Lichtblau on Exposing the NSA's Warrantless Wiretapping Program and How the White House Pressured the New York Times to Kill the Story." <http://www.democracynow.org/2008/4/1/exclusivebushs_law_eric_lichtblau_on_exposing>.

publishing the secret history of the Vietnam War).[150] With the threat of a possible injunction looming, the New York Times made the decision to post the story online before such an injunction could stop it.

As the time approached for the reauthorization of the *Patriot Act's* sunset provisions, the story was a bombshell and certainly generated widespread debate in Congress. The Administration went into immediate damage control mode, trying to contain and explain the new revelations about the super secret program. The following day President Bush, in his weekly radio address, admitted that he had authorized the program but contended that NSA's actions were "consistent with U.S. law and the Constitution," and that the surveillance was intended only "to intercept the international communications of people with known links to Al Qaeda and related terrorist organizations."[151]

Rather than responding immediately to the new revelations about warrantless surveillance in his radio address, Bush used the opportunity to first stress the need for the Senate to reauthorize the soon to expire sunset provisions of the *Patriot Act* – emphasizing that America's law enforcement personnel had used this:

> …critical law to prosecute terrorist operatives and supporters and to break up terrorist cells in New York, Oregon, Virginia, California, Texas, and Ohio.[152]

---

150 Lichtblau, Eric. Bush's Law: The Remaking of American Justice . New York: Pantheon, 2008, p. 194.

151 New York Times. "Bush on the Patriot Act and Eavesdropping" (Transcript of Weekly Radio Address). December 18, 2005. <http://query.nytimes.com/gst/fullpage.html?res=9A05E6D61630F93BA25751C1A9639C8B63>.

152 Government Printing Office. "The President's Radio Address." December 17, 2005. <http://fdsys.gpo.gov/fdsys/pkg/WCPD-2005-12-26/html/WCPD-2005-12-26-Pg1880.htm>.

He began his address by focusing on the *Patriot Act.* This was legislation passed in a time of crisis with almost unanimous consent – passing by a ninety-eight to one bipartisan majority in the Senate. In doing so, he was able to seize the opportunity to chastise those Senators who were currently filibustering over reauthorization as undermining the safety of the country, since the U.S. could "not afford to be without this law for a single moment." [153]

By placing the emphasis on the *Patriot Act*, President Bush was attempting to mitigate rising concerns in the media over the program of warrantless surveillance operating under his authorization. His speech writers clearly sought to shape his remarks in such a way as to make any covert actions seem completely understandable, if not excusable. Appealing to the authority vested in him by the Congress through the *Joint Authorization for Use of Military Force (AUMF)*, in combination with his powers as Commander in Chief, President Bush was asserting a claim (one that he would continue to stand by for the rest of his presidency) that he had acted within the bounds of the Constitution and the law. President Bush summed up his address with a short reference to the breaking controversy, stating simply that he had:

> …authorized the National Security Agency, consistent with U.S. law and the Constitution, to intercept the international communications of people with known links to al Qaeda and related terrorist organizations. [154]

The claim that 'only persons with known links to Al Qaeda' were the targets of such surveillance is one that was widely contested in the press. What is known is that shortly after 9/11 the

[153] Ibid.
[154] Ibid.

President ordered the NSA to secretly wiretap the "international telephone calls and email messages of Americans without obtaining warrants."[155] This secret wiretapping was made possible through a public-private partnership between the NSA and various telecommunications companies – the source of the data.

As for the nature of the program, that was "highly classified." The purpose however, was not inconsistent with other post 9/11 initiatives, in that its main objective was to detect and prevent terrorist attacks against the U.S. The media, according to the President, had now endangered Americans by leaking the existence of this program. The possible chilling effect on free speech was also clear as President Bush stated flatly that:

> As a result, our enemies have learned information they should not have, and the unauthorized disclosure of this effort damages our national security and puts our citizens at risk. Revealing classified information is illegal, alerts our enemies, and endangers our country.[156]

Pointing to the example of the two terrorist hijackers who flew a jet into the Pentagon, Nawaf al Hamzi and Khalid al Mihdhar, President Bush noted that had their communications to members of Al Qaida overseas been intercepted, that tragedy might have been avoided. By authorizing the secret NSA program, President Bush claimed his actions were fully consistent with his

---

[155] Huhn, Wilson R. "Congress has the Power to Enforce the Bill of Rights Against the Federal Government; therefore FISA is Constitutional and the President's Terrorist Surveillance Program is Illegal." William & Mary Bill of Rights Journal 16 (2007): 537.

[156] Government Printing Office. "The President's Radio Address." December 17, 2005. <http://fdsys.gpo.gov/fdsys/pkg/WCPD-2005-12-26/html/WCPD-2005-12-26-Pg1880.htm>.

"constitutional responsibilities and authorities," [157] and would increase the likelihood that "killers" such as those involved in the 9/11 hijackings would be identified and located in time. [158] President Bush went even further in his defense of the program by stating that since its authorization, the program had helped to both detect and prevent possible terrorist attacks at home and abroad. [159]

In terms of oversight, the President was quick to point out that he had been reviewing the program's activities approximately every 45 days in consultation with the DOJ, and top legal officials within NSA, including the Attorney General and the Counsel to the President, as well as "leaders in Congress" who had apparently been briefed more than a dozen times. [160] It would later be revealed that the leaders the President referred to were the "gang of eight" a subset of the leaders within Congress which included the speakers and the minority leaders from both the House and the Senate and the chairs and ranking members of the House and Senate intelligence committees – which itself was controversial because the full membership of the intelligence committees had not been briefed on the program. [161] As a result of these consultations, the President announced in his address that he had thus far reauthorized the program more than 30 times since the September the 11th attacks, and would continue to do so as long as the country faced threats from Al Qaeda and other terrorist groups,

> This authorization is a vital tool in our war against the terrorists. It is critical to saving American lives. The American people expect me to do everything in my power under our

157 Ibid.
158 Ibid.
159 Ibid.
160 Ibid.
161 Lichtblau, Eric. Bush's Law: The Remaking of American Justice . New York: Pantheon, 2008, p. 168.

> laws and Constitution to protect them and their civil liberties. And that is exactly what I will continue to do, so long as I'm the President of the United States. [162]

Presidential Power and the TSP

The Bush Administration's position on the matter was clear – that the President had acted within his authority in authorizing the Terrorist Surveillance Program. At the start of February 2006 the Senate Judiciary Committee began its hearings.[163] The committee's chairman, Senator Arlen Specter, opened them by stating that his committee would be:

> …examining the Administration's contention that, notwithstanding the *Foreign Intelligence Surveillance Act*, there is statutory authority for what the president has done by virtue of the resolution of Congress authorizing the use of force against the terrorists.[164]

In reference to the President's assertion that he was acting in accordance with the powers given to him in the emergency resolution passed by Congress shortly after 9/11, not all lawmakers shared the President's position on the matter. As Senator Leahy commented, Democrats and Republicans did not give the President the authority to "go around the *FISA* law to wiretap Americans illegally." Rather, the authorization in question, according to Leahy, was simply the

---

[162] Government Printing Office. "The President's Radio Address." December 17, 2005. <http://fdsys.gpo.gov/fdsys/pkg/WCPD-2005-12-26/html/WCPD-2005-12-26-Pg1880.htm>. See also http://georgewbush-whitehouse.archives.gov/news/releases/2005/12/20051217.html for a live file of the speech.

[163] The Washington Post. "Transcript: U.S. Senate Judiciary Committee Holds a Hearing on Wartime Executive Power and the NSA's Surveillance Authority." February 6, 2006. <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html>.

[164] Ibid.

means necessary to give the President the go ahead to:

> …to capture or kill Osama bin Laden and to use the American military to do that. It did not authorize domestic surveillance of American citizens. [165]

Questions concerning whether or not the President had the original authority to implement a program such as the TSP (given *FISA*'s intent – not least of which is to curb executive abuses of such powers) were at the heart of the Committee's concerns. Even on the chance that the President was correct in authorizing such a program, there was still the issue of oversight and where that oversight might belong (i.e. with Congressional Intelligence Committee or with the Foreign Intelligence Surveillance Court (FISC)). On March 28, 2006 the Committee heard the testimony of five former FISC judges. It was their opinion that the FISC should be given the formal oversight role over the TSP.[166]

The Role of the Telecoms

Whether the President had acted in accordance with the law was certainly debatable, but even if the President had acted within proper bounds, questions concerning the role of the telecom companies within the program and their potential legal liability were now being raised. Clearly, the program could not have existed without their cooperation; however, their ability to refuse to participate, as well as the scope of the presidential order in question, was not fully understood at the outset. As Don J. Michaels notes:

---

[165] Ibid.

[166] Lichtblau, Eric. "Judges on Secretive Panel Speak Out on Spy Program." New York Times. March 29, 2006. <http://www.nytimes.com/2006/03/29/politics/29nsa.html>.

> …intelligence agencies depend greatly on private actors for information gathering. Second, the Executive is institutionally predisposed to act decisively and unilaterally during times of crisis, even if that means bypassing legal restrictions, skirting congressional and judicial oversight, and encroaching on civil liberties. Third, to the extent corporations currently are (or can be made to be) willing partners, the Executive may choose to conduct intelligence policy through informal collaborations, notwithstanding the legal, political, and structural collateral harms these inscrutable bargains may generate.[167]

More than a month after the news broke about the TSP, the Electronic Frontier Foundation (EFF) filed a class action lawsuit against telecom giant AT&T on January 31, 2006.[168] The EFF lawsuit alleged that AT&T violated the *Stored Communications Act*, Title II of the *Electronic Communications Privacy Act (ECPA)*; the *Wiretap Act*, Title I of the *ECPA*; and the *Pen Register Statute*, Title III of the *ECPA*.[169] With the media frenzy underway, and Senate Judiciary Hearings set to begin, any hopes that the Bush Administration may have had that the issue would simply blow over seemed to have been dashed.

Indeed with papers like *USA Today* reporting that AT&T, Sprint and MCI were all participating in the program of warrantless surveillance, the number of possible partners within the TSP appeared to be growing, as was interest in the story both in the media and within the Government

---

[167] Michaels, Jon D. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror." California Law Review 96: 901, p. 907.

[168] Electronic Frontier Foundation. "NSA Multi-District Litigation." December 8, 2009. <http://www.eff.org/cases/att>.

[169] Wolfson, Stephen Manuel. "National Security Surveillance and National Authentication System: The NSA, AT&T, and the Secrets of Room 641A." I/S: A Journal of Law & Policy for the Information Society 3 (2008): 411, p. 417.

itself. The spring of 2006 gave way to increasingly negative press reports and mounting public concern over the scope of the program. *Newsweek* reported that the NSA had apparently revealed the names of more than 10,000 U.S. citizens that it had monitored.[170] In addition, the scope of the participation by the telecom companies in the TSP made further headlines on May 11, 2006 when *USA Today* reported that NSA had constructed a "massive database of Americans' phone calls."[171] The call records of perhaps tens of millions of Americans, the paper alleged, had been provided to NSA using data provided by AT&T, Verizon and BellSouth. The collection of these call records, according to reporter Seymour Hersh, initially began with the tracking of chains of phone numbers connected to phones that had called high-risk regions.[172] Basically, the way it worked according to Hersh's reporting, is that programmed computers were used to:

> …map the connections between telephone numbers in the United States and suspect numbers abroad, sometimes focussing on a geographic area, rather than on a specific person—for example, a region of Pakistan. Such calls often triggered a process, known as "chaining," in which subsequent calls to and from the American number were monitored and linked. [173]

Inevitably, as the telephone chains grew longer, more and more American calls were being swept into the monitoring.

---

[170] Hosenball, Mark. "Spying: Giving Out U.S. Names: National Security Agency's Release of Names of Americans on "Intercept" List." Newsweek May 2, 2006: 10.
[171] Cauley, Leslie. "NSA has massive database of Americans' phone calls." May 11, 2006. <http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm>.
[172] Hersh, Seymour. "National Security Dept. Listening In." The New Yorker. <http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh>.
[173] Ibid.

With more and more telecoms being implicated, several were quick to proclaim their non involvement with the TSP. Companies like Qwest, although never named in the original press reports, announced publicly that it had not participated in the program (it later became known that its lawyers were more than skeptical about any potential legal liability that compliance would bring and advised the company not to participate).[174] This was soon followed by pronouncements from BellSouth and Verizon that they were never involved in the program – forcing *USA Today* to amend its original claim that these companies had participated in the program.[175] That said, AT&T neither confirmed nor denied assisting the NSA – with the media and legal storm around that company's involvement continuing as new revelations about its involvement in the NSA program were coming out in the press.[176]

As details emerged about the program through documents and interviews with the whistle blower at the centre of the EFF class action suit, Mark Klein, it appeared that AT&T had provided NSA with access to phone and internet traffic passing through its San Francisco switching center, which it could then sift using data mining software.[177] If this could be happening at AT&T, the question on the minds of those in the media and civil liberties groups was where else could this be happening? Piecing together the investigative reporting of numerous journalists, and the details emerging from the EFF case, as well as the Administration's account of the program, a particular picture began to take shape as to just how the program was operating. As Richard A. Posner describes it, the TSP's main operation was one of interception, data mining, and human

---

174 PBS. "Frontline: Spying on the Home Front (streamed video) " 2007. <http://www.pbs.org/wgbh/pages/frontline/homefront/>.

175 Drinkard, Jim. "Verizon says it isn't giving call records to NSA." USA Today. May 16, 2006. <http://www.usatoday.com/news/washington/2006-05-16-verizon-nsa_x.htm>.

176 Ibid.

177 Singel, Ryan. "Whistle-Blower Outs NSA Spy Room." Wired. April 7, 2006. <http://www.wired.com/science/discoveries/news/2006/04/70619>.

search of intercepted messages. Once a communication was intercepted it could then be filtered through computer data mining techniques and eventually, if there was reason to believe that the communication was of interest, it could be passed through a human filter. [178]

Legal Troubles Ahead

The Administration's legal woes with regard to the program were just beginning, and certainly District Court Judge Anna Diggs Taylor's decision on August 17th 2006 in the case of AC*LU v. NSA*,[179] was to be a serious setback for the President. According to Justice Taylor's ruling, the President did not have the power to authorize the NSA's domestic spying program under either the Iraq War resolution or the Constitution. Her 44 page opinion was viewed as a judicial check on executive power – a biting reminder to the President that his powers were not without their limits:

> It was never the intent of the Framers to give the President such unfettered control, particularly where his actions blatantly disregard the parameters clearly enumerated in the Bill of Rights.[180]

Taylor, knowing full well that the Government would appeal the decision, stayed her ruling pending appeal.[181] In October 2006, a three judge panel of the Sixth U.S. Circuit Appeals Court

---

[178] Posner, Richard A. "Privacy, Surveillance, and Law." University of Chicago Law Review 75 (2008): 245, p. 253.

[179] ACLU v. Nat'l Sec. Agency / Central Sec. Serv., 438 F. Supp. 2d 754, 2006 U.S. Dist. LEXIS 57338 (2006)

[180] Ibid.

[181] Judges have the ability to 'stay' a ruling if they know an appeal is imminent. What that means is that rather than changing the law immediately (i.e. striking it down a law as unconstitutional), the judge can provide their ruling but temporarily suspend it pending the appeal. This means that we have the rationale for their ruling, but the ruling itself cannot take effect either until the proscribed amount of time has passed or the higher court has ruled on the appeal case.

ruled that the NSA's TSP program could continue through the appeal process.[182] The program was not dead, but for the moment it was on life support.

As the *ACLU v. NSA* case was working its way through the courts in 2006-2007, Attorney General Gonzales was doing his best to assure the public that there was sufficient legal oversight in place and that there was a unified legal opinion amongst DOJ and Administration officials that the program itself was constitutional.[183] Still the court of public opinion did not seem convinced – and in a surprising reversal, the Attorney General announced on January 17th 2007 that:

> …any electronic surveillance that was occurring as part of the Terrorist Surveillance Program will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court….[184]

The announcement came in the form of a letter addressed to the Chairman of the Senate Judiciary Committee, Patrick Leahy, and Ranking Minority Member, Arlen Spector concerning the NSA program. As the Attorney General noted, by bringing the TSP under the supervision of the FISC, the President would no longer have to authorize the program as he has been doing (every 45 days or so).[185] Despite the willingness of the Administration to bring the program under the purview of the courts, they were very much still in hot water over a program which had authorized warrantless surveillance of American citizens.

---

[182] ACLU v. NSA/Central Sec. Serv., 467 F.3d 590, 2006 U.S. App. LEXIS 32346 (6th Cir., 2006)

[183] After the news of the program broke, Gonzales was making appearances on programs like PBS's *The New Hour with Jim Lehrer* to defend the President's actions as constitutional. See January 23, 2006 transcript of interview for the program <http://www.pbs.org/newshour/bb/law/jan-june06/gonzales_1-23.html>.

[184] Lichtblau, Eric, and David Johnston. "Court to Oversee U.S. Wiretapping in Terror Cases." New York Times. January 18, 2007. <http://www.nytimes.com/2007/01/18/washington/18intel.html>.

[185] Gonzales Letter is available online through the New York Times: <http://graphics8.nytimes.com/packages/pdf/politics/20060117gonzales_Letter.pdf>.

In the months that followed, the Attorney General's testimony before the Senate Judiciary Committee was long and labored. The issue of the TSP had not disappeared from the public radar, and along with the recent firing of eight U.S. Attorneys, it had proved to be yet another scandal for the Administration. Due to the inherent secrecy of the TSP, Attorney General Gonzales was not at liberty to answer some of the questions for national security reasons. This resulted in gaps, inconsistencies and conflicting accounts in his testimony. The differing accounts of Gonzales and the former Deputy Attorney General, James Comey over a March 2004 hospital visit to a very sick Attorney General John Ashcroft (Gonzales' predecessor), [186] received a lot of media attention. Gonzales, then serving as White House Counsel, along with Andy Card, the President's Chief of Staff, according to Comey, were upset with his (Comey's) decision not to reauthorize the program due to DOJ concerns that the program was illegal. In an attempt to bypass Comey, the two men attempted to persuade Ashcroft to reauthorize Bush's domestic surveillance program.[187]

Comey's testimony was particularly damning in that it cast Gonzales and Card as trying to take advantage of a sick man in an attempt to get the DOJ's blessing for continued authorization of the TSP program. Despite their best efforts John Ashcroft told the two men that that he was not the Attorney General (those powers had been transferred to Comey), and that he would not sign the authorization. [188] The testimony was a stark contrast to the claims being made by the Administration that there was no question among Administration and DOJ officials as to the

---

[186] Eggen, Dan, and Paul Kane. "Gonzales Hospital Episode Detailed: Ailing Ashcroft Pressured on Spy Program, Former Deputy Says." The Washington Post May 16, 2007: A01.

[187] Politicstv. "Gonzales: Pressured Hospitalized Ashcroft to OK Spying (Testimony of James Comey before the Senate Judiciary Committee." May 15, 2007. <http://www.youtube.com/watch?v=hxHjWYA50Ds>.

