JICLT
Journal of International Commercial Law and Technology
Vol. 7, Issue 2 (2012)

Privacy & Terrorism Review
Where Have We Come In 10 Years?

Besar Xhelili,
Barrister & Solicitor
Law Society of Upper Canada

Emir Crowne
Barrister & Solicitor
Law Society of Upper Canada
Associate Professor,
University of Windsor Faculty of Law
emir@uwindsor.ca

Abstract: *As a result of terrorist attacks in the United States on September 11 and subsequent attacks on other influential western countries, new laws have been put in place to supposedly be an effective tool to prevent terrorist attacks and conjointly fight the war on drugs. These laws and presidential executive orders have not been without controversy. The Patriot Act will be used as the primary source of legislation in illustrating how in times of fear governments introduce laws, which normally would not be accepted by the general population as a clear invasion of their privacy. In addition, Canada and the United Kingdom's anti-terrorist legislations will be compared with the United States. Money laundering, terrorist anti-terrorist finance, government investigative surveillance, and data mining will be the areas this paper will focus on to illustrate the emerging invasion on privacy for the sake of security. Despite the fact that we are losing our privacy to our fears of danger, a light will be shed as to the effectiveness of these new laws. Case law will be used to illustrate that the courts have been reluctant in invalidating laws that infringe our constitutionally given rights of privacy. Possible alternative measures will be given to deal with acts of terrorism. This paper will argue that privacy rights have seen a shift from its traditional understanding since the recent terrorist attacks on the western governments and that security has taken a primary role; privacy rights have been traded as a commodity in the market by the U.S and to a lesser extent the Canadian government.*

1. Introduction

As a result of terrorist attacks in the United States on September 11 and subsequent attacks on other influential western countries, new laws have been put in place to supposedly be an effective tool to prevent terrorist attacks and conjointly fight the war on drugs. These laws and presidential executive orders have not been without controversy.

This paper will argue that privacy rights have seen a shift from its traditional understanding since the recent terrorist attacks on the western governments and that security has taken a primary role; privacy rights have been traded as a commodity in the market by the U.S and to a lesser extent the Canadian government. The *Patriot Act* will be used as the primary source of legislation in illustrating how in times of fear governments introduce laws, which normally would not be accepted by the general population as a clear invasion of their privacy.[1] In

[1] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001*, Pub. L. No. 107-56, 115 Stat. 272 (2001)

addition, Canada and the United Kingdom's anti-terrorist legislations will be compared with the United States. Money laundering, terrorist anti-terrorist finance, government investigative surveillance, and data mining will be the areas this paper will focus on to illustrate the emerging invasion of privacy for the sake of *security*. Despite the fact that we are losing our privacy to our fears of danger, a light will be shed as to the effectiveness of these new laws. Case law will be used to illustrate that the courts have been reluctant in invalidating laws that infringe our constitutionally given rights of privacy. Possible alternative measures will be given to deal with acts of terrorism.

2. Privacy Defined

In order to engage in a discussion of privacy and its infringement, a brief explanation of what it means for western societies is necessary. Alan Westin's four basic states of privacy are: solitude, intimacy, anonymity and reserve.[2] The traditional understanding of privacy focuses primarily with individual rights of privacy against state interference. This understanding of privacy leads to the legal analysis that sees privacy as an interest that competes with security. Westin argues that privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.[3]

Privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, whether in a state of solitude or small group intimacy or, when among larger groups, in a condition of anonymity or reserve.[4] The individual's desire for privacy is never absolute since their desire to participate in a society is equally as powerful. There is always a balancing act between the desire for privacy and the desire for disclosure and communication to himself and to others in light of social norms set by the society he lives in.[5] People often perceive that their privacy is in danger but they are not sure what to do to protect themselves.[6] We often have inconsistent views about privacy for we may want its protections yet we also want the benefits that come as a result of practices that undermine those protections.[7]