[188] Eggen, Dan, and Paul Kane. "Gonzales Hospital Episode Detailed: Ailing Ashcroft Pressured on Spy Program, Former Deputy Says." The Washington Post May 16, 2007: A01.

legality of the TSP program.[189] With dozens of class action lawsuits being filed across the country against both the Government and the telecom companies for their participation in the TSP program, it appeared that this problem was not going away any time soon.

Change in the Legal and Political Tide

Despite all the media attention and conflicting testimonies before the Senate Judiciary Committee, a curious thing happened in July 2007. The ACLU's victory in the *ACLU v. NSA* case was overturned on appeal marking a change in the legal tide. The Appeals Court did not address any of the legality issues surrounding the program, but rather only the issue of whether the plaintiffs lacked standing.[190] In order to prove that they had legal standing, the plaintiffs would have had to demonstrate that their rights had actually been infringed, and given the secret nature of the program, finding the evidence to prove such violation would have been close to, if not, impossible. The end result, a 2 – 1 ruling, found the plaintiffs lacking such standing, and therefore the case was overturned.[191]

With a change in the legal tide there was a corresponding shift in the political tide. With the original ruling now struck down, the question of constitutionality of the program was, for the moment at least, moot. The Administration had its program (Justice Taylor's tongue lashing no longer applied) and it had already addressed the issue of its operating outside of the courts by bringing it under the watchful eye of the FISC. That said, there still remained the pesky problem of lawsuits against the telecoms – the providers of the very data required to run the TSP - as well

189 Goldsmith, Jack. The Terror Presidency: Law and Judgment Inside the Bush Administration. New York: Norton, 2007.
190 ACLU v. NSA, 493 F.3d 644, 2007 U.S. App. LEXIS 16149 (6th Cir.) (6th Cir. Mich., 2007)
191 Ibid.

as the need, more importantly to protect the Administration and its agencies and departments against any further lawsuits in the event that any future plaintiffs could prove their legal standing in court.

Addressing the Remaining Legal Concerns

Several legal questions remained, not least of which was whether authorization of the program was within the President's powers. Even if it were, the constitutional questions as to whether NSA's data collection methods were in violation of Fourth Amendment rights also had to be taken into account. In his book, *In the Common Defence: National Security Law for Perilous Times*, military judge James E. Baker sets out a number of legal arguments facing the President and his legal advisors in response to both sides of the argument for and against Presidential authority in authorizing the TSP.

In his arguments for the program, Judge Baker looks at the constitutional framework which established the President's powers as Commander-in-Chief. The courts have recognized that this power is not subject to legislative interference when acting in this capacity. In times of war, it is well agreed upon that:

> …the president has no higher constitutional responsibility than to protect the United States from attack. [192]

Taking into account the fact that Congress cannot legislatively interfere with the President's war

[192] Baker, James E. In the Common Defence: National Security Law in Perilous Times . Cambridge: Cambridge University Press, 2007.

time powers, *FISA* would in this sense be acting unconstitutionally if it acted in such a way as to impede the President's ability to carry out his constitutional duties as Commander in Chief. Judge Baker best sums up these arguments as follows:

> Based on the president's broad constitutional authority in the area of national security, including his authority to collect the intelligence necessary to effectively execute those duties, the president may lawfully authorize the TSP. This argument is enhanced to the extent the president determines the FISA requirements are impractical in application and prevent the president from undertaking his core security functions.[193]

In presenting arguments against the President's authority, Judge Baker examines the constitutional framework as laid out by the Fourth Amendment which provides a guarantee against unreasonable searches and seizures. As a matter of law, *FISA* requires that judicial approval for a warrant be obtained in order to conduct electronic surveillance within the U.S. To argue that *FISA* would be unconstitutional in impeding the President's ability to conduct warrantless surveillance would ignore the fact that the statute allows him to conduct such surveillance in periods of declared war and in periods of emergency, where obtaining such a warrant may not be possible given the time constraints involved. In those cases the warrant can be applied for after the fact. Baker sums up his arguments against as follows:

> Absent a compelling demonstration that the surveillances falls outside the *FISA's* parameters…presidential authorization of warrantless surveillance at best places the

[193] Ibid.

> president at a low ebb of his authority. The better view, in light of the specificity of the statute, and the longstanding acquiescence of the executive in the Act's constitutionality, is that *FISA* did not leave the president at a low ebb in exercising residual inherent authority, but extinguished that authority. [194]

In examining these arguments it is clear that there are merits on both sides, if the President is truly acting within his capacity as Commander-in-Chief. Assuming that he is acting within his capacity, the arguments on the side of the President seem strongest if *FISA* is actually impeding his ability to carry out those duties. What is not clear, though, is why *FISA* would actually be doing so. If it is possible to obtain such warrants without prior judicial approval (assuming that these can be easily gotten retroactively) then the argument for presidential authority begins to weaken. Of more concern then become the Fourth Amendment arguments:

> The issue of whether the TSP violates the Fourth Amendment entails a reasonableness analysis that strikes a balance between governmental and individual interests.[195]

In examining this issue, Richard Henry Seamon presents the original three-part test as laid out by Justice Jackson in *Youngstown Sheet and Tube Co. v. Sawyer*. In this case, President Truman tried, albeit unsuccessfully, to take over the steel mills in order to ensure that they would produce enough steel for the Korean War effort. In this instance the Court rejected the President's Commander-in-Chief arguments on the grounds that although the President is Commander-in-Chief he is not Commander of the Country. That test puts in place a framework that, according

[194] Ibid.
[195] Seamon, Richard Henry. "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits." Hastings Constitutional Law Quarterly 35: 449, p. 466.

to Justice Jackson, "reflects the interdependence of the President and Congress in certain matters, including war." [196] The test lays out three scenarios that rank presidential power against that of Congress in descending order of legitimacy and works as follows:

1. President acts with express or implied authority from Congress
    - This is presidential power at its maximum
2. President acts with neither congressional approval nor denial
    - President must rely upon his own independent powers
3. President acts in defiance of congressional orders
    - This is presidential power at its "lowest ebb" [197]

By Seamon's analysis, the application of the same test in *Youngstown* to the TSP provides an interesting juxtaposition. As Seamon states:

> Justice Jackson's framework makes it important to determine whether the TSP is authorized by - or is instead inconsistent with - the express or implied will of Congress. The President argues that the TSP was authorized at its inception by the AUMF, but this argument lacks merit. Without the AUMF to support it, the TSP violates FISA and so presents Justice Jackson's third situation. Accordingly, the surveillance can fall within the President's power, despite violating FISA, only to the extent that Congress is constitutionally "disabled" from curbing the President's power. [198]

[196] Ibid.
[197] Ibid, p. 469.
[198] Ibid, p. 469.

Although the Court in *Youngstown* did not find President Truman's actions to fall within the scope of the President's Commander-in-Chief powers as such actions were not authorized by any statute or any extra-statutory power under the Constitution, [199] assume for argument's sake that this did not apply in the TSP case. Even if this were a genuine situation whereby war time power applies, the question of the Fourth Amendment still requires consideration, since it would only seem sensible that whatever course of action the President took, his advisors should be advocating measures which would impair those rights as minimally as possible.

Ethical Concerns

The response to the disclosure of the TSP, both pro and con, has, in much the same way as the *Patriot Act*, taken the form of competing utilitarian and contractarian ethical arguments. Those supporters of the Administration's decision to work outside of *FISA* have cited the "prevention of harm" – in this case the protection of national security interests – as the grounds for keeping the program secret.[200] For many of these supporters, the idea that the New York Times would disclose the program is tantamount to treason because it had the potential to place the country in harm's way by revealing to the enemy the methods being used to collect information on terrorist activities – perhaps tipping off the enemy to use alternative means of communication in order to avoid detection. That being said, given the nature of the program – which is secret – the only way to justify its existence on utilitarian grounds is to take the word of those officials who are party to the program. The consequentialist approach would seem to require lexically that: 1. it has in some demonstrable way prevented terrorist attacks, and 2. that the overall good it has achieved in meeting this goal, has outweighed any harmful effect that has resulted in a reduction

[199] Ibid, p. 467.
[200] Goldsmith, Jack. The Terror Presidency: Law and Judgment Inside the Bush Administration. New York: Norton, 2007, p. 180.

of civil liberties for those whose communications have been caught up in the sweep of the program.

In contrast, to the utilitarian arguments, those who have expressed their concern that the program violated not only *FISA* but also protected Fourth Amendment rights under the U.S. Constitution, have appealed largely to contractarian / rights-based arguments.[201] Similar to the arguments expressed in the previous chapter on the *Patriot Act*, the fact that the TSP operated under such a high level of secrecy, that it lay outside of the normal checks and balances, disregarding *FISA* as set out by Congress and operating outside the normal judicial oversight of the FISC, makes it difficult, although not impossible to defend on contractarian grounds. The caveat here is that to defend it on such grounds, requires that the Commander-in-Chief arguments must be held above all others in the ordering of conflicting constitutional claims. In terms of wartime presidential power, this argument would certainly hold sway and would, I think be justified under a Rawlsian approach; however, as we have seen above, this argument is harder to defend in a perpetual war on terror where the threat level is increasingly difficult to measure and relies on a paternalistic, 'trust us,' approach to information sharing.

In addition to the ethical concerns generated by the program's mere existence, the TSP program also raises a number of important ethical questions at an operational level concerning how the data were obtained, the ways in which the data can be used and ultimately the trade offs involved, that is to say, what the true impact on civil liberties has been. Given the secret nature of the program and its intended purpose, which is to act as one of the many tools at the

[201] One only needs to look at the objections raised by the ACLU, The Electronic Frontier Foundation and other civil liberties groups for a comprehensive discussion of the rights-based concerns.

Government's disposal to guard against future terrorist attacks, it becomes hard to evaluate the program in the absence of specifics. Although those in the media have suggested what they think is going on through a number of confidential sources / whistle blowers,[202] the program remains highly guarded and thus it is not clear how the program is actually operating.

Like many of the post 9/11 ethical debates, the TSP has been framed in a utilitarian light, one which requires that the citizen trust the few members of the executive, and now legislative and judicial branches who have been involved in the program, to protect the greater good of their national security. Prior to the December 2005 disclosure of the program, the simple fact that the program was operating outside of the purview of the courts and was even hidden from members of the House Intelligence Committee, was perhaps most disturbing because the potential for the abuse of unchecked power was at its greatest. In light of the recent changes to the TSP, which occurred as a result of the public revelations of the program's existence, some of the early ethical concerns have undoubtedly been mitigated. That said, there are still issues about the program which require further examination.

First is the issue of how corporations are used in the operation of the program. In order to gather the data from which the NSA may mine for possible terrorist threats, the co-operation of telecommunications corporations is required. As was seen in the example of Qwest, the inability of the company to publicly challenge the legality of the Government request, due to the secret nature of the program, was problematic. Qwest alleged that it lost government contracts as a result of its unwillingness to co-operate with a program that its legal counsel thought was illegal.

[202] Reporters from a number of major papers such as the *New York Time, Washington Post, USA Today* have speculated about the full extent of the TSP based on the information obtained from their sources; however, the details of the program remain classified.

If corporations are pressured into co-operation for fear of lost business or other reprisals, the Government's position begins to lose some of that moral high ground luster. Although the program has now been acknowledged, the alleged action of the Government in the Qwest case could prove problematic given the number of 'other programs' operating under high level secrecy about which the public has not been made aware (President Bush in his radio address on December 17th alluded, as did former Attorney General Gonzales in his Senate Judiciary testimony that there were other programs). [203]

Second, there remains the overarching concern about right to privacy as constitutionally guaranteed. Richard A. Posner asserts that in the chain of events (interception, data mining and human searches) it is only the last event which raises constitutional and legal concern. His argument is that computer generated searches are not actual impairments to an individual's privacy rights, but is this actually the case? The potential for targets being deemed of interest or appearing on watch lists before human searches are able to rule them out as false positives would arguably be just as damaging, if not more. To assert, as he does, that "[c]omputer searches do not invade privacy because search programs are not sentient beings," [204] appears disingenuous.

The concerns that the TSP raises within the debate over privacy rights during times of insecurity have the potential to shape future legislation and to influence policy decisions at the highest levels. What is crucial here is the ability to maintain some kind of balance between the security concerns that the TSP was set up to address and the civil liberties concerns that any infringement

[203] Eggen, Dan, and Paul Kane. "Gonzales, Senators Spar on Credibility Account of Meeting In '04 Is Challenged" The Washington Post Wednesday, July 25, 2007 <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/24/AR2007072400207.html>.

[204] Posner, Richard A. "Privacy, Surveillance, and Law." University of Chicago Law Review 75 (2008): 245.

of protected Fourth Amendment rights entails. The changes to *FISA* as outlined in the following chapter provide an interesting window into the Bush Administration's response to the media storm surrounding the TSP and its attempts to minimize the legal and political fallout that occurred as a result of the program's disclosure.

Chapter 6.

FISA Modernization: Mitigating Legal Liability

Numerous changes were made to the *Foreign Intelligence Surveillance Act (FISA)* in the post 9/11 period, with many having been incorporated into the *Patriot Act* itself. Regardless of these changes, and the potential that existed for further changes in the period immediately following the September 11th attacks, the Administration did not press Congress to legislate additional measures that would surely have avoided the legal questions that arose after the public disclosure of the Terrorist Surveillance Program (TSP). Rather, prior to that disclosure, the executive branch merely chose to ignore the law, thereby avoiding any of the legislative details that might have thrown a kink in the operation of the TSP itself. Then came the New York Times story, and with it came the claim by the Government that *FISA* lacked the ability to keep up with the pace of technological change. Where the TSP had managed to tip toe around the legislation for the previous four years, it seemed that this was no longer the case. Bringing the program under the Foreign Intelligence Surveillance Court (FISC) in January of 2007 provided additional legitimacy to the program now that there was judicial oversight. That said, the original rationale for keeping the program outside the *FISA* had not disappeared and hence the push for modernization was just beginning. If the executive branch had to work with *FISA*, then it might as well be on its terms.

The claim by the Administration was clear: *FISA* was out of date and in desperate need of modernization. As a justification for circumventing the Act all together, the argument was pretty

weak, but given the potential legal liability of telecommunications companies and government officials – the need for revising the Act became a matter of urgency.

Backgrounder: *The Protect America Act of 2007*

On August 5th 2007, President Bush signed into law the *Protect America Act of 2007 (PAA)*,[205] effectively broadening and legitimizing the activities which NSA's TSP was already engaged in – that being warrantless surveillance of the phone and electronic communications of Americans with the aim of routing out potential terrorist threats. In early August, Senators Mitch Connell and Christopher Bond sponsored legislation to amend *FISA.* In speaking to the legislation, which was eventually to become the *Protect America Act (PAA),* Senator McConnell stressed the urgency that accompanied the bill. This was a bill that had garnered support from the Director of National Intelligence, Admiral Mike McConnell. Admiral McConnell, having had a chance to examine the bill himself, had "certified [to its drafters and to the Senate in a prepared statement that it] would give him and [the] intelligence community the ability to protect the homeland."[206]

Senator McConnell's co-sponsor, Senator Christopher Bond, echoed these sentiments. In his opening remarks in support of the bill, he emphasized the sheer necessity of the bill's passage, stating:

> It is absolutely critical for our national security that we change the law which currently, by its application, is denying our intelligence community a very significant portion of the signals intelligence they could collect on al-Qaida and other terrorist sources who may

[205] *Protect America Act of 2007* Public Law no: 110-55.

[206] Senator McConnell's comments on the Senate Floor in reference to Admiral McConnell's support for the McConnell-Bond bill: < http://www.c-spanvideo.org/congress/?q=node/77531&id=7705146>.

well be planning another 9/11 attack on the United States.[207]

Among the changes proposed, this new legislation would allow the Director of National Intelligence and the Attorney General to authorize collection of information concerning persons outside the U.S. without warrants, the warrants being replaced by a series of notifications to the FISC that proper procedures had been followed.[208] The change was a major departure from traditional procedures under *FISA* and represented a major shift in the role of the FISC as a means for judicial oversight. Knowing full well the magnitude of this shift, the Senate had a six-month sunset provision written into the legislation.[209] With the sunset clause in place, the message the Senate sent out to Congress was clear: this was temporary legislation, meant only to fill the stop gap.

With the passage of this new law, the TSP program had a framework from which it could now legally operate. Although the President had, up until the passage of this act, been asserting his authority in authorizing the TSP under his Commander-in-Chief's powers, Congress, by passing the act, had now legitimized the program and by default the actions of the President. In essence, through this action, Congress had now enabled the President to act with maximum power. According to James Risen, by enacting the legislation, the White House was in effect responding to:

---

[207] Senator Bond's comments from the Senate Floor [Congressional Record: August 3, 2007 (Senate)] <http://ftp.fas.org/irp/congress/2007_cr/s080307.html>

[208] *Protect America Act of 2007* Public Law no: 110-55

[209] Nakashima, Ellen and Hsu, Spencer S. "Democrats Offer Compromise Plan On Surveillance; Proposal Would Involve FISA Court in Warrants." Washington Post. August 2, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/08/01/AR2007080101514.html?nav=emailpage>

> …a still classified ruling earlier [that] year by the special intelligence court, [that] said the government needed to seek court-approved warrants to monitor those international calls going through American switches.[210]

The new legislation, which was "largely drafted by the White House and received no committee hearing,"[211] provided a legislative exemption from obtaining warrants under *FISA* for persons reasonably believed to be outside the U.S. Under the new law, the old system of warrants was now replaced with a system of court notifications whereby the Government would notify the Court that the surveillance had occurred, and the Court's role would be to ensure that the Government had followed proper procedures in filing the notification.

In reporting on the program the day after the legislation was passed, Charlie Savage of *The Boston Globe* rightly noted that the *PAA* had in essence broadened the Government's powers to conduct warrantless surveillance. The first way it did this was through its requirement that telecommunications companies make their facilities available for government wiretaps. Since companies no longer had the ability to 'opt out,' the new statute contained a provision that shielded companies from lawsuits. This 'immunity provision' was viewed as a necessary precondition in order to ensure compliance with the law. The second way in which it broadened power was through its removal of the original requirement of the TSP that surveillance be restricted to calls and e-mails involving a suspected terrorist - the new law makes no such

---

[210] Risen, James. "Bush Signs Law to Widen Reach for Wiretapping." The New York Times. August 6, 2007. <http://www.nytimes.com/2007/08/06/washington/06nsa.html>.

[211] Savage, Charlie. "New law expands power to wiretap - Diminishes oversight of NSA spy program." The Boston Globe. August 6, 2007. <http://www.boston.com/news/nation/washington/articles/2007/08/06/new_law_expands_power_to_wiretap/>.

distinction.[212] Rather than allowing oversight to remain with FISC, as had been granted by Attorney General Gonzales in early 2007, the new law gave the Attorney General and the Director of National Intelligence "the power to approve the international surveillance, rather than the special intelligence court."[213] The conversion of the Court's role to merely procedural, rather than substantive, oversight meant that the Court would no longer be involved in scrutinizing the cases of individuals targeted for surveillance. Instead, under the new law, the Court would only concern itself with questions surrounding whether or not the Government had "applied proper procedures used in the surveillance after it has been conducted."[214] Given the sweeping nature of the reforms that the *PAA* made to *FISA*, its passage was made conditional on there being a sunset provision built into the legislation that would allow Congress to revisit the changes in six months time, when it could decide to make the legislation permanent, further amend it, or repeal it.

Expired on Sunset: Filling the gap left by the lost legislation

In a speech delivered before a large banner that read "Threat Operations Centre" at the NSA, President Bush urged Congress to make permanent the provisions of the *PAA*. Playing on the fears and emotions of a country not quite recovered from the September 11th terrorist attacks, the President thanked intelligence, law enforcement and homeland security professionals who worked tirelessly against a ruthless enemy "determined to murder innocent people." Without pause, he informed Congress that it was their duty to "give the professionals the tools they need

---

212 Savage, Charlie. "New law expands power to wiretap - Diminishes oversight of NSA spy program." The Boston Globe. August 6, 2007. <http://www.boston.com/news/nation/washington/articles/2007/08/06/new_law_expands_power_to_wiretap/>.

213 Risen, James. "Bush Signs Law to Widen Reach for Wiretapping." The New York Times. August 6, 2007. <http://www.nytimes.com/2007/08/06/washington/06nsa.html>.

214 Ibid.

to do their work as effectively as possible."[215]

In a speech that emphasized tools, there was of course no mention of the controversial TSP - the tool in question. Instead, the President focused on the need to amend the *FISA*. For those who had been following the story, this was an attempt by the Administration to address the constitutional questions that remained in terms of that program's legality in the face of multiple class action lawsuits that were brewing. By portraying the *FISA* as "dangerously out of date," the President implied that anyone who questioned the Administration's proposed amendments to *FISA* was endangering national security. The President's message was clear on this point when he stated that:

> Unfortunately, some in Congress now want to restrict the tools. These restrictions would impede the flow of information that helps us protect our people. These restrictions would reopen gaps in our intelligence that we had just closed… The question I'm going to ask is, do our professionals have the tools necessary to do the job to protect the American people from further attack? [216]

The Administration's claim that *FISA* had not kept pace with technological developments like the disposable cell phone and the Internet skirted around the real issue - not whether *FISA* was technologically up to date, but rather whether or not the Government's reliance on private infrastructure to conduct its intelligence operations left the telecoms vulnerable to lawsuits, and in turn left the Government's warrantless surveillance operations open to further public scrutiny.

---

[215] White House. "Transcript: President Bush Discusses the Protect America Act of 2007." Sept. 19, 2007. <http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070919.html>.

[216] Ibid.

If the telecoms were not immunized from such lawsuits, it would be impossible for the Government to compel them to co-operate in its spying operations; likewise, the potential for disclosure of evidence in such telecom cases had, in the Government's view, the potential to place national security operations at risk. On this point the President was clear:

> It's particularly important for Congress to provide meaningful liability protection to those companies now facing multi-billion dollar lawsuits only because they are believed to have assisted in efforts to defend our nation following the 9/11 attacks. Additionally, without this protection, state secrets could be revealed in connection with those lawsuits -- and our ability to protect our people would be weakened. [217]

Of course, if the telecoms required immunity from class action suits for breaking the law, the obvious question was: is the program legal to begin with?

Arguments for Modernization

According to David S. Kris, there are three main arguments for modernizing *FISA*. The first argument is that *FISA* must be modernized because the statute's regulatory reach has been artificially expanded by the transition from satellite to fiber optic cable for carriage of transoceanic communications. *FISA*, as passed in 1978, did not regulate satellite communications because they involved the use of radio waves to carry international calls, but the language did regulate surveillance of international wire or cable communications. The Government claim was that surveillance of international communications that used to be

[217] Ibid.

conducted outside of FISA was now subject to the statute because of changing technology. According to Kris this claim has proven to be exaggerated "since the transition from satellite to cable was neither as dramatic, nor as unanticipated, as the Government argues."[218]

The second argument is that *FISA* does regulate surveillance of international wire or cable communications, to or from the U.S., when conducted inside this country. As long as no particular American in the U.S. is being targeted, *FISA* does not regulate surveillance of those same communications, on those same wires or cables, when conducted on a portion of the wire or cable located outside this country. If the Government wants or needs to conduct such surveillance inside the U.S., (which it would if relying on the infrastructure of private telecommunications companies) it would bring that surveillance under *FISA*. One of the key issues in the debate about *FISA* modernization is whether that change in the location of the surveillance should continue to trigger the statute's application. [219]

And finally Kris' third argument is that *FISA*'s regulation of email communications is problematic. While *FISA* does not regulate surveillance of a foreign-to-foreign telephone call (even if monitored from within the U.S.), it does regulate surveillance of a foreign-to-foreign e-mail messages if acquired from electronic storage inside the U.S. Part of the problem of email is that you cannot always determine "consistently, reliably, and in real time" the location of parties to an e-mail communication. In the absence of a requirement to verify the location of the email communications (to and from) the "exemption may be too broad, potentially embracing domestic e-mail, which even the Director of National Intelligence has said should remain subject to

[218] Kris, David. "A Guide to the New FISA Bill, Part I." Balkinization. June 21, 2008. <http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-i.html>.
[219] Ibid.

traditional *FISA*. This is one of the main problems that has bedeviled efforts at *FISA* modernization."[220]

Of these three arguments, Kris notes that only the first argument was advanced publicly by the Bush Administration: that *FISA* must be modernized because the statute's regulatory reach has been artificially expanded by the transition from satellite to fiber optic cable for carriage of transoceanic communications. In drafting the *FISA Amendments Act of 2008 (FAA)* these three main arguments were taken into account, but were hardly the main grounds for pushing modernization; and certainly of these issues, as Kris notes, only the first was even publicly discussed. The real issue at hand was still addressing the legal liability that had arisen out of the operation of the TSP.

Retroactive Immunity and *the FISA Amendments Act of 2008*

With the *PAA* set to expire, pressure from the Administration was building. For the Administration, the act became a symbol of their 'tough on terror' stance, and any reluctance to pass it was merely playing into the hands of those terrorists who were bent on harming Americans. With an election looming, the tough on terror approach no doubt played its part in securing the passage of the Act, which was now being touted as a bipartisan bill. In an unusual move, the House held a secret session before the legislation was even tabled to discuss the issues at stake before moving on to the specifics of the new bill. With C-span cameras halted for one hour[221] and representatives having taken an oath not to disclose the nature of the proceedings, the details of that meeting are out of the public record, but one can only speculate that the meeting,

[220] Ibid.

[221] C-Span. "Capital News: House of Representatives to go into closed session tonight to discuss classified FISA information." March 13, 2008. <http://www.youtube.com/watch?v=kB-JGqDukbY>.

in combination with the political sensitivities faced by Democrats in an arena of 'tough on terror' politics, may have had an impact on the final outcome of the bill.

In commenting on the *FAA* the night before the House was set to vote on it, the bill's sponsor, Democratic Congressman Silvestre Reyes, the Chairman of the House Permanent Select Committee on Intelligence, referred to the *FAA* as a bipartisan compromise. By repealing the *PAA* and replacing it with this new "vital national security legislation," Silvestre asserted that the change would both modernize and strengthen *FISA* while at the same time "protecting Americans' constitutional rights."[222] Reyes defended the amendments in the new legislation as necessary for intelligence agencies to conduct lawful surveillance of:

> …foreign terrorists or other foreign agents overseas whose electronic communications may pass through the United States.[223]

In recognizing that intelligence is the first line of defense in preventing terrorist attacks, Reyes noted the importance of the bipartisan bill as it related to national security; however, he was quick to point out that the legislation served another "vital function" in that it strengthened the constitutional rights of Americans by protecting them from "unlawful surveillance." Here Reyes was taking direct aim at President Bush's claim of executive power to conduct warrantless surveillance of Americans. [224] By bringing the TSP and all other such surveillance programs authorized by the President under the scope of *FISA* and FISC, Reyes was implying that the new

---

[222] Congressman Silvestre Reyes TX. "Rep. Reyes released a statement on the bipartisan compromise on H.R. 6304, the Foreign Intelligence Surveillance Act (FISA) Amendments of 2008." Jun 19, 2008. <http://reyes.house.gov/News/DocumentSingle.aspx?DocumentID=110549>.

[223] Ibid.

[224] Ibid.

law had the necessary judicial oversight that had been absent at the time of the TSP's disclosure.

Reyes' press release did not give any details regarding the scope of FISC's powers as they would now be constituted under the new legislation. His co-sponsor, Republican Congressman Peter Hoekstra, was much more forthcoming in his description of the Court's role in a speech he gave on the House floor the day the bill was passed. In describing the role of the Court, Hoekstra explained that the authority of the Court was an issue of great debate during the drafting of the new legislation. What is striking though, given the remarks made by the bill's sponsor regarding limiting presidential power, is Hoekstra's comment that the law as amended would:

> …statutorily insert the *FISA* court in a limited way into the Executive's Constitutional authority to collect foreign intelligence information targeting foreign persons in foreign countries.[225]

Hoekstra's point is crystal clear – the President was within his rights in authorizing the TSP or any other such program. Although the President, it can be inferred from Hoekstra's comments, was acting within the scope of his powers as Commander-in-Chief as delineated under the U.S. Constitution, the purpose of this compromise bill was to allow the Court to:

> …provide some sort of additional check to ensure that the IC [Intelligence Community] is properly using its procedures to target a foreigner abroad and to minimize U.S. person

[225] Congressional Record (Extensions). "FISA Amendments Act of 2008." June 26, 2008. <http://www.fas.org/irp/congress/2008_cr/h062608.html>.

information that may be incidentally obtained. [226]

Hoekstra explains that unlike traditional *FISA* applications, there is no mechanism included in the amending legislation that would require that the Government demonstrate probable cause in its notification to the Court. This would be a major break with past practice for *FISA* applications. The new law would merely prescribe a method for FISC to verify that the intelligence community had followed proper procedures when surveilling targets – the Court's oversight role in determining the existence of probable cause having effectively been removed.[227]

The lack of a probable cause requirement was something that Congressman Bobby Scott, chairman of the House Crime Subcommittee, took issue with. Scott opposed the bill on the grounds that it provided for "widespread acquisition of private conversations without meaningful court review."[228] As Scott noted, the only court review in the whole process was a "check on whether or not the Government certifies that the process has been followed." [229] Scott also noted his concern over the Government's collection procedures with regards to the Court. In terms of data collection under the new legislation, the Government could now surveil a target for up to 7 days without court approval, a change from 48 hours under the old *FISA*. The *FAA's* emergency provisions would allow for data collection to continue even if the Court rejected the Government's certification on procedural grounds - this collection could continue for a period of 60 days pending appeal. In terms of the immunity provisions, Scott argued that this was an area

---

226 Ibid.
227 Ibid.
228 Congressional Record (House). "FISA Amendments Act of 2008." June 20, 2008. <http://www.fas.org/irp/congress/2008_cr/house-fisa.html>.
229 Ibid.

that "should be reviewed by the courts, not decided here in Congress." The lack of meaningful court review, in Scott's view, was reason enough to defeat the bill.

Scott's sentiments were certainly shared by other congressmen and women. Congresswoman Zoe Lofgren rose in opposition to this bill, stating that she could not support the legislation's "deeply flawed provisions relating to the issue of immunity for telecommunications companies."[230] Under the current legislation, Lofgren argued, the role of the Court would be relegated to that of a rubber stamp for the Administration. The review process provided in the bill, according to Lofgren was really just window dressing:

> …an empty formality that will lead to a preordained conclusion, dismissing all cases with no examination on their merits. Under this bill, the courts are not allowed to ask whether the conduct of the corporations who assisted was in fact legal. They may only note that the administration says that it was legal. In other words, the decision on the ultimate question of legality, a decision the Constitution dedicates to the judiciary, will instead be made by the executive branch with the judiciary acting as a rubber stamp. [231]

Despite the objections raised by Lofgren, Scott and others, concerning the lack of judicial oversight and the immunity provisions, the supporters of the act ultimately prevailed. For them, the legislative compromise, as it was being touted, although imperfect, at least garnered some oversight by the courts. The immunity provisions would secure the participation of the telecommunications companies. Even though their participation was required by law, the

[230] Ibid.
[231] Ibid.

chances of a company suing the Government on the grounds that the statute was unconstitutional seemed slight at the time. On June 20th 2008 the amendments to *FISA* passed the House of Representatives by a vote of 293 to 129.[232]

Having just passed in the House of Representatives, the legislation now proceeded to the Senate for approval. Speaking in support of the bill, Senator Kyl presented the *FAA* as being "a law that our Nation needs." According to Kyl, the new bill would allow "immediate and real-time surveillance of overseas targets as soon as they become apparent in the course of a foreign-intelligence investigation." Noting a 2007 FISC decision that interpreted *FISA* to apply to foreign-to-foreign communications routed through the U.S., Kyl stated that the new legislation would correct this problem. Although the problem which Kyl cites is an obvious one, which would no doubt require amendment, he seems to question the Court's competence in being able to make certain judgements regarding intelligence collection. Kyl notes that the Court would provide the procedural oversight, but in terms of the new legislation's removal of probable cause determinations, Kyl believes that the Court should:

> …not be second-guessing intelligence judgments, and should not be imposing procedures or making demands that will consume intelligence resources and divert agents from their primary mission. This limited role should also allow the *FISA* Court to decide these cases very quickly, minimizing the burden on both the intelligence community and on those judges who are assigned to the *FISA* Court.[233]

---

232 Ibid.

233 Congressional Record (Senate). "FISA Amendments Act of 2008." June 24, 2008. <http://www.fas.org/irp/congress/2008_cr/fisa062408b.html>.

In making this statement, Kyl would seem to be confirming Congressman Lofgren's concern about the Court being turned into the rubber stamp for the Administration. Whatever the oversight function Kyl envisioned for the Court, it would appear to be minimal at best.

Senator Jay Rockefeller, speaking in favor of the bill from the Senate floor on July 8, 2008, was quick to point out that:

> …the President made the very misguided decision to create a secret surveillance program that circumvented the judicial review process and authorization required by *FISA* and was kept from the full congressional oversight committees. [234]

For Rockefeller it was understandable that many congressmen and women would be upset by the President's 'go it alone' approach. That being said, the business now before the Senate required immediate action. According to Rockefeller, the new legislation would accomplish three important goals with respect to the President's warrantless program:

1. Provides a means for learning the truth about the President's program as it requires the relevant Inspectors General of the various elements of the intelligence community to submit an unclassified report;
2. Tightens the exclusivity of the *FISA* law, making it improbable for any future President to argue that acting outside of *FISA* is lawful;
3. Addresses the problems the President's decision has caused for the telecommunications

[234] Congressional Record (Senate). "Foreign Intelligence Surveillance Amendments Act of 2008." July 8, 2008. <http://www.fas.org/irp/congress/2008_cr/fisa070808.html>.

> companies that were told their cooperation was both legal and necessary to prevent another terrorist attack.[235]

Whether or not the legislation would actually go far enough in terms of meeting these goals was debatable, and there were certainly a number of senators who took issue with the bill. Among them, Senator Patrick Leahy proved to be a vocal opponent. In his remarks on the Senate floor, Leahy made his discontent known. The idea that there would be no accountability for either the Administration or the telecoms who participated in the warrantless surveillance program was disconcerting for Leahy because it would no doubt result in the dismissal of ongoing cases. If the lawsuits were unable to proceed, then it would be certain that no court would ever be in a position to review whether the program itself was legal. According to Leahy:

> …the bill would have the affect of ensuring that this administration is never called to answer for its actions – never held accountable in a court of law.[236]

By violating the provisions of *FISA*, Leahy argued that the President, consistent with *Youngstown*, had sought to act in an area in which Congress had already acted and exercised its authority, thereby reducing presidential power to the 'lowest ebb.' If a court had an opportunity to review the legality of the TSP in light of the President's decision to bypass *FISA*, Leahy did not believe that the President's action would be upheld on the basis of his Commander-in-Chief

---

235 Ibid.

236 Senator Patrick Leahy (D-Vt.). "Closing Statement Of Sen. Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee, On Senate Consideration Of The FISA Amendments Act Of 2008." July 9, 2008. <http://leahy.senate.gov/press/200807/070908b.html>.

powers. [237]

Leahy expressed his frustration over the Administration's efforts to ensure that Congress "could not effectively review the legality of the program." [238] He also noted that, in attempting to investigate the TSP, the Judiciary Committee's efforts to obtain the necessary information to evaluate the administration's legal arguments were stonewalled. His comment concerning the attempts to issue subpoenas is telling:

> Indeed, Senator Specter, when he was chairman of the Judiciary Committee, prepared subpoenas for the telecommunications carriers to obtain information, simply because the administration would not tell us directly what it had done. But those subpoenas were never issued; Vice President Cheney intervened to undercut Senator Specter and prevent the Committee from voting on them.[239]

Senator Russ Feingold similarly was concerned about the impact that this legislation would have. Referring to his role on the Intelligence and Judiciary Committees, Feingold felt that he was in a good position to comment on the changes being proposed to *FISA* as one of the few members of the Senate who had been fully briefed on the TSP. Because of the classified nature of the program, Feingold was not in a position to publicly discuss the details of the program, but he did warn his colleagues that if more "information was declassified that members of the Senate would regret their having passed this legislation."[240]

---

237 Ibid.
238 Ibid.
239 Ibid.
240 U.S. Senator Russ Feingold Wisconsin. "Remarks of U.S. Senator Russ Feingold in Opposition to the FISA

> Publicly, all I can say is that I have serious concerns about how those activities may have impacted the civil liberties of Americans. If we grant these new powers to the government and the effects become known to the American people, we will realize what a mistake it was, of that I am sure.[241]

Several attempts were made by individual senators to modify the legislation. Senator Arlen Specter proposed limiting retroactive immunity for telecoms to cases where a Federal court had determined such assistance as being constitutional. Senator Bingaman proposed that the Congress legislate that the courts stay any pending cases against certain telecommunications companies until the final report of the Inspector General on the President's Surveillance Program is submitted to Congress. And finally, Senators Dodd, Feingold, and Leahy jointly proposed an amendment to remove the immunity provisions from the act altogether. These amendments were rejected by the White House which issued a press release stating that the President would veto any such amendments to the bill as passed by the House.[242] With the threat of a veto looming, and the pre-election jitters on the part of some Democrats who were afraid of appearing weak on national security issues, it is little wonder that the bill passed with a vote of 69 – 28 in the Senate on July 9th 2008, receiving the President's signature the next day.[243] The only saving grace left for those who opposed the bill was that it too would sunset, like much of the other controversial legislation of the post 9/11 period, in 2012. This would allow time for the next Administration to review the legislation, and to decide if it was indeed effective, let alone constitutional.

Amendments Act " July 9, 2008. <http://feingold.senate.gov/record.cfm?id=306014>.

241 Ibid.

242 White House Press Release. "Fact Sheet: Retroactive Liability Protection Is Critical to Our National Security " July 8, 2008. <http://www.usdoj.gov/archive/ll/docs/fisa-factsheet-070808.pdf>.

243 "H.R. 6304--110th Congress: FISA Amendments Act of 2008." GovTrack.us (database of federal legislation). 2008. Feb 11, 2010 <http://www.govtrack.us/congress/bill.xpd?bill=h110-6304>

Legislative Provisions

With the passage of the *FAA*, the Administration's concerns over legal liability for the telecoms were now addressed. With the immunity protections for the telecoms secured, the potential for the class action lawsuits then before the courts to proceed (assuming that the courts found the law itself to be consistent with the constitution) was slight. Although the press coverage focused largely on the issue of telecom immunity, the new law entrenched the role of FISC as laid out in the *PAA*, a role which had more to do with seeing that the procedures inherent in the use of *FISA* certifications were followed than it had to do with the substantive nature of the certifications themselves.

With the oversight role of the FISC having been greatly diminished, it seemed only fitting that the new law require some sort of additional check on the President's Surveillance Program. That check was a provision in the legislation requiring an annual review by the "head of each element of the intelligence community," a reference to the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency (NSA), the Department of Defense (DOD), and any other element that participated in the President's Surveillance Program. The provision required these officers to:

1. conduct a review of, among other things, the establishment, implementation, product, and use of the product of the Program; and
2. provide an interim and final review report to the intelligence and judiciary committees[244]

[244] The Library of Congress Thomas. Bill Summary and Status-110th Congress (2007-2008) H.R.6304. CRS Summary. August 2007. <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR06304:@@@D&summ2=m&>.

With the issuance of such a report a year away at that point, the Bush Administration could celebrate for the moment. As the President professed at the signing of the *FAA:*

> Today I'm pleased to sign landmark legislation that is vital to the security of our people. The bill will allow our intelligence professionals to quickly and effectively monitor the communications of terrorists abroad while respecting the liberties of Americans here at home.[245]

For President Bush, the passage of this legislation was confirmation that his surveillance programs (the TSP being one such program) now had the official blessing of Congress. Although the programs had previously been operating outside of *FISA*, the passage of the new law brought the programs within the scope of the act while maintaining a minimal level of oversight by the FISC.

Legal Outcomes: Ruling of the *FISA* Court

In a most unusual move in January 2009, the Foreign Intelligence Review Court (the appeal court of FISC) released its August 2008 ruling that telecommunications companies must comply with government requests to monitor the electronic communications of individuals in terrorism-related investigations.[246] The ruling was in response to an unidentified company's 2007 challenge of the *PAA* on Fourth Amendment grounds. In that case the company refused to

---

[245] White House Press Release. "Speech by President Bush after he signs H.R. 6304, FISA Amendments Act of 2008." July 10, 2008. <http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/20080710-2.html>.

[246] See <http://www.fas.org/irp/agency/doj/fisa/fiscr082208.pdf > for copy of heavily redacted FISC ruling

cooperate with government demands for information in the absence of a warrant under the *PAA*.[247]

According to the New York Times:

> The company was forced to comply, under threat of contempt, while it challenged the law in the *FISA* court, the opinion noted. The company argued that the law violated the constitutional rights of its customers and that the act placed too much power and discretion in the hands of the executive branch. It also raised specific privacy problems, which the court ruling did not identify, that could occur under the surveillance directives it had received from the government. [248]

Although the ruling was released after the legislation in question had been replaced with the *FISA Amendments Act of 2008 (FAA)*, its finding that the *Fourth Amendment's* requirement for warrants is not applicable to foreign collection of intelligence involving Americans is the first of its kind.[249]

As a result of the privacy safeguards that the Administration had put in place, the Court rejected the claim that the Act violated the Fourth Amendment. Although the ruling was narrowly focused on the application of the new legislation, and did not comment on the President's constitutional powers in ordering domestic wiretapping without warrants, the New York Times

---

247 Risen, James, and Eric Lichtblau. "Court Affirms Wiretapping Without Warrants" The New York Times. January 16, 2009. <http://www.nytimes.com/2009/01/16/washington/16fisa.html>.
248 Ibid.
249 Ibid.

quoted Peter Hoekstra, the ranking Republican on the House Intelligence Committee, as saying that the ruling "reinforces the significant, bipartisan political consensus" in favor of the president's broad assertions of wiretapping powers.[250]

Dismissal of the Class Action Lawsuits

In addition to the Foreign Intelligence Review Court's decision, the changes to *FISA* law have also had an impact on the multiple class action lawsuits facing the telecoms that participated in the Terrorist Surveillance Program (TSP). The wrangling over the legality of those telecoms participation in the TSP, at least for the moment while pending appeal, has ended in some three dozen class action suits being thrown out in June 2009. Despite the fact that "consumer and privacy groups raised important constitutional issues in their claims," Chief Judge Vaughn R. Walker of the Federal District Court in Northern California, ruled "that Congress had left no doubt about its 'unequivocal intention' when it passed a measure last summer giving immunity to phone carriers in the wiretapping program."[251] Indeed the *FAA* has achieved its primary purpose: the granting of retroactive immunity.

Ethical Concerns

Although the Act may have achieved its primary purpose (the granting of retroactive immunity), many ethical questions remain concerning whether or not the President acted within his constitutional authority, or indeed overstepped his bounds.[252] By passing the *FAA* in its current

---

250 Ibid.

251 Lichtblau, Eric. "Telecom Companies Win Dismissal of Wiretap Suits." New York Times. June 4, 2009. <http://www.nytimes.com/2009/06/04/us/politics/04nsa.html>.

252 "Recent Legislation: Electronic Surveillance - Congress Grants Telecommunications Companies Retroactive Immunity from Civil Suits for Complying with NSA Terrorist Surveillance Program. - FISA Amendments Act of 2008, Pub. L. no. 110-261, 122 Stat. 2436. " Harvard Law Review 122 (2009): 1271.

form, Congress effectively removed any ability of the courts to rule on this constitutional issue because the new legislation clarified Congress's intention which was to legitimize the President's actions through the granting of retroactive immunity to the telecommunications companies who participated in the program.

Had Congress not passed this legislation, the courts would have been able to assess the legality of the President's actions according to the legal framework laid out by James E. Baker in the previous chapter, that is, to assess whether or not the President was acting within the bounds of his Commander-in-Chief powers. The passage of this legislation has meant that a definitive answer as to whether or not the courts would have deemed such actions constitutional will never be forthcoming.

The utilitarian defense that continued cooperation on the part of the telecoms required the passage of the *FAA*, faces the same problems as the utilitarian arguments for the original *Patriot Act* or for the operation of the President's Surveillance Program (PSP) prior to their disclosure. The actual benefits of the *FAA* cannot be assessed if the information required to do so is secret. Therefore, it is impossible to really assess these measures in any meaningful sense because the knowledge required to do so (in order to formulate any kind of actual utilitarian calculus) is unavailable. These examples only work to illustrate why public debate about 'trade offs' in the national security v. civil liberties is so frustrating as an intellectual exercise.

From a contractarian view, the PSPs might have been saved if, as James E. Baker notes, the courts found such programs to have been justified under the President's Commander-in-Chief

powers. The passage of the *PAA* and the subsequent *FAA* has made any attempt to answer this question in a meaningful way a moot point. Although the public will never have an answer to this question from the courts, the ethical questions concerning potential abuse of presidential power remain. The impact that this episode in American history will have on arguments concerning the limits of this power for future presidencies is yet to be tested.

In all three of the case studies examined in this paper, questions of proportionality are of central importance if there is ever to be any meaningful discussion of achieving a balance in the debate over liberty versus security. Although much of the debate has been framed using utilitarian and contractarian / rights-based arguments, these two ethical theories are often viewed as incompatible or competing theories. In my next chapter I take an alternative view, one that sees both theories as contributing to an applied ethical framework through the use of practical proportionality tests which can be applied by the courts in their decision making.

Part IV:

THE FUTURE OF PRIVACY IN POST 9/11 AMERICA

Chapter 7

Privacy Rights and Limits of Government Intrusion

The concept of the right to privacy was first articulated in the American legal literature over a century ago by Samuel Warren and Louis D. Brandeis.[253] Concern over how technology was being used to capture private information necessitated, in their view, an examination of the ways in which technological advances could allow intrusions into an individual's private realm, and the ways in which the law could be used to prevent such intrusions by upholding the right to privacy. Today we live in an age where technological change is rapid and ever advancing. As stated in the preceding chapters, the ability of the Government to collect huge swaths of data through domestic legislation such as the *Patriot Act*, and foreign intelligence information through *FISA*, the *PAA* and the subsequent *FAA* raises numerous privacy questions for Americans.

The future of privacy for post 9/11 America is largely dependent upon there being some mechanism for government accountability and oversight in areas where data collection and surveillance are conducted. This is not simply a matter of protecting the 'right to privacy;' it is also a matter of respecting the rule of law. If there is agreement that Government should be open and accountable to the people, the question remains, how may such openness and accountability be achieved in an age of terrorism? Furthermore, what are the boundaries limiting government intrusion on privacy rights in times of heightened security concerns?

The simple solution seems to be that the Government cannot be above the law – that it should be

[253] Warren, Samuel, and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890): 193.

held accountable in a court of law. That said, as we saw in the last chapter, Congress, by passing the *FAA*, effectively stripped the Court of any ability to rule on the legality of the President's Surveillance Program (PSP) because it legalized the President's activity prior to any court ruling on such activity. Retroactive legislation which prevents a court from ruling on constitutional matters seems to flout the very idea of the rule of law and the supremacy of the courts in interpreting the Constitution. The only saving grace that we may have here is that Congress, through its secret session, may have had very good security reasons for protecting the PSPs so that their details would never become known.

The Path Forward

In writing about the post 9/11 period one needs to remain mindful that the attacks which took place on September 11th, 2001 have no doubt left an indelible mark on the American psyche. In order to advance a means for moving forward there is no simple calculus for how to balance liberty and security since both are equally important. That does not mean that there is no way forward, or that the discussion of the two will not bear fruit; it is merely to say that this dissertation does not provide a calculus. What it aims to do is to advocate a test for achieving some kind of proportionality that is compatible with protecting the security of Americans while at the same time respecting their rights to privacy.

The potential for catastrophic consequences from acts of terrorism has reached a new peak, on par with acts of war perpetrated by individual states. As was seen on 9/11, the need for some sort of pre-emptive surveillance is crucial in order to prevent such attacks. That said, the need for oversight and accountability to ensure that such pre-emptive collection of data is within the

scope of the law is paramount. Several authors have advanced the idea of incorporating the proportionality of a *Terry stop* into electronic surveillance investigations where Fourth Amendment rights may be infringed. In this chapter I seek to build upon their ideas with a proposal that the courts use a more rigorous form of proportionality standard than that which the *Terry stop* currently provides. The proportionality model which I advocate is one that seeks to address both the contractarian and utilitarian concerns that have shaped the 'liberty versus security' debate. Rather than inventing a new legal test, I look to the two pronged test as laid out in the Canadian case of *R. v. Oakes*[254] which seeks to do precisely that: balance the competing ethical concerns in cases where an individuals' rights may be limited under the *Canadian Charter of Rights and Freedoms*.[255] The resulting new proportionality model that I am advocating, although based on Canadian rather than American jurisprudence, is one that I believe it still applicable as it is merely an ethical test to be used in the balancing of competing contractarian and utilitarian claims. Although I have opted to use the Canadian proportionality test, it should be noted that there is an overwhelming mass of legal doctrine supporting the principle of proportionality from various foreign jurisdictions.[256]

Terry v. Ohio:[257] **Proportionality**

In the seminal case of *Terry v. Ohio* (1968),[258] the U.S. Supreme Court held that the Fourth Amendment prohibition on unreasonable searches and seizures had not been violated in a case of a stop and frisk where a police officer had reasonable suspicion that a crime was about to be

---

254 R. *v.* Oakes, [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200.

255 *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act*, *1982*, being Schedule B to the *Canada Act 1982*, (U.K.) 1982, c. 11. lays out the rights and freedoms that are entrenched in the Canadian Constitution.

256 Christoffersen, Jonas. Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights. Leiden, Netherlands: Martinus Nijhoff, 2009. p. 31.

257 Terry v. Ohio, 392 U.S. 1 (1968).

258 See Appendix F of this dissertation on page 204 for a summary of this case.

committed. In *Terry*, a plain clothes police officer observed two men who he believed were "casing" a store front with the intention of committing an armed robbery of the store. Upon a pat down[259] of the two men's clothing weapons were discovered and seized. The court ruled that such searches could be conducted without probable cause, so long as the officer had a reasonable suspicion that a crime had been, was being, or was about to be committed. Reasonable suspicion in such cases could not be based on mere intuition or a hunch, but rather had to be based on "specific and articulable facts."[260] In its ruling the Court found that "there is 'no ready test for determining reasonableness other than by balancing the need to search (or seize) against the invasion which the search (or seizure) entails.'"[261]

The idea of incorporating the reasonableness of a search and seizure into the discussion of balancing liberty and security concerns is one that authors such as Christopher Slobogin, K.A. Taipale, and Stephanie Cooper Blum have advocated. Slobogin in his work, *Privacy at Risk*, sets out a framework for proportionality that is built on two propositions. The first proposition is that the interest that the Fourth Amendment protects is security from unjustified government infringement on individuals' property, autonomy (in the sense of ability to control one's movements), and privacy. The second proposition is that the greater the threat to that security, the greater justification the Government should have to show.[262]

Starting with these two propositions Slobogin seeks to use *Terry v. Ohio* as a case for

---

[259] The officer did not proceed to search inside the men's clothing until he had felt the weapons. The court viewed the frisk of the outer garments for weapons as being less than a full blown search.

[260] Terry v. Ohio as cited in Slobogin, Christopher. Privacy at Risk: The New Government Surveillance and the Fourth Amendment. Chicago: University of Chicago Press., 2007, p. 22.

[261] Ibid, p. 21.

[262] Ibid, p. 23.

proportionality that is compatible with any limitation on Fourth Amendment rights, one that is not just limited to a brief stop and frisk but one that might be applicable to various forms of government surveillance. His first proposition suggests that we need to protect against unjustified intrusions upon the right – but does not suggest that no intrusion would ever be permissible. His second proposition suggests that any relaxation of the Fourth Amendment in the name of national security should not be automatic. That is to say, the Government requires legal justification for any intrusion upon the right in question. To go back to the Court's decision, that would mean that the Government would still need to demonstrate that it had in its possession 'specific and articulable' facts before it could place any limitation on a Fourth Amendment right.

For Taipale, the use of a reasonable suspicion standard as found in Terry would combine the statutory mechanism for congressional authorization and oversight with an explicit statutory basis for judicial orders and review.[263] What is interesting here is that Taipale's proposal also incorporates the idea that "legitimate foreign intelligence requirements can be met without resorting to unilateral secret executive branch approvals or by shoehorning 'innovative' solutions not explicitly anticipated under *FISA*."[264] The idea of placing the ability to determine reasonableness, in this case balancing the need to search (or seize) against the intrusion that such a search presents for Fourth Amendment rights, back in the hands of the court is a promising one.

The analogy of using a traditional *Terry stop*, when trying to decide whether a warrantless search

[263] Taipale, K. A. "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance." Yale Journal of Law & Technology 9 (2007): 128, p. 161.
[264] Ibid, p. 161.

is justified, is one that Cooper Blum believes could be useful in any future amendment of *FISA*. According to Blum, "Congress should amend *FISA* to require probable cause that a terrorist (not just a foreign national as the FAA currently requires) has had contact with a U.S. person."[265] Cooper Blum incorporates Taipale's *Terry stop* suggestion, as a means for continued surveillance for a given period on the U.S. person to determine if he is a terrorist. The use of a *Terry stop* in the conducting of electronic surveillance, under these circumstances, would allow an authorized period for additional monitoring or initial investigation to determine whether the communications have any intelligence value.[266] As Cooper Blum notes, "if this follow-up surveillance revealed that the U.S. person was an agent of a foreign power, then a traditional *FISA* warrant could be obtained based on probable cause."[267] The end result would allow that "probable cause could still be the predicate standard for FISC ex ante review-but it would apply to a very different inquiry than is currently required under *FISA* and the *FAA*." [268]

As Slobogin, Taipale, and Cooper Blum note, that the idea of a *Terry stop* equivalent for electronic surveillance provides a useful analogy for potential *FISA* and *FAA* modification in instances involving U.S. persons (since these persons' communications would be outside the scope of *FISA*) . If applied to cases involving electronic surveillance for foreign intelligence purposes, the flexibility that this new standard would allow – that is a shift from probable cause to reasonable suspicion - would enable the Government to engage in electronic surveillance for the purposes of identifying whether a U.S. person was actually engaged in the planning, and / or commission of, or had already committed a terrorist act.

---

265 Blum, Stephanie Cooper. "What really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." Boston University Public Interest Law Journal 18 (2008): 269. p. 311.
266 Ibid, p. 309.
267 Ibid, p. 309.
268 Ibid, p. 311.

A More Rigorous Proportionality: Oakes Test

The Court in *Terry v. Ohio* found that there is no ready test for determining reasonableness other than balancing the need to search (or seize) against the infringement of the right in question. The court, in its ruling, has clarified that there must be proportionality in terms of the Government's need to protect public safety and security against any infringement of an individual's Fourth Amendment rights. The need to balance these competing interests is evident in the Court's decision; however the balancing mechanism used in *Terry* could be further clarified by incorporating another balancing mechanism used by the Canadian judiciary to ascertain when a protected Charter right may be subject to limitation.

In the Canadian context the use of the *Oakes Test* for determining when a Charter right[269] may be subject to limitation, is compatible with the need for proportionality as demonstrated in *Terry*. In the case of *R. v. Oakes,*[270] David Edwin Oakes was arrested by police officers who found eight one-gram vials of hash oil in his possession. At that time Section 8 of the Narcotics Act stipulated that once the court has determined that an individual was in possession of illegal narcotics, the burden of proof was on the individual to demonstrate that he or she was not in possession of them for the purposes of trafficking (a much more serious crime). Oakes challenged that the reverse onus of proof was contrary to Section 11 (d) of the *Canadian Charter of Rights and Freedoms*, which guarantees the right to be "presumed innocent until proven guilty."[271] In addressing the Charter challenge, the Supreme Court of Canada had to consider whether Section 8 of the Narcotics Act could be saved under Section 1 of the Charter which

[269] The phrase 'Charter right' is commonly used to refer to a constitutionally protected right as laid out in the *Charter of Rights and Freedoms*

[270] See Appendix E of this dissertation on page 199 for a summary of this case.

[271] R. *v.* Oakes, [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200.

states that:

> The Canadian Charter of Rights and Freedoms guarantees the rights and freedoms set out in it subject only to such reasonable limits prescribed by law as can be demonstrably justified in a free and democratic society.[272]

In addressing this concern the Court developed what has come to be known as the *Oakes Test* which is a test that is used to determine the constitutionality of legal limitations on Charter Rights as a whole (although this case dealt with a search and seizure, the test is applicable to all Charter rights). This test is the model used in Canada to determine if a limitation by the Government on a protected Charter right is a reasonable limitation of the right being infringed. The Court found that the Crown must be able to demonstrate, on the balance of probabilities, the following:

1. **Purpose or Objective of the Law**

The law must be a response to a *"pressing and substantial"* problem in order to consider overriding a Charter Right

2. **Proportionality**

In order to arrive at a calculation of the suitability of the means used to pursue the Law's objective, the following three questions must be answered:

[272] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*, (U.K.) 1982, c. 11

(a) Are the means rational and non arbitrary?

(b) Is there minimal impairment to the right?

(c) Is the good that will be achieved by these means sufficient to outweigh the negative effects caused by the infringement of the right in question?

Since the test is really an ethical test that seeks to balance the contractarian concerns (upholding the right itself) against the utilitarian concerns (protecting the greater good), its application I would argue should not be simply limited to the Canadian context. Indeed the Court's ruling in *Terry v. Ohio*, which called for balancing the need to search (or seize) against the invasion which the search or seizure entails, demonstrates that the Court knew it needed to address both concerns making it compatible with the proportionality test as laid out in the *Oakes Test*.

When applying the *Oakes Test* to the Fourth Amendment cases, the following two objectives must be satisfied in order to override the right in question: (1) the law must be a response to a pressing and substantial concern; (2) the law must be proportional, that is, that the good that will be achieved by the law in question must outweigh the negative effects caused by the law. Proportionality is further determined by a three pronged proportionality test (outlined above). The first prong of this test requires that the limit on the right be rationally connected to the legislative objective of the law. Second, the Government must demonstrate that the limit on the right in question represents the least restrictive means of achieving this objective. And lastly, the third prong examines whether the collective benefits to society as a whole outweigh its individual costs.[273] The *Oakes test* combines both contractarian (2.a & b) and utilitarian

[273] Manfredi, C. P., & Rush, M. E. (2008). *Judging democracy*. Peterborough, Ont: Broadview Press, p. 34.

elements (2.c) in its assessment of the overall proportionality of any legislation which impinges on a protected right.

The Oakes test has been applied to Canadian cases ranging from commercial expression (*Irwin Toy Ltd. V. Quebec*[274]), to hate speech (R. v. *Keegstra*[275]), to obscenity (R. v. *Butler*[276]), and child pornography (*R. v. Sharpe*[277]), among others. In each of these Charter cases, the purpose or objective of the law in Part 1 of the *Oakes test* was not the driving issue, rather it was the proportionality tests as laid out in Part 2 which concerned the court.

The case of *Ford v. Quebec*,[278] is a prime example of a Charter case[279] where the purpose or objective of the law was insupportable when applying the proportionality test as laid out in *Oakes.* In that case, the Supreme Court of Canada found that Quebec's objective of protecting the French language was sound, but the means with which it attempted to do so did not meet the criteria laid out in the proportionality test in *Oakes*. Although there was a rational connection to the law's objective, the preservation of the French language, there was no evidence that the exclusive use of French-language signage was the only means available to achieve that purpose. By contrast, the predominant display of the French language in addition to other languages (perhaps in smaller font) would be sufficient to achieving that purpose. A total ban on the use of other languages could not be viewed as a minimal impairment on the right to freedom of expression. Furthermore, the province's outright ban on the use of English signage

[274] *Irwin Toy Ltd. v. Quebec (Attorney general)*, [1989] 1 S.C.R. 927.
[275] *R. v. Keegstra*, [1996] 1 S.C.R. 458.
[276] *R. v. Butler*, [1992] 1 S.C.R. 452.
[277] *R. v. Sharpe*, 2001 SCC 2, [2001] 1 S.C.R. 45.
[278] *Ford v. Quebec (Attorney General)*, [1988] 2 S.C.R. 712.
[279] The phrase 'Charter case' refers to constitutional cases involving the *Charter or Rights and Freedoms*

disproportionately disadvantaged the English minority in the province.

Slobogin, Taipale, and Cooper Blum point to the need for a proportionality standard in conducting electronic surveillance; however the level of proportionality afforded by *Terry*, I would argue, is insufficient to this task. If we examine the circumstances in *Terry* and apply them against the *Oakes Test* criteria, this becomes clearer. In terms of the purpose or objective of the law (Part 1. of the *Oakes Test*), *Terry* allows for a reduction of the probable cause standard to one of reasonable suspicion in order to allow law enforcement officials to apply investigative techniques in situations where they believe a crime has, is, or will be committed by a potentially armed suspect. The case could be made that combating this type of crime is a "pressing and substantial" concern for society as a whole and thus requires a relaxation in the standard so that law enforcement officials have an additional tool at their disposal to best address the problem. In terms of the proportionality aspect (Part 2.) *Terry* only really addresses the last prong of the proportionality test (2.c), that is the utilitarian aspect of the test.

Applying *Terry* to the proportionality test in Part 2 of the *Oakes test* is revealing. In responding to each of the questions posed in Part 2, I found the following:

2. (a) Are the means rational and non arbitrary?

The stop and frisk for weapons is connected to protecting the safety of the officers investigating a person who they believe has, is, or is about to commit a crime. The lowered standard from one of probable cause to reasonable suspicion is deemed necessary for the protection of the officers. The reduced standard also ensures that the exclusionary rule[280] is not applicable on the grounds

[280] If weapons are found, the argument that such evidence should be excluded in Court because the weapons were found as a result of an unlawful search and seizure, would not be applicable.

of unlawful search and seizure. The Court has specified that the only restriction on this reduced standard is that the officers must be able to demonstrate "specific and articulable facts"[281] - this reasonableness criterion is one which the court has said there is "no ready test for determining reasonableness other than by balancing the need to search [or seize] against the invasion which the search [or seizure] entails."[282] What would have otherwise been a contractarian test in *Oakes* would now seem to rest on a utilitarian calculus as a result of this last criterion, which is slightly problematic because the 'right' is now subject to a weighing of harms rather than having the emphasis remain on whether or not the right has actually been infringed in any absolute sense.

2. (b) Is there minimal impairment to the right?

The Court in *Terry* has pointed to the need to balance the 'search (or seize) against the invasion which the search (or seizure) entails'[283] suggesting that minimal impairment to the right is key to the successful application of the *Terry stop* standard; however the court does not enter into a discussion of possible alternatives that might take the place of a *Terry stop*.

2. (c) Is the good that will be achieved by these means sufficient to outweigh the negative effects caused by the infringement of the right in question?

The implication in *Terry* is that the answer is yes - that a stop and frisk which results in apprehension of an individual who has, is, or is about to commit a crime and is believed to be armed with a weapon outweighs the negative effects so long as it is based on reasonable suspicion rather than a mere hunch.

[281] Terry v. Ohio, 392 U.S. 1 (1968).
[282] Ibid.
[283] Ibid.

A simple application of the grounds laid out in *Oakes*, would demonstrate the utilitarian nature of the original decision in *Terry*. The real strength in *Oakes* is that it combines both the contractarian and utilitarian tests in order to provide a better overall protection for rights against purely utilitarian reasoning. *Oakes* provides a test which is easily generalizable and transferable, making application of the test by subsequent courts consistent - unlike the American decisions that have cited *Terry* in their rationale. These courts have worked to expand the definition of a *Terry stop* by extrapolation rather than through the application of a clearly defined test like the one laid out in *Oakes*.[284]

In the Canadian context the *Oakes test* is used to test limitations on all Canadian Charter rights, not just those involving search and seizure, which would require that the principles laid out in the test could be applied to all such protected rights. The reasoning implied in the *Terry stop* is utilitarian in nature; combining it with the contractarian principles in the *Oakes test* would yield better protections for the Fourth Amendment rights in a way that is generalizable enough to easily encompass electronic surveillance under *FISA*. A modified *Oakes* test could take the following form:

1. Purpose or Objective of the Law

The law must be a response to a *"pressing and substantial"* problem in order to reduce the standard of probable cause to one of reasonable suspicion under the Fourth Amendment.

[284] The Supreme Court used the precedent set in *Terry v. Ohio* as the grounds for its ruling in Michigan v. Long, 463 U.S. 1032 (1983) that car compartments could be searched if an officer had reasonable suspicion that they contained a concealed weapon.

2. Proportionality

In order to determine the suitability of this lowered standard, the infringing statute must:

(a) be rational and non arbitrary

(b) result in minimal impairment to the right

(c) demonstrate that the good that will be achieved by such infringement sufficiently outweighs any deleterious effect on the Fourth Amendment.

This modified version of the *Oakes test*, unlike the *Terry stop* advocated by Slobogin and others, would provide the courts with a more rigorous tool for calculating the proportionality of any proposed limitation on Fourth Amendment rights under *FISA* regarding the standard accorded to electronic surveillance: reasonable suspicion v. probable cause. If the proposed amendments were able to prevail overt what is essentially a combination of contractarian and utilitarian tests the court would be in a better position to actually determine the reasonableness of a search or seizure rather than simply having to appeal to a utilitarian calculus for "balancing the need to search (or seize) against the invasion which the search (or seizure) entails."[285]

[285] Ibid.

Chapter 8

The Future of Privacy in Post 9/11 America: Conclusion

What are the boundaries limiting government intrusion on privacy rights and how are such boundaries drawn?

As a central research question, this is a complicated and difficult question to attempt to answer. Regardless, it is a question that needs to be asked. In conducting my research, I focused on three case studies in point: the *Patriot Act*; The Terrorist Surveillance Program (and subsequent President's Surveillance Program); and the amendments to the *Foreign Intelligence Surveillance Act* that resulted from the revelation by the New York Times that such warrantless surveillance programs existed. In each of my case studies I examined the above research question in a way that was narrowly focused on the Government's use of electronic surveillance and its impact on protected Fourth Amendment rights.

The ethical, legal and political considerations with regard to the collection, classification, and dissemination of intelligence information are many. Clearly the Government has a duty to protect the national security of its citizens, but that duty must also be balanced against a competing duty to uphold the Constitution. In the American context, the place of Fourth Amendment rights in foreign intelligence investigations has been vigorously debated in the post 9/11 period. The need to balance competing rights claims is not simply an academic exercise; it is of practical concern at a time in which heightened security concerns have indeed resulted in an

encroachment on civil liberties.

Initially 9/11 provided the exceptional circumstances that seemed to justify a reduction in privacy rights in the interest of national security. However, with the passage of time, and the December 2005 revelation in the New York Times that the Government had been conducting warrantless surveillance on American citizens, those same privacy rights have been brought to the forefront. The need for a public discussion about the reasonableness of such limitations on civil liberties, particularly Fourth Amendment rights in the face of terrorist threats, is of the utmost importance because without it we cannot determine the boundaries beyond which such encroachments cease to be reasonable.

Academics from a variety of disciplines have contributed to this public discussion with the vast amount of resulting scholarship focusing on the legal and political concerns inherent in this debate. This dissertation has sought to build upon this literature, examining not only the discussion of the legal and political, but also the ethical constraints that arise from the Government's use of electronic surveillance in gathering its intelligence information. That is to say, rather than simply looking for a constitutional basis for any discussion of legislative or policy reforms affecting such surveillance, that we also should be looking for a moral basis in any discussion of a reduction in privacy rights.

Developing an Ethical Framework

As an applied study in information ethics, this dissertation has sought to provide an ethical framework that incorporates the individual rights-based (contractarian) concerns along with the

collective consequentialist (utilitarian) concerns that arise from any threat to national security. This is not to suggest that other ethical theories could not have been used to address this question, for example, Kantian and Communitarian ethical theories could be used to address the same questions as is evidenced by Chapter 3 of this dissertation. The underlying rationale for trying to incorporate the utilitarian and contractarian approaches was based largely on the fact that these two ethical approaches have been used at cross purposes with no ground for compromise. If the choices are framed as civil liberties versus national security, there clearly will be no room for compromise.

The Bush Administration's defense of its various legislative and other anti-terrorist measures was visibly consequentialist. With its constant juxtaposition of liberty versus security, the Bush Administration frequently demonstrated its tendency to treat the Constitution as an impediment rather than a guide. With seemingly unchecked presidential wartime powers in a perpetual state of 'War on Terrorism,' there was little attempt by the Bush Administration to reconcile these two ethical frameworks except to pay lip service to the idea that somehow rights still mattered.

As the case studies examined in this dissertation demonstrate, the utilitarian 'prevention of harm' formed the cornerstone of that Administration's ethical arguments, be it in the form of perpetual gag order provisions under the *Patriot Act*, the rationale for the Terrorist Surveillance Program (among other secret Presidential Surveillance Programs (PSPs)) operating outside the purview of the Foreign Intelligence Surveillance Court (FISC), or the resulting changes to the *Foreign Intelligence Surveillance Act (FISA)* to make any potentially illegal actions on the part of the Administration legal, at least retroactively.

Do the utilitarian arguments suffice? As has been discussed throughout the dissertation, part of the problem in assessing whether or not the means used to prevent such harm to national security is justified is the fact that much of the information required to make such a calculation is secret and therefore beyond the bounds of discussion. That is not to diminish the Administration's need for secret information – clearly there is a need for that – but what is most worrying, especially in light of the President's creation of a warrantless surveillance program, was the way in which the Bush Administration chose to completely by-pass Congress and the courts in its pursuit of such intelligence gathering methods. The lack of congressional and judicial oversight which would hold the Administration accountable for its actions is an issue that should cause concern, because it paves the road for potential abuses.

Need for Checks and Balances

What are the boundaries limiting government intrusion on privacy rights and how are such boundaries drawn?

From a legal and political point of view, this research question implies that there should be some sort of check on government power. The fundamental means by which the U.S. Constitution establishes such a check is through a division of powers. By establishing a system of government with three distinct branches – executive, legislative and judicial – the founding fathers were clear in their intention to build a system that possessed the necessary checks and balances. Thus any discussion on the limitation of government powers should also involve a discussion of all three branches and their ability to keep each other in check. That is to say, that

except for any true instances of Presidential wartime powers, of the sort which James E. Baker describes, the executive does not have a monopoly on determining the limitation of Fourth Amendment rights in times of increased threats to the national security.

All three branches of government need to be involved in the discussion of civil liberties in a time of heightened threats to national security. The need for reasonableness in any attempt to override a constitutionally protected right, such as the Fourth Amendment, should be of the highest concern for each of these branches. Building upon the suggestions put forth by authors such as Christopher Slobogin, K.A. Taipale, and Stephanie Cooper Blum, to incorporate the equivalent of a *Terry stop* for determining the reasonableness of electronic surveillance under *FISA* where American persons are involved, this dissertation has outlined the limitations of *Terry* and instead advocated the use of the Canadian *Oakes test* as a model for achieving a more rigorous form of proportionality test.

The modified Oakes test as presented in Chapter 7 balances the contractarian concerns – that is the importance of the right being infringed, against the utilitarian concerns – that is the Government's need for limitation of the right in instances where a lack of limitation has the potential for great harm. If the courts were to apply such a test in cases involving Fourth Amendment concerns in the area of electronic surveillance, I am quite certain that the application would be instructive to both the executive and legislative branches in their lawmaking. Indeed, it would be desirable not least of all because it would permit them to engage in a balancing of public security and private rights that is not simply utilitarian. The application of such a test works best if it is applied at the point where lawmakers are actually engaged in the drafting of

legislation. At this stage, lawmakers can test to see if their legislation is indeed proportional before it reaches a stage where the courts are asked do so for them in a constitutional legal challenge. The potential for this kind of proportionality test is of course not limited to *FISA* alone. Although such a standard would no doubt have been useful in the early *Patriot Act* challenges, the introduction of such a standard at the present time would provide all three branches with a tool for assessing whether any potential override or limitation upon protected a right is indeed permissible under the Constitution and ethically based.

Contribution to the Information Studies Literature

With the introduction of the *Patriot Act*, there was a great deal of concern amongst library and information professionals regarding the impact that this legislation would have on privacy rights in America. Professional associations like the American Library Association were quick to link the potential threat the act posed to patron privacy with new threats to intellectual freedom, freedom to read, and freedom of expression.[286] These concerns were echoed in the scholarly information studies literature from an information policy perspective.[287] One of the gaps that was apparent in the literature (both professional and scholarly) was any discussion of the ethical issues involved. In conducting the literature review for this dissertation it became clear to me that the bulk of the literature (both in information studies and in other disciplines) focused on the debate surrounding liberty versus security from either a political or legal angle. Work written from the political angle reflected a simple utilitarian calculus that paid insufficient attention to

[286] American Library Association. "Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users" January 29, 2003. <http://www.ala.org/template.cfm?section=ifresolutions&template=/contentmanagement/contentdisplay.cfm&contentid=11891>.

[287] The works of authors such as Paul T. Jaeger, John Carlo Bertot, Charles R. McClure, Katherine Coolidge, and Priscilla M. Regan who have been cited throughout the dissertation were among the first to address these issues in the professional literature.

the question of rights. Work written from the legal angle paid insufficient attention to the common good. In answering my research question concerning limits of government intrusion upon privacy rights, it was important to find some way of balancing Fourth Amendment rights against legitimate national security concerns in a manner that respects both utilitarian and contractarian (rights-based) ethical concerns.

Challenges and Limitations of Information Ethics Research

There are many challenges in conducting research in the field of information ethics. In selecting to conduct this research on U.S. foreign intelligence surveillance, it became evident that this issue could be examined through the different branches of ethics: meta-ethical, normative and applied; and that within each of these branches it could be examined using a variety of different ethical approaches. This research is focused on the combination of two specific normative ethical approaches because of their common application to U.S. foreign intelligence surveillance, but that is not to say that other approaches, such as Etzioni's Communitarian approach or a Kantian rules based approach, among others, could not have been used to conduct the same study. However, as stated in Chapter 3, these approaches seemed insufficient to the task of trying to reconcile what appeared to be competing interests in the 'liberty versus security' debate surrounding U.S. foreign intelligence surveillance. That said, the decision to focus on utilitarian and contractarian approaches in this research was not arbitrary. Given the way in which this debate was framed in the media, and the arguments being presented by the Government, special interest groups and scholars, it was important to try to acknowledge these competing claims. The idea of a proportionality test as a means for addressing the reasonableness of U.S. foreign intelligence surveillance is very appealing; however the test offered by the decision in *Terry v.*

Ohio is not without its limitations. Upon closer examination this test does not adequately address the contractarian ethical concerns as laid out in Chapter 7. In seeking to address both the utilitarian and contractarian concerns I opted to use the Canadian *Oakes test* because of my own familiarity with it as a Canadian. That is not suggest that there are no other jurisdictions outside Canada that have proportionality tests which address both concerns - the *Oakes test* itself was inspired by German legal doctrine. [288]

In choosing to focus my attention in the dissertation on three case studies (The *Patriot Act*, the Terrorist Surveillance Program, and the amendments to *FISA* that resulted from the *Protect America Act of 2007* and the *FISA Amendments Act of 2008*) there is also the potential challenge that the results of my study may be limited in their applicability to other case studies or to other jurisdictions. Although I concede that the details of these American examples are unique to that country and came about as a result of the September 11th attacks on that country, the use of a proportionality test which combines utilitarian and contractarian principles, such as the *Oakes test* (a Canadian legal test), is one which I believe has application beyond the case studies examined for this dissertation.

Lastly, in writing about the post 9/11 period, I am well aware that my research area is highly political. Throughout my study I have tried to be mindful of the fact that the legal, political and ethical criticisms I raise in my case examples could be viewed as being the product of bias. I have tried throughout my research to mitigate this through the development of an ethical framework that is based on a proportionality test that takes into account both the contractarian

[288] Christoffersen, Jonas. Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights. Leiden, Netherlands: Martinus Nijhoff, 2009. p. 71.

and utilitarian ethical concerns which shaped the 'liberty versus security' debate. It is my hope that this approach has resulted in a balanced examination of the ethical issues involved in the three case examples studied.

Directions for Future Research

The ethical framework used in this dissertation could act as a guide to future research for a host of applied issues in information policy where there is a clear tension between individual civil liberties and the collective good of society. Contemporary issues regarding U.S. airport passenger screening, would be a natural extension of this research given the similar tensions between individual civil liberties and the need for protecting national security. The Transport Security Agency's (TSA) introduction of full body imaging scanners, which show images of bodies through their clothes to reveal any hidden objects that might pose a threat to security, has alarmed civil liberties groups and resulted in a wave of complaints from air travelers, sparking a public debate over whether the measures have gone too far in their attempts to thwart potential terrorist attacks.[289]

Additional areas of application could include, but are not limited to: racial and ethnic profiling (particularly of individuals of middle eastern origin) since September 11th; the use of data mining to determine patterns of behaviour through purchase and other transaction records in an effort to combat terrorism;[290] and access to government information (especially in light of information that has been reclassified and is no longer publicly available due to security concerns),[291] to

[289] New York Times. "Do Body Scanners Go too Far?" November 23, 2010. http://www.nytimes.com/roomfordebate/2010/11/22/do-body-scanners-make-us-safer
[290] Leslie, Neil Richard. "Privacy, Biometrics and Terrorism," Atlantic Council, October 8, 2008.
[291] American Library Association. "House Subcommittee Blasts Document Reclassification," June 30, 2006.

name but a few areas where individual rights and national security interests have come into conflict.

http://www.ala.org/ala/alonline/currentnews/newsarchive/2006abc/march2006ab/narahearing.cfm

Works Cited

ACLU v. Nat'l Sec. Agency / Central Sec. Serv., 438 F. Supp. 2d 754, 2006 U.S. Dist. LEXIS 57338 (2006).

ACLU v. NSA, 493 F.3d 644, 2007 U.S. App. LEXIS 16149 (6th Cir.) (6th Cir. Mich., 2007).

ACLU v. NSA/Central Sec. Serv., 467 F.3d 590, 2006 U.S. App. LEXIS 32346 (6th Cir., 2006).

American Civil Liberties Union. "ACLU Blasts Justice Department's Attempts to Manipulate Truth About PATRIOT Act Ruling." October 1, 2004. <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16631&c=282>.

---. "ACLU: National Security Letters." <http://www.aclu.org/safefree/nationalsecurityletters/index.html>.

---. "In ACLU Case, Federal Court Strikes Down PATRIOT Act Surveillance Power As Unconstitutional." September 29, 2004. <http://www.aclu.org/safefree/spying/18589prs20040929.html>.

---. "Secure Flight Re-Engineering Welcomed but Watchlist Problems Remain Unaddressed. " October 22, 2008. <http://www.aclu.org/technology-and-liberty/secure-flight-re-engineering-welcomed-watchlist-problems-remain-unaddressed>.

---. "Surveillance Under the USA PATRIOT Act " April 3, 2003. <http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=12263&c=206>.

American Library Association. "House Subcommittee Blasts Document Reclassification," June 30, 2006. <http://www.ala.org/ala/alonline/currentnews/newsarchive/2006abc/march2006ab/naraheari ng.cfm>

---."Resolution on the USA Patriot Act and Related Measures That Infringe on the Rights of Library Users." January 29, 2003. <http://www.ala.org/template.cfm?section=ifresolutions&template=/contentmanagement/contentdisplay.cfm&contentid=11891>.

Baker, James E. In the Common Defence: National Security Law in Perilous Times . Cambridge: Cambridge University Press, 2007.

Banks, Christopher P. "Protecting (Or Destroying) Freedom through Law." American National Security and Civil Liberties in an Era of Terrorism. Ed. David B. Cohen and John W. Wells. New York: Palgrave Macmillan, 2004.

Barbour, Ava. "Ready…aim…FOIA! A Survey of the Freedom of Information Act in the Post-9/11 United States." The Boston Public Interest Law Journal 13 (2004): 203.

Baxter, Pamela, and Susan Jack. "Qualitative Case Study Methodology: Study Design and Implementation for Novice Researchers. ." The Qualitative Report 13.4 (2008): 544.

Belt, Dave. "Domestic security: The homefront and the war on terror for." The NewsHour (PBS). March 27, 2006. <http://www.pbs.org/newshour/indepth_coverage/terrorism/homeland/patriotact.html>.

Benton, Robert J. "Political Expediency and Lying: Kant vs Benjamin Constant." Journal of the History of Ideas . 43.1 (Jan. - Mar., 1982), 135.

Blum, Stephanie Cooper. "What really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future Surveillance Reform." Boston University Public Interest Law Journal 18 (2008): 269.

---. "What really is at Stake with the FISA Amendments Act of 2008 and Ideas for Future

Surveillance Reform " Boston University Public Interest Law Journal 18 (2009): 269.

Bradley, Alison A. "Extremism in the Defense of Liberty? the Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT Act." Tulane Law Review 77 (2002): 465.

Breglio, Nola K. "Leaving FISA Behind: The Need to Return to Warrantless Foreign Intelligence Surveillance." Yale Law Journal 113 (2003): 179.

Breinholt, Jeff. "How about A Little Perspective: The USA PATRIOT Act and the Uses and Abuses of History." Texas Review of Law & Politics 9 (2004): 17.

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982*, (U.K.) 1982, c. 11.

Cauley, Leslie. "NSA has massive database of Americans' phone calls." May 11, 2006. <http://www.usatoday.com/news/washington/2006-05-10-nsa_x.htm>.

Christoffersen, Jonas. Fair Balance: Proportionality, Subsidiarity and Primarity in the European Convention on Human Rights. Leiden, Netherlands: Martinus Nijhoff, 2009.

Cole, David. "Enemy Aliens and American Freedoms." September 5, 2005. <http://www.thenation.com/doc/20020923/cole>.

Congressional Record(Extensions). "FISA Amendments Act of 2008." June 26, 2008. <http://www.fas.org/irp/congress/2008_cr/h062608.html>.

Congressional Record(House). "FISA Amendments Act of 2008." June 20, 2008. <http://www.fas.org/irp/congress/2008_cr/house-fisa.html>.

Congressional Record(Senate). "FISA Amendments Act of 2008." June 24, 2008. <http://www.fas.org/irp/congress/2008_cr/fisa062408b.html>.

---. "Foreign Intelligence Surveillance Amendments Act of 2008." July 8, 2008. <http://www.fas.org/irp/congress/2008_cr/fisa070808.html>.

Congressional Research Service. "CRS Report for Congress: The USA PATRIOT Act: A Legal Analysis." CRS Report for Congress. April 2002. <http://www.fas.org/irp/crs/RL31377.pdf>.

---. "National Security Letters in Foreign Intelligence Investigations: A Glimpse of the Legal Background and Recent Amendments." CRS Report for Congress. September 8, 2009. <http://www.fas.org/sgp/crs/intel/RS22406.pdf>.

Congressman Silvestre Reyes TX. "Rep. Reyes released a statment on the bipartisan compromise on H.R. 6304, the Foreign Intelligence Surveillance Act (FISA) Amendments of 2008." Jun 19, 2008. <http://reyes.house.gov/News/DocumentSingle.aspx?DocumentID=110549>.

Coolidge, Katherine K. "Baseless Hysteria: The Controversy between the Department of Justice and the American Library Association Over the USA PATRIOT Act." American Association of Law Libraries Law Library Journal 97 (Winter 2005): 7.

Copeland, Rebecca A. "War on Terrorism Or War on Constitutional Rights? Blurring the Lines of Intelligence Gathering in Post-September 11 America." Texas Tech Law Review 35.1 (2004): 1.

C-Span. "Capital News: House of Representatives to go into closed session tonight to discsuss classified FISA information." March 13, 2008. <http://www.youtube.com/watch?v=kB-JGqDukbY>.

D'Agostino, Fred. "Contemporary Approaches to the Social Contract." Stanford Encyclopedia of Philosophy. September 5 2008. <http://plato.stanford.edu.proxy.library.carleton.ca/entries/contractarianism-contemporary/>.

Democracy Now. "Change Player Size Exclusive: Bush's Law: Eric Lichtblau on Exposing the

NSA's Warrantless Wiretapping Program and How the White House Pressured the New York Times to Kill the Story." <http://www.democracynow.org/2008/4/1/exclusivebushs_law_eric_lichtblau_on_exposing>.

"Department of Justice: Fact Sheet overview of information sharing initiative in the war on terrorism." Federation of American Scientists. 2002. <http://www.fas.org/irp/agency/doj/fs091902.html>.

Department of Justice. Office of the Inspector General. Special Report. A Review of the Federal Bureau of Investigation's Use of National Security Letters (Unclassified). (March 2007) <http://www.justice.gov/oig/special/s0803b/final.pdf>.

Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004).

Doe v. Gonzales 500 F. Supp. 2d 379 (2007).

Doe v. Mukasey, 2008 U.S. App. LEXIS 25193 (2d Cir. N.Y., Dec. 15, 2008).

Dowley, Michael F. "Government Surveillance Powers Under the USA PATRIOT Act: Is it Possible to Protect National Security and Privacy at the Same Time? A Constitutional Tug-of-War." Suffolk University Law Review 36 (2002): 165.

Drinkard, Jim. "Verizon says it isn't giving call records to NSA." USA Today. May 16, 2006. <http://www.usatoday.com/news/washington/2006-05-16-verizon-nsa_x.htm>.

Edgar, Stacey L. Morality and Machines: Perspectives on Computer Ethics. Sudbury, Mass: Jones and Bartlett Publishers, 2002, p. 58 - 59

Edgar, Timothy, and Witold Walczak. "Perspectives on the USA PATRIOT Act: We can be both Safe and Free: How the PATRIOT Act Threatens Civil Liberties." Pennsylvania Bar Association Quarterly 76 (2005): 21.

Eggen, Dan. "Judge Invalidates PATRIOT Act Provisions: FBI Is Told to Halt Warrantless Tactic." The Washington Post. September 7, 2006. <http://www.washingtonpost.com/wp-dyn/content/article/2007/09/06/AR2007090601438.html>.

Eggen, Dan, and Paul Kane. "Gonzales Hospital Episode Detailed: Ailing Ashcroft Pressured on Spy Program, Former Deputy Says." The Washington PostMay 16, 2007: A01.

---. "Gonzales, Senators Spar on Credibility Account of Meeting In '04 Is Challenged" The Washington Post Wednesday, July 25, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/07/24/AR2007072400207.html>.

Electronic Frontier Foundation. "NSA Multi-District Litigation." December 8, 2009. <http://www.eff.org/cases/att>.

Etzioni, A. How Patriotic is the Patriot Act?: Freedom Versus Security in the Age of Terrorism. New York: Routledge, 2004.

---. Rights and the Common Good: The Communitarian Perspective. New York: St. Martin's Press., 1995.

"Fact Sheet : The Protect America Act."White House. August 7, 2007. <http://www.whitehouse.gov/news/releases/2007/08/20070806-5.html>.

FISA Amendments Act of 2008 Public Law110-261.

Ford v. Quebec (Attorney General), [1988] 2 S.C.R. 712.

Foreign Intelligence Surveillance Act of 1978, Public Law 95-511, 92 Stat. 1783, 50 U.S.C. ch. 36 s. 1566.

Goldsmith, Jack. The Terror Presidency: Law and Judgment Inside the Bush Administration. New York: Norton, 2007.

Government Printing Office. "The President's Radio Address." December 17, 2005. <http://fdsys.gpo.gov/fdsys/pkg/WCPD-2005-12-26/html/WCPD-2005-12-26-Pg1880.htm>.

Gregor, Mary. Groundwork of the Metaphysics of Morals / Immanuel Kant. Trans. Mary Gregor. Cambridge: Cambridge University Press, 1998.

Gross, Emanuel. "The Struggle of a Democracy Against Terrorism – Protection of Human Rights: The Right to Privacy Versus the National Interest - the Proper Balance." Cornell International Law Journal 37 (2004): 27.

Hayden, Michael V. "Balancing Security and Liberty: The Challenge of Sharing Foreign Signals Intelligence." Notre Dame Journal of Law, Ethics & Public Policy 19 (2005): 247.

Henry, Ed and Ahlers, Mike. "Kennedy: Airline security risk? Senator tells of Screening Stops at Airport." CNN. August 19, 2004. <http://www.cnn.com/2004/ALLPOLITICS/08/19/kennedy.airlines/index.html>.

Hersh, Seymour. "National Security Dept. Listening In." The New Yorker. <http://www.newyorker.com/archive/2006/05/29/060529ta_talk_hersh>.

Heymann, Philip B. "Civil Liberties and Human Rights in the Aftermath of September 11." Harvard Journal of Law & Public Policy 25.2 (2002): 441.

Homeland Security. Press Release. "TSA to Assume Watch List Vetting with Secure Flight Program" October 22, 2008. <http://www.dhs.gov/xnews/releases/pr_1224686539438.shtm>.

Hosenball, Mark. "Spying: Giving Out U.S. Names: National Security Agency's Release of

Names of Americans on "Intercept" List." Newsweek May 2, 2006: 10.

Huhn, Wilson R. "Congress has the Power to Enforce the Bill of Rights Against the Federal Government; therefore FISA is Constitutional and the President's Terrorist Surveillance Program is Illegal." William & Mary Bill of Rights Journal 16 (2007): 537.

Human Rights Watch. "Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees." United States Report 14.4 (G). (August 2002) <http://www.hrw.org/reports/2002/us911/USA0802.pdf>.

"In ACLU Case, Federal Court Strikes Down PATRIOT Act Surveillance Power As Unconstitutional." American Civil Liberties Union. September 29, 2004. <http://www.aclu.org/safefree/spying/18589prs20040929.html>.

Irwin Toy Ltd. v. Quebec (Attorney general), [1989] 1 S.C.R. 927.

Jaeger, Paul T., et al. "The USA PATRIOT Act, the Foreign Intelligence Surveillance Act, and Information Policy Research in Libraries: Issues, Impacts and Questions for Libraries and Researchers." Library Quarterly 74.2 (2004): 99.

Kris, David. "A Guide to the New FISA Bill, Part I." Balkinization. June 21, 2008. <http://balkin.blogspot.com/2008/06/guide-to-new-fisa-bill-part-i.html>.

Leslie, Neil Richard. "Privacy, Biometrics and Terrorism." Atlantic Council. October 8, 2008. http://www.acus.org/new_atlanticist/biometrics-civil-liberties-and-war-against-terror

Lichtblau, Eric. "Telecom Companies Win Dismissal of Wiretap Suits." New York Times. June 4, 2009. <http://www.nytimes.com/2009/06/04/us/politics/04nsa.html>.

Lichtblau, Eric, and David Johnston. "Court to Oversee U.S. Wiretapping in Terror Cases." New York Times. January 18, 2007. <http://www.nytimes.com/2007/01/18/washington/18intel.html>.

Lichtblau, Eric. Bush's Law: The Remaking of American Justice . New York: Pantheon, 2008.

---. "Judges on Secretive Panel Speak Out on Spy Program." New York Times. March 29, 2006. <http://www.nytimes.com/2006/03/29/politics/29nsa.html>.

Locke : Political Essays. Ed. Mark Goldie. Cambridge: Cambridge University Press, 1997.

Manfredi, C. P., & Rush, M. E. (2008). *Judging democracy*. Peterborough, Ont: Broadview Press.

Michaels, Jon D. "All the President's Spies: Private-Public Intelligence Partnerships in the War on Terror." California Law Review 96: 901.

Mill, John Suart. On Liberty. Ed. Alan S. Kahan. Boston: St. Martins, 2008.

---. Utilitarianism. Buffalo, N.Y.: Prometheus Books, 1987.

Nakashima, Ellen and Hsu, Spencer S. "Democrats Offer Compromise Plan On Surveillance; Proposal Would Involve FISA Court in Warrants." Washington Post. August 2, 2007. <http://www.washingtonpost.com/wp-dyn/content/article/2007/08/01/AR2007080101514.html?nav=emailpage>.

New York Times. "Do Body Scanners Go too Far?" November 23, 2010. http://www.nytimes.com/roomfordebate/2010/11/22/do-body-scanners-make-us-safer

---."Transcipt of President's Weekly Radio Address: Bush on the Patriot Act and Eavesdropping." December 18, 2005. <http://query.nytimes.com/gst/fullpage.html?res=9A05E6D61630F93BA25751C1A9639C8B63>.

Nussbaum, Martha. Frontiers of Justice: Disability, Nationality, Species Membership. Cambridge, MA: Harvard University Press, 2006.

Office of the Press Secretary. "President Bush: Information Sharing, PATRIOT Act Vital to

Homeland Security." Remarks by the President in a Conversation on the USA Patriot Act, Kleinshans Music Hall, Buffalo, New York." April 20, 2004. <http://www.whitehouse.gov/news/releases/2004/04/20040420-2.html>.

Online Transcript. "Gonzales Discusses Patriot Act: U.S. Attorney General Wrote Op-Ed in Today's Post." December 14, 2005. <http://www.washingtonpost.com/wp-dyn/content/discussion/2005/12/13/DI2005121301425.html>.

Orwell, George. Nineteen Eighty-Four. New York: Harcourt, 1949.

PBS. "Frontline: Spying on the Home Front (streamed video) " 2007. <http://www.pbs.org/wgbh/pages/frontline/homefront/>.

Pillard, Cornelia T. L. "The Unfulfilled Promise of the Constitution in the Executive Hands." Michigan Law Review 103 (2005): 676.

Politicstv. "Gonzales: Pressured Hospitalized Ashcroft to OK Spying (Testimony of James Comey before the Senate Judiciary Committee." May 15, 2007. <http://www.youtube.com/watch?v=hxHjWYA50Ds>.

Poluka, Joseph G., "The Patriot Act: Indispensable tool against Terror." Pennsylvania Bar Association Quarterly 76 (2005):33.

Posner, Richard A. "Privacy, Surveillance, and Law." University of Chicago Law Review 75 (2008): 245.

Protect America Act of 2007 Public Law 110-55.

R. v. Butler, [1992] 1 S.C.R. 452.

R. v. Keegstra, [1996] 1 S.C.R. 458.

R. v. Oakes, [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200.

R. v. Sharpe, 2001 SCC 2, [2001] 1 S.C.R. 45.

Rawls, John. A Theory of Justice. Cambridge, Mass: Belknap Press, 2005 reprint of 1971 edition.

"Recent Legislation: Electronic Surveillance - Congress Grants Telecommunications Companies Retroactive Immunity from Civil Suits for Complying with NSA Terrorist Surveillance Program. - FISA Amendments Act of 2008, Pub. L. no. 110-261, 122 Stat. 2436. " Harvard Law REview 122 (2009): 1271.

Regan, Priscilla M. "Old Issues, New Context: Privacy, Information Collection, and Homeland Security." Government Information Quarterly 21.4 (2004): 481.

Risen, James. "Bush Signs Law to Widen Reach for Wiretapping." The New York Times. August 6, 2007. <http://www.nytimes.com/2007/08/06/washington/06nsa.html>.

Risen, James, and Eric Lichtblau. "Bush Lets U.S. Spy on Callers Without Courts." December 16, 2005. <http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089>.

---. "Bush Lets U.S. Spy on Callers Without Courts." The New York Times. December 16, 2005. <http://www.nytimes.com/2005/12/16/politics/16program.html?ex=1292389200&en=e32070e08c623ac1&ei=5089>.

---. "Court Affirms Wiretapping Without Warrants " The New York Times. January 16, 2009. <http://www.nytimes.com/2009/01/16/washington/16fisa.html>.

Samek, Toni. Librarianship and Human Rights: A Twenty-First Century Guide. Oxford: Chandos, 2007.

Savage, Charlie. "New law expands power to wiretap - Diminishes oversight of NSA spy program." The Boston Globe. August 6, 2007.

<http://www.boston.com/news/nation/washington/articles/2007/08/06/new_law_expands_power_to_wiretap/>.

Seamon, Richard Henry. "Domestic Surveillance for International Terrorists: Presidential Power and Fourth Amendment Limits." Hastings Constitutional Law Quarterly 35: 449.

Senator Patrick Leahy (D-Vt.). "Closing Statement Of Sen. Patrick Leahy (D-Vt.), Chairman, Senate Judiciary Committee, On Senate Consideration Of The FISA Amendments Act Of 2008." July 9, 2008. <http://leahy.senate.gov/press/200807/070908b.html>.

Singel, Ryan. "Whistle-Blower Outs NSA Spy Room." Wired. April 7, 2006. <http://www.wired.com/science/discoveries/news/2006/04/70619>.

Singleton, Solveig. "Privacy and Twenty-First Century Law Enforcement: Accountability for New Techniques." Ohio Northern University Law Review 30 (2004): 417.

Slobogin, Christopher. Privacy at Risk: The New Government Surveillance and the Fourth Amendment. Chicago: University of Chicago Press., 2007.

Smart, J. J. C. "Extreme and Restricted Utilitarianism." Theories of Ethics. Ed. Philippa Foot. Oxford: Oxford University Press, 1967.

Stolz, Barbara Ann. "The Foreign Intelligence Surveillance Act of 1978: The Role of Symbolic Politics." Law & Policy 24.3 (2002): 269.

Sullivan, Jennifer L. "From 'the Purpose' to 'a Significant Purpose': Assessing the Constitutionality of the Foreign Intelligence Surveillance Act Under the Fourth Amendment." Notre Dame Journal of Law, Ethics & Public Policy 19 (2005): 379.

Swain, Laura Taylor. "Liberty in the Balance: The Role of the Third Branch in a Time of Insecurity." Suffolk University Law Review 37 (2004): 51.

Taipale, K. A. "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance." Yale

Journal of Law & Technology 9 (2007): 128.

---. "The Ear of Dionysus: Rethinking Foreign Intelligence Surveillance." Yale Journal of Law & Technologyle Journal of 9 (2007): 128.

Terry v. Ohio, 392 U.S. 1 (1968).

The Library of Congress Thomas. "Bill Summary and Status: 110th Congress (2007-2008) H.R.6304 CRS Summary." July 10, 2008. <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR06304:@@@D&summ2=m&>.

The Washington Post. "Transcript: U.S. Senate Judiciary Committee Holds a Hearing on Wartime Executive Power and the NSA's Surveillance Authority." February 6, 2006. <http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020600931.html>.

U.S. Senator Russ Feingold Wisconsin. "Remarks of U.S. Senator Russ Feingold in Opposition to the FISA Amendments Act " July 9, 2008. <http://feingold.senate.gov/record.cfm?id=306014>.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT) Act of 2001. Public Law 107-56, § 214(a)(1), 115 Stat. 272, 286 (Amending 50 U.S.C. § 1842(a)(1) (2000)).

Warren, Samuel, and Louis D. Brandeis. "The Right to Privacy." Harvard Law Review 4 (1890): 193.

White House Press Release. "Fact Sheet: Retroactive Liability Protection Is Critical to Our National Security." July 8, 2008. <http://www.usdoj.gov/archive/ll/docs/fisa-factsheet-070808.pdf>.

---. "Speech by President Bush after he signs H.R. 6304, FISA Amendments Act of 2008." July

10, 2008. <http://georgewbush-whitehouse.archives.gov/news/releases/2008/07/20080710-2.html>.

White House. "Transcript: President Bush Discusses the Protect America Act of 2007." Sept. 19, 2007. <http://georgewbush-whitehouse.archives.gov/news/releases/2007/09/20070919.html>.

Wolfson, Stephen Manuel. "National Security Surveillance and National Authentication System: The NSA, AT&T, and the Secrets of Room 641A." I/S: A Journal of Law & Policy for the Information Society 3 (2008): 411.

Wong, Katherine. "The NSA Terrorist Surveillance Program." Harvard Journal of Law & Public Policy 43 (2006): 517.

Zetter, Kim. "'John Doe' Who Fought FBI Spying Freed From Gag Order After 6 Years" in Wired. August 10, 2010. <http://www.wired.com/threatlevel/2010/08/nsl-gag-order-lifted/#ixzz0wcPM40Dg>.

APPENDICES

The following appendices are a compilation of the actual Congressional Research Service Legislative Summaries provided to Congress. For lengthier legislative summaries, only selected sections have been included where the text of the legislation is specifically relevant to the issues discussed in this dissertation. The Case Summaries provided have been obtained through the Canadian Legal Information Institute (CanLII) and the Legal Information Institute (LII) databases. Both CanLII and LII are non-profit organizations which strive to make legal information freely available to the public via the Internet in their respective countries: Canada and the U.S.

Appendix A.

The U.S.A. PATRIOT ACT of 2001:

The following is a list of selected sections as referenced in this dissertation, with annotations courtesy of the Congressional Research Service Legislative Summaries:

(Sec. 214) Prohibits use of a pen register or trap and trace devices in any investigation to protect against international terrorism or clandestine intelligence activities that is conducted solely on the basis of activities protected by the first amendment to the U.S. Constitution.

(Sec. 215) Authorizes the Director of the FBI (or designee) to apply for a court order requiring production of certain business records for foreign intelligence and international terrorism investigations. Requires the Attorney General to report to the House and Senate Intelligence and Judiciary Committees semi-annually.

(Sec. 412) Provides for mandatory detention until removal from the United States (regardless of any relief from removal) of an alien certified by the Attorney General as a suspected terrorist or threat to national security. Requires release of such alien after seven days if removal proceedings have not commenced, or the alien has not been charged with a criminal offense. Authorizes detention for additional periods of up to six months of an alien not likely to be deported in the reasonably foreseeable future only if release will threaten U.S. national security or the safety of

the community or any person. Limits judicial review to habeas corpus proceedings in the U.S. Supreme Court, the U.S. Court of Appeals for the District of Columbia, or any district court with jurisdiction to entertain a habeas corpus petition. Restricts to the U.S. Court of Appeals for the District of Columbia the right of appeal of any final order by a circuit or district judge.

(Sec. 505) Allows the FBI to request telephone toll and transactional records, financial records, and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities only if the investigation is not conducted solely on the basis of activities protected by the first amendment to the U.S. Constitution.

The Library of Congress Thomas. "Bill Summary and Status-107th Congress (2001-2002) HR 3162 CRS Summary." October 24, 2001. <http://thomas.loc.gov/cgi-bin/bdquery/z?d107:HR03162:@@@D&summ2=m&>.

Appendix B.

The Protect America Act of 2007:

The following legislative summary is courtesy of the Congressional Research Service Legislative Summaries:

Amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to state that nothing under its definition of "electronic surveillance" shall be construed to encompass surveillance directed at a person reasonably believed to be located outside the United States. Allows the Director of National Intelligence (DNI) and the Attorney General (AG), for periods up to one year, to authorize the acquisition of foreign intelligence information concerning persons outside the United States if the DNI and AG determine that: (1) there are reasonable procedures in place for determining that such acquisition concerns persons outside the United States, and such procedures will be subject to review by the Foreign Intelligence Surveillance Court (Court); (2) the acquisition does not constitute electronic surveillance; (3) the acquisition involves obtaining foreign intelligence information from or with the assistance of a communication service provider or other person who has access to communications; (4) a significant purpose of the acquisition is to obtain foreign intelligence information; and (5) the minimization procedures (procedures to ensure the smallest level of privacy intrusion while obtaining such information) to be used meet the definition of minimization procedures under FISA. Requires such determination to be certified and submitted to the Court.

Requires the AG to report to: (1) the Court the procedures by which the Government determines that such acquisitions do not constitute electronic surveillance; and (2) the congressional intelligence and judiciary committees semiannually concerning acquisitions made during the previous six-month period. Terminates this Act 180 days after its enactment. Makes authorizations for the acquisition of information made by this Act, and directives issued pursuant to such authorizations, effective until their expiration.

The Library of Congress Thomas. "Bill Summary and Status: 110th Congress (2007-2008) S.1927 CRS Summary." August 5, 2007. <*http://thomas.loc.gov/cgi-bin/bdquery/z?d110:SN01927:@@@D&summ2=m&*>.

Appendix C.

USA PATRIOT Improvement and Reauthorization Act of 2005

The following is a list of selected sections courtesy of the Congressional Research Service Legislative Summaries:

Title I: USA PATRIOT Improvement and Reauthorization Act - (Sec. 102) Repeals the sunset date for (thus making permanent) the surveillance provisions of the USA PATRIOT Act, with the following exceptions. Provides for a four-year extension (through December 31, 2009) of provisions: (1) granting roving surveillance authority under the Foreign Intelligence Surveillance Act of 1978 (FISA) where the Court finds that the actions of the target may thwart the identification of a specified person; and (2) authorizing the Director of the Federal Bureau of Investigation (FBI) to apply for a court order requiring production of tangible things (including books, records, papers, and documents) for foreign intelligence and international terrorism investigations.

(Sec. 103) Amends the Intelligence Reform and Terrorism Prevention Act of 2004 to: (1) extend for four years (through December 31, 2009) provisions revising the definition of an "agent of a foreign power" to include any non-U.S. person who engages in international terrorism or preparatory activities (thus permitting issuance of FISA orders targeting such persons without a showing that they are members or agents of a terrorist group or a foreign power ["lone wolf" provision]); and (2) repeal the sunset date for provisions setting forth additions to the offense of providing material support to terrorists.

(Sec. 105) Amends FISA to apply provisions governing the duration of an order for electronic surveillance or a physical search to surveillance targeted against a foreign power who is not a U.S. person. Limits to one year an order (or extension) for the use of pen registers and trap and trace devices where the applicant has certified that the information likely to be obtained is foreign intelligence information not concerning a U.S. person.

(Sec. 106) Amends the FISA provisions governing orders for the production of tangible things to authorize the Director of the FBI to delegate to the Deputy Director or the Executive Assistant Director for National Security the authority to make an application for such an order involving library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person. Requires an application for such an order to: (1) include a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation; (2) include an enumeration of minimization procedures adopted by the Attorney General that are applicable to the retention and dissemination by the FBI of any tangible things produced; and (3) describe the tangible things to be produced with sufficient particularity to permit them to be fairly identified. Sets forth provisions concerning review by a panel of three judges of petitions filed by recipients challenging an order's legality. Requires the Attorney General to report to specified congressional committees annually on requests and order applications for the production of tangible things and semiannually on orders for the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, and medical records that would identify a person.

(Sec. 106A) Directs the Inspector General of the Department of Justice (DOJ) to perform and report to Congress on a comprehensive audit of the effectiveness and use of the investigative authority provided to the FBI under FISA.

(Sec. 107) Requires the Attorney General to submit to the House and Senate Judiciary Committees an annual report containing accounts from which DOJ has received voluntary disclosures of customer communications or records in emergencies involving immediate danger of death or serious physical injury.

(Sec. 108) Requires applications for roving wiretaps to include specific facts. Requires an order approving electronic surveillance where the nature and location are unknown to direct the applicant to provide notice to the court, within 10 days after the surveillance begins, of: (1) the nature and location of each new facility or place at which the electronic surveillance is directed; (2) the facts and circumstances relied upon to justify the belief that such facility is or was being used by the target of the surveillance; (3) any proposed minimization procedures that may be necessitated by a change in the facility; and (4) the total number of electronic surveillances conducted under the authority of the order. Directs the Attorney General to inform the House and Senate Judiciary Committees semiannually concerning electronic surveillance under FISA, including regarding: (1) electronic surveillance orders where the nature and location of each targeted facility are unknown; (2) criminal cases in which information acquired has been authorized for use at trial; and (3) emergency employments of electronic surveillance.
(Sec. 109) Requires the Attorney General to inform such Committees regarding: (1) emergency

physical searches authorized; and (2) pen registers and trap and trace devices authorized on an emergency basis. Requires the Secretary of Homeland Security to report to the Judiciary Committees semiannually on internal affairs operations at U.S. Citizenship and Immigration Services, including regarding investigations conducted.

(Sec. 110) Amends the federal criminal code to rewrite provisions prohibiting acts of destruction and violence against trains, railroad equipment and structures, and the mass transportation system to: (1) correspond with current prohibitions against acts of violence against the mass transportation system; (2) apply such provisions to acts committed knowingly (currently, willfully); (3) cover such acts against passenger vessels; and (4) add as an aggravated offense the commission of such prohibited act under circumstances in which the railroad on-track equipment, passenger vessel, or mass transportation vehicle was carrying high-level radioactive waste, spent nuclear fuel, or specified hazardous material. Prohibits surveilling, photographing, videotaping, diagramming, or otherwise collecting information with the intent to plan specified terrorist acts against mass transportation systems. Provides for the death penalty where the offense results in the death of any person.

(Sec. 111) Provides for the civil forfeiture of any property traceable to proceeds obtained from, or used to facilitate, trafficking in nuclear, chemical, biological, or radiological weapons technology or material.

(Sec. 112) Includes as a predicate offense to a "federal crime of terrorism" a crime related to: (1) military-type training from a foreign terrorist organization; or (2) narco-terrorism.

(Sec. 113) Expands the circumstances under which the interception of wire, oral, or electronic communications is authorized to cover offenses related to: (1) biological weapons; (2) violence at international airports; (3) animal enterprise terrorism; (4) nuclear and weapons of mass destruction threats; (5) explosive materials; (6) possession of weapons in federal facilities; (7) U.S. officers and employees; (8) protection of foreign officials; (9) terrorist attacks against mass transportation; (10) torture; (11) arson within special maritime and territorial jurisdiction; (12) conspiracy to harm persons or property overseas; (13) structuring financial transactions to evade reporting requirements; (14) aircraft piracy; (15) assault on a flight crew with a dangerous weapon; (16) explosive or incendiary devices, or endangerment of human life, by means of weapons on aircraft; (17) aggravated identity theft; and (18) certain antitrust criminal violations.

(Sec. 114) Authorizes the delay of notice of the execution of a search warrant for a reasonable period not to exceed 30 days after execution or until a later date if the facts justify a longer delay. Requires the issuing or denying judge to report to the Administrative Office of the United States Courts regarding warrants authorizing delayed notice or denials of warrants and requires the Director of the Administrative Office to report annually to Congress.

(Sec. 115) Authorizes the recipient of a request for records in connection with an authorized investigation concerning terrorism or clandestine intelligence activities, the Fair Credit Reporting Act (FCRA), the Right to Financial Privacy Act (RFPA), or the National Security Act of 1947 (NSA) (a national security letter) to petition the U.S. district court for the district in which that person or entity does business or resides for an order modifying or setting aside the request. Permits the court to modify or set aside the request if compliance would be unreasonable or

oppressive. Sets forth procedures for petitions for an order modifying or setting aside a nondisclosure requirement imposed in connection with such a request. Authorizes the court to modify or set aside the requirement if it finds that there is no reason to believe that disclosure may endanger U.S. national security, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person. Treats a certification made by the Attorney General, the Director of the FBI, or the head of a federal department that disclosure may endanger national security or interfere with diplomatic relations as conclusive unless the court finds it was made in bad faith. Authorizes the Attorney General to invoke the aid of a U.S. court to compel compliance with a request for information.

(Sec. 116) Prohibits disclosure of such a request if the Director of the FBI certifies that otherwise there may result a danger to U.S. national security, interference with a criminal, counterterrorism, or counterintelligence investigation, interference with diplomatic relations, or danger to the life or physical safety of any person. Requires a person, at the request of the Director of the FBI, to identify the person to whom a disclosure was or will be made.

(Sec. 117) Sets penalties for knowing violations of nondisclosure provisions under the federal criminal code, FCRA, RFPA, or NSA.

(Sec. 118) Directs that any report made to a congressional committee regarding national security letters also be made to the House and Senate Judiciary Committees. Requires the Attorney General to: (1) inform specified other committees semiannually regarding FCRA requests; and

(2) submit to Congress annually an aggregate report on the total number of DOJ requests made concerning U.S. persons.

(Sec. 119) Directs the Inspector General of DOJ to audit and report to the Attorney General and the Director of National Intelligence (DNI) on the use of national security letters issued by DOJ. Directs the Attorney General and DNI to jointly submit to the Judiciary and Intelligence Committees a report on the feasibility of applying minimization procedures in the context of national security letters to ensure the protection of the constitutional rights of U.S. persons.

(Sec. 120) Subjects to forfeiture any domestic or foreign assets of a person engaged in any federal crime of terrorism (currently, in any act of international or domestic terrorism) against the United States, U.S. citizens or residents, or their property.

(Sec. 123) Prohibits interfering with or disabling anyone engaged in the authorized operation of an aircraft or air navigation facility with intent to endanger or with reckless disregard for human safety.

(Sec. 124) Expresses the sense of Congress that government should not investigate an American citizen solely on the basis of the citizen being a member of a nonviolent political organization or engaging in other lawful political activity.

(Sec. 126) Directs the Attorney General to submit to Congress a report on any DOJ initiative that uses or is intended to develop pattern-based data-mining technology.

(Sec. 127) Expresses the sense of Congress that victims of terrorist attacks should have access to forfeited assets.

(Sec. 128) Requires: (1) an ex parte order for a pen register or trap or trace device for foreign intelligence purposes to direct that, upon the applicant's request, the service provider disclose specified information about the customer and the service provided; and (2) the Attorney General to fully inform the House and Senate Judiciary Committees regarding uses of such devices.

The Library of Congress Thomas. "Bill Summary and Status: 109th Congress (2005-2006) H.R. 3199. CRS Summary." March 9, 2006. <http://thomas.loc.gov/cgi-bin/bdquery/z?d109:HR03199:@@@D&summ2=m&>.

Appendix D.

The FISA Amendments Act of 2008

The following legislative summary is courtesy of the Congressional Research Service Legislative Summaries:

Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 or FISA Amendments Act of 2008:

Title I: Foreign Intelligence Surveillance - (Sec. 101) Amends the Foreign Intelligence Surveillance Act of 1978 (FISA) to add a new title concerning additional procedures for acquiring the communications of certain persons outside the United States.

Authorizes the Attorney General (AG) and Director of National Intelligence (DNI) to jointly authorize, for periods up to one year, the targeting (electronic surveillance) of persons located outside the United States in order to acquire foreign intelligence information, under specified limitations, including: (1) prohibiting an acquisition intentionally targeting a person reasonably believed to be outside the United States in order to acquire the communications of a specific person reasonably believed to be inside the United States; and (2) requiring the targeting to be conducted in a manner consistent with the fourth amendment to the Constitution. Requires: (1) certain targeting and minimization procedures to be followed; (2) the AG to adopt guidelines to ensure that such limitations and procedures are followed; (3) the AG to submit such guidelines to the congressional intelligence and judiciary committees and the Foreign Intelligence Surveillance Court (Court) for review; and (4) prior to such targeting, a certification by the AG and DNI as to

the necessity of such targeting and that appropriate procedures and limitations will be followed. Allows the AG and DNI, if immediate targeting is determined to be required due to an emergency situation, to commence such targeting, but to submit the certification within seven days of such determination. Requires all certifications to be submitted to the Court for review.

Authorizes the AG and DNI to direct an electronic communication service provider to: (1) immediately provide the government with all information, facilities, and assistance necessary to accomplish an acquisition; and (2) maintain under security procedures any records concerning such acquisition. Outlines legal procedures with respect to directive challenges, standards for review, enforcement, and appeals. Provides for: (1) judicial review of certifications and targeting and minimization procedures; and (2) review of Court rulings by the Foreign Intelligence Surveillance Court of Review (with certiorari to the Supreme Court). Outlines conditions under which the AG and DNI may, through the Court: (1) replace a targeting acquisition already in effect before the enactment of this Act with an acquisition authorized under this Act; or (2) reauthorize a current acquisition under the procedures and guidelines of this Act. Requires Court maintenance and security of records and proceedings with respect to acquisition applications, orders, appeals, and determinations.

Requires the AG and DNI, at least every six months, to: (1) assess compliance with required targeting and minimization procedures and related guidelines; and (2) submit assessment results to the Court and the intelligence and judiciary committees. Authorizes inspectors general of the Department of Justice (DOJ) and elements of the intelligence community (IC) authorized to acquire foreign intelligence information to review their agency or element's compliance with

such procedures and guidelines and provide review results to the AG, the DNI, and the intelligence and judiciary committees. Requires the head of any IC element conducting an acquisition of foreign intelligence information to annually review such acquisitions and report review results to the Court, the AG, the DNI, and the intelligence and judiciary committees.

Provides Court jurisdiction for approving the targeting of a U.S. person located outside the United States when the acquisition of information is conducted inside the United States. Requires an application for such acquisition to be made by a federal officer (and approved by the AG), and to contain certain requirements, including that the target is believed to be a foreign power or agent, officer, or employee of a foreign power. Provides for judicial review of a Court order approving such an acquisition. Makes approval orders effective for 90 days, with authorized 90-day renewals. Allows the AG to authorize an emergency acquisition of such a target under certain circumstances, including: (1) determining that an emergency exists; (2) informing a Court judge of such determination; and (3) applying within seven days for a Court order authorizing such surveillance. Provides similar Court jurisdiction and outlines similar procedures for the acquisition (and emergency acquisition) by an IC element of a physical search.

Authorizes the: (1) joint applications and concurrent approvals of requests for acquisitions proposed to be conducted both inside and outside the United States; and (2) concurrent authorizations of electronic surveillance and physical searches.

Directs the AG to report semiannually to the intelligence and judiciary committees concerning the implementation of acquisition requirements.

(Sec. 102) States that, other than by express statutory authorization, FISA and the procedures of chapters 119 (Wire and Electronic Communications Interception and Interception of Oral Communications), 121 (Stored Wire and Electronic Communications and Transactional Records Access), and 206 (Pen Registers and Trap and Trace Devices) of the federal criminal code shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

(Sec. 103) Requires the AG to submit semiannually to the intelligence committees copies of any orders of the Court or the Foreign Intelligence Surveillance Court of Review that include significant construction or interpretation of FISA, including any such orders issued during the five-year period before the enactment of this Act. Allows for the redaction of submitted materials for the protection of national security.

(Sec. 104) Revises provisions concerning the application for, and issuance of, Court orders, including provisions concerning paperwork requirements and government officials who may authorize FISA actions.

(Sec. 105) Allows the AG to authorize the emergency employment of electronic surveillance if the AG, among other things: (1) determines that an emergency exists; (2) informs a Court judge of such determination; and (3) applies for a Court order authorizing such surveillance.

(Sec. 107) Provides similar revisions and outlines similar procedures as in sections 104 and 105 above for the emergency employment of physical searches.

(Sec. 108) Requires the AG, after authorizing the installation and use of a pen register or trap and

trace device on an emergency basis, to apply to the Court for an authorization order within seven days (current law requires 48 hours) after the emergency installation and use.

(Sec. 109) Authorizes the Court to sit en banc when: (1) necessary to secure or maintain uniformity of Court decisions; or (2) the proceeding involves a question of exceptional importance.

(Sec. 110) Authorizes the acquisition of foreign intelligence information from an entity not substantially composed of U.S. persons that is engaged in the international proliferation of weapons of mass destruction, or in activities in preparation therefor on behalf of a foreign power.

Title II: Protections for Electronic Communication Service Providers - (Sec. 201) Prohibits any federal or civil action against any person (including an electronic communication service provider or a landlord or custodian) providing surveillance assistance to an IC element if the AG certifies that such assistance was: (1) provided pursuant to an order or directive under FISA; (2) in connection with an intelligence activity authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, and designed to detect or prevent a terrorist attack against the United States; (3) the subject of a written request from the AG or IC element head to the provider indicating that the activity was authorized by the President and determined to be lawful; or (4) not provided. Allows for the judicial review of such certifications. Limits certification disclosure for national security purposes. Prohibits state law preemption of the protections afforded assistance providers under this section. Requires semiannual reports from the AG to the intelligence and judiciary committees on the

implementation of this title.

Title III: Review of Previous Actions - (Sec. 301) Directs the inspectors general of DOJ, the Office of the DNI, the National Security Agency (NSA), the Department of Defense (DOD), and any other IC element that participated in the President's Surveillance Program (a program authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007, and including the program commonly known as the Terrorist Surveillance Program) to: (1) conduct a review of, among other things, the establishment, implementation, product, and use of the product of the Program; and (2) provide an interim and final review report to the intelligence and judiciary committees. Allows for, in conjunction with such reviews, expedited security clearances and the hiring of necessary additional personnel.

Title IV: Other Provisions - (Sec. 401) Provides severability protections for this Act and its amendments.

(Sec. 403) Repeals FISA provisions made inconsistent by provisions of this Act.

(Sec. 404) Outlines transition procedures.

The Library of Congress Thomas. "Bill Summary and Status: 110th Congress (2007-2008) H.R.6304 CRS Summary." July 10, 2008. <http://thomas.loc.gov/cgi-bin/bdquery/z?d110:HR06304:@@@D&summ2=m&>.

Appendix E.

R. v. Oakes, [1986] 1 S.C.R. 103

Case Summary Courtesy CanLII:

Respondent was charged with unlawful possession of a narcotic for the purpose of trafficking, contrary to s. 4(2) of the *Narcotic Control Act*, but was convicted only of unlawful possession. After the trial judge made a finding that it was beyond a reasonable doubt that respondent was in possession of a narcotic, respondent brought a motion challenging the constitutional validity of s. 8 of the *Narcotic Control Act*. That section provides that if the Court finds the accused in possession of a narcotic, the accused is presumed to be in possession for the purpose of trafficking and that, absent the accused's establishing the contrary, he must be convicted of trafficking. The Ontario Court of Appeal, on an appeal brought by the Crown, found that this provision constituted a "reverse onus" clause and held it to be unconstitutional because it violated the presumption of innocence now entrenched in s. 11(*d*) of the *Canadian Charter of Rights and Freedoms*. The Crown appealed and a constitutional question was stated as to whether s. 8 of the *Narcotic Control Act* violated s. 11(*d*) of the *Charter* and was therefore of no force and effect. Inherent in this question, given a finding that s. 11(*d*) of the *Charter* had been violated, was the issue of whether or not s. 8 of the *Narcotic Control Act* was a reasonable limit prescribed by law and demonstrably justified in a free and democratic society for the purpose of s. 1 of the *Charter*.

Held: The appeal should be dismissed and the constitutional question answered in the affirmative.

Per Dickson C.J. and Chouinard, Lamer, Wilson and Le Dain JJ.: Pursuant to s. 8 of the *Narcotic Control Act*, the accused, upon a finding beyond a reasonable doubt of possession of a narcotic, has the legal burden of proving on a balance of probabilities that he was not in possession of the narcotic for the purpose of trafficking. On proof of possession, a mandatory presumption arises against the accused that he intended to traffic and the accused will be found guilty unless he can rebut this presumption on a balance of probabilities.

The presumption of innocence lies at the very heart of the criminal law and is protected expressly by s. 11(*d*) of the *Charter* and inferentially by the s. 7 right to life, liberty and security of the person. This presumption has enjoyed longstanding recognition at common law and has gained widespread acceptance as evidenced from its inclusion in major international human rights documents. In light of these sources, the right to be presumed innocent until proven guilty requires, at a minimum, that: (1) an individual be proven guilty beyond a reasonable doubt; (2) the State must bear the burden of proof; and (3) criminal prosecutions must be carried out in accordance with lawful procedures and fairness.

A provision which requires an accused to disprove on a balance of probabilities the existence of a presumed fact, which is an important element of the offence in question, violates the presumption of innocence in s. 11(*d*). The fact that the standard required on rebuttal is only a balance of probabilities does not render a reverse onus clause constitutional.

Section 8 of the *Narcotic Control Act* infringes the presumption of innocence in s. 11(*d*) of the *Charter* by requiring the accused to prove he is not guilty of trafficking once the basic fact of

possession is proven.

The rational connection test -- the potential for a rational connection between the basic fact and the presumed fact to justify a reverse onus provision -- does not apply to the interpretation of s. 11(*d*). A basic fact may rationally tend to prove a presumed fact, but still not prove its existence beyond a reasonable doubt, which is an important aspect of the presumption of innocence. The appropriate stage for invoking the rational connection test is under s. 1 of the *Charter*.

Section 1 of the *Charter* has two functions: First, it guarantees the rights and freedoms set out in the provisions which follow it; and second, it states explicitly the exclusive justificatory criteria (outside of s. 33 of the *Constitutional Act, 1982*) against which limitations on those rights and freedoms may be measured.

The onus of proving that a limitation on any *Charter* right is reasonable and demonstrably justified in a free and democratic society rests upon the party seeking to uphold the limitation. Limits on constitutionally guaranteed rights are clearly exceptions to the general guarantee. The presumption is that *Charter* rights are guaranteed unless the party invoking s. 1 can bring itself within the exceptional criteria justifying their being limited.

The standard of proof under s. 1 is a preponderance of probabilities. Proof beyond a reasonable doubt would be unduly onerous on the party seeking to limit the right because concepts such as "reasonableness", "justifiability", and "free and democratic society" are not amenable to such a standard. Nevertheless, the preponderance of probability test must be applied rigorously.

Two central criteria must be satisfied to establish that a limit is reasonable and demonstrably justified in a free and democratic society. First, the objective to be served by the measures limiting a *Charter* right must be sufficiently important to warrant overriding a constitutionally protected right or freedom. The standard must be high to ensure that trivial objectives or those discordant with the principles of a free and democratic society do not gain protection. At a minimum, an objective must relate to societal concerns which are pressing and substantial in a free and democratic society before it can be characterized as sufficiently important. Second, the party invoking s. 1 must show the means to be reasonable and demonstrably justified. This involves a form of proportionality test involving three important components. To begin, the measures must be fair and not arbitrary, carefully designed to achieve the objective in question and rationally connected to that objective. In addition, the means should impair the right in question as little as possible. Lastly, there must be a proportionality between the effects of the limiting measure and the objective -- the more severe the deleterious effects of a measure, the more important the objective must be.

Parliament's concern that drug trafficking be decreased was substantial and pressing. Its objective of protecting society from the grave ills of drug trafficking was self-evident, for the purposes of s. 1, and could potentially in certain cases warrant the overriding of a constitutionally protected right. There was, however, no rational connection between the basic fact of possession and the presumed fact of possession for the purpose of trafficking. The possession of a small or negligible quantity of narcotics would not support the inference of trafficking.

Per Estey and McIntyre JJ.: Concurred in the reasons of Dickson C.J. with respect to the

relationship between s. 11(*d*) and s. 1 of the *Charter* but the reasons of Martin J.A. in the court below were adopted for the disposition of all other issues.

R. v. Oakes, [1986] 1 S.C.R. 103, 26 D.L.R. (4th) 200. <http://www.canlii.org/en/ca/scc/doc/1986/1986canlii46/1986canlii46.html>.

Appendix F.

Terry v. Ohio, 392 U.S. 1 (1968)

Case Summary Courtesy LII:

A Cleveland detective (McFadden), on a downtown beat which he had been patrolling for many years, observed two strangers (petitioner and another man, Chilton) on a street corner. He saw them proceed alternately back and forth along an identical route, pausing to stare in the same store window, which they did for a total of about 24 times. Each completion of the route was followed by a conference between the two on a corner, at one of which they were joined by a third man (Katz) who left swiftly. Suspecting the two men of "casing a job, a stick-up," the officer followed them and saw them rejoin the third man a couple of blocks away in front of a store. The officer approached the three, identified himself as a policeman, and asked their names. The men "mumbled something," whereupon McFadden spun petitioner around, patted down his outside clothing, and found in his overcoat pocket, but was unable to remove, a pistol. The officer ordered the three into the store. He removed petitioner's overcoat, took out a revolver, and ordered the three to face the wall with their hands raised. He patted down the outer clothing of Chilton and Katz and seized a revolver from Chilton's outside overcoat pocket. He did not put his hands under the outer garments of Katz (since he discovered nothing in his pat-down which might have been a weapon), or under petitioner's or Chilton's outer garments until he felt the guns. The three were taken to the police station. Petitioner and Chilton were charged with carrying [p2] concealed weapons. The defense moved to suppress the weapons. Though the trial court rejected the prosecution theory that the guns had been seized during a search incident to a

lawful arrest, the court denied the motion to suppress and admitted the weapons into evidence on the ground that the officer had cause to believe that petitioner and Chilton were acting suspiciously, that their interrogation was warranted, and that the officer, for his own protection, had the right to pat down their outer clothing having reasonable cause to believe that they might be armed. The court distinguished between an investigatory "stop" and an arrest, and between a "frisk" of the outer clothing for weapons and a full-blown search for evidence of crime. Petitioner and Chilton were found guilty, an intermediate appellate court affirmed, and the State Supreme Court dismissed the appeal on the ground that "no substantial constitutional question" was involved.

Held:

1. The Fourth Amendment right against unreasonable searches and seizures, made applicable to the States by the Fourteenth Amendment, "protects people, not places," and therefore applies as much to the citizen on the streets as well as at home or elsewhere.

2. The issue in this case is not the abstract propriety of the police conduct, but the admissibility against petitioner of the evidence uncovered by the search and seizure.

3. The exclusionary rule cannot properly be invoked to exclude the products of legitimate and restrained police investigative techniques, and this Court's approval of such techniques should not discourage remedies other than the exclusionary rule to curtail police abuses for which that is not an effective sanction.

4. The Fourth Amendment applies to "stop and frisk" procedures such as those followed here.

(a) Whenever a police officer accosts an individual and restrains his freedom to walk away, he has "seized" that person within the meaning of the Fourth Amendment.

(b) A careful exploration of the outer surfaces of a person's clothing in an attempt to find weapons is a "search" under that Amendment.

5. Where a reasonably prudent officer is warranted in the circumstances of a given case in believing that his safety or that of others is endangered, he may make a reasonable search for weapons of the person believed by him to be armed and dangerous [p3] regardless of whether he has probable cause to arrest that individual for crime or the absolute certainty that the individual is armed.

(a) Though the police must, whenever practicable, secure a warrant to make a search and seizure, that procedure cannot be followed where swift action based upon on-the-spot observations of the officer on the beat is required.

(b) The reasonableness of any particular search and seizure must be assessed in light of the particular circumstances against the standard of whether a man of reasonable caution is warranted in believing that the action taken was appropriate.

(c) The officer here was performing a legitimate function of investigating suspicious conduct

when he decided to approach petitioner and his companions.

(d) An officer justified in believing that an individual whose suspicious behavior he is investigating at close range is armed may, to neutralize the threat of physical harm, take necessary measures to determine whether that person is carrying a weapon.

(e) A search for weapons in the absence of probable cause to arrest must be strictly circumscribed by the exigencies of the situation.

(f) An officer may make an intrusion short of arrest where he has reasonable apprehension of danger before being possessed of information justifying arrest.

6. The officer's protective seizure of petitioner and his companions and the limited search which he made were reasonable, both at their inception and as conducted.

(a) The actions of petitioner and his companions were consistent with the officer's hypothesis that they were contemplating a daylight robbery and were armed.

(b) The officer's search was confined to what was minimally necessary to determine whether the men were armed, and the intrusion, which was made for the sole purpose of protecting himself and others nearby, was confined to ascertaining the presence of weapons.

7. The revolver seized from petitioner was properly admitted into evidence against him, since the

search which led to its seizure was reasonable under the Fourth Amendment.

Affirmed.

Terry v. Ohio, 392 U.S. 1 (1968), Syllabus.

<http://www.law.cornell.edu/supct/html/historics/USSC_CR_0392_0001_ZS.html>.