The issues on privacy protection have primarily emerged from the development of new technology. Data that is acquired, merged, and shared through connecting computer networks, whether with or without our complicity, invades our privacy. Surveillance technologies are another aspect that is of great concern to civil liberties groups on invasion of privacy. Surveillance technologies could weaken the social value of privacy and can increase the risk of adverse social consequences.[8] Increased scrutiny by state agents can: (a) stifle political dissent as individuals fear reprisal by government actors; (b) inhibit freedom of expression from individuals fear public scrutiny of their views of behaviour; (c) lead to racial or religious profiling, that is discrimination which targets identifiable groups despite no evidence of individual wrong-doing; (d) have a disproportionately adverse impact on lower income citizens who tend to make a greater use of public spaces, which are increasingly subjected to state scrutiny; (e) result in political complacency to the extent that ubiquitous surveillance eliminates any subjective expectation of privacy and discourages citizens from questioning more and more state scrutiny; and (f) make it harder to hold state agents accountable for their potentially abusive behaviour in part because of the secret nature of the new technologies.[9] The new technologies will inevitably make the public less secure in the

[2] Andrew Askland, "WHAT, ME WORRY? THE MULTI-FRONT ASSAULT ON PRIVACY", 2006, 25 St. Louis U. Pub. L. Rev. 33.
[3] Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", 2007) 40 U.B.C. L. Rev. 41 – 67.
[4] Ibid.
[5] Ibid.
[6] Andrew Askland, "WHAT, ME WORRY? THE MULTI-FRONT ASSAULT ON PRIVACY", 2006, 25 St. Louis U. Pub. L. Rev. 33.
[7] Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", 2007) 40 U.B.C. L. Rev. 41 – 67.
[8] Ibid.
[9] Ibid.

long run because the religious or racial groups that become targets of profiling without any evidence will make member of that group not aid law officials in their investigations.

The constitutional heritage of both the United States and Canada do not directly address the privacy implications that confront our society. The U.S has failed to provide protection to privacy whereas European countries have a set of national privacy laws.[10] European countries regard privacy as a personal right that is non-proprietary and the burden is shifted on those who want to affect such right whereas in the United States privacy is an economic commodity.[11] The United States government relies upon the War on Terror to justify law enforcement activities, which deviate from the traditional constitutional protection.

Much like the terrorist attack on September 11, the countermeasures against terrorism have a psychological value far out of the proportions to their effectiveness.[12] In London, England 1940 a surprise terrorist attack hit the city. The terrorists were the Nazis launching an aerial attack into civilian targets in dense populated areas of London. The attack by the Germans was not consistent with the law of war. They were not tactical strikes to take out military bases. Instead these attacks were done solely on the purpose of terrorizing the city of London and demoralizing the whole country.[13] The attacks were not conventional by nature and they can be easily classified alongside current terrorist attacks. The only reason why the Nazis resorted to terrorist attacks is that they simply add a psychological warfare component to the rest of the attack.[14] The most effective counter-terrorist act is for the political leadership to boost up public confidence to avoid further panic.[15] Winston Churchill addressed the public and reassured the nation that all would be fine. The British deployed highly visible and noisy anti-aircraft guns around the city, although military experts in Britain knew that these guns had no chance in intercepting German planes but it was necessary to create an illusion of security.[16] The decision to put the anti-aircraft guns was temporary unlike the decisions made by the United States post September 11 terrorist attacks. The United States and to a lesser extent Canada have implemented what seems to be permanent legislation in the fight against terrorism.

3. The Fourth Amendment

The Fourth Amendment to the United States Constitution is the part of the Bill of Rights, which guards against unreasonable search and seizure. It purports that any arrest should have (1) some form of individualized suspicion (probable cause), (2) judicial review where feasible, (3) notice of any search and seizure.[17] Many of the provisions of the Patriot Act have seen a great level of public resistance. The Bill of Rights Defense Committee led seven states and 399 cities to adopt a resolution condemning many provisions of the Patriot Act. The Committee believed that the Patriot Act provisions are a threat to the value of privacy, freedom of speech, freedom of religion, and other associations that one can have.[18]

The Patriot Act has brought a shift in which the Congress is protecting our freedoms and not the judiciary.[19] The groups that have expressed great concern about the enhanced government surveillance are the politically

[10] Andrew Askland, "WHAT, ME WORRY? THE MULTI-FRONT ASSAULT ON PRIVACY", 2006, 25 St. Louis U. Pub. L. Rev. 33.
[11] Ibid.
[12] Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.
[13] Ibid.
[14] Ibid.
[15] Ibid.
[16] Ibid.
[17] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[18] Ibid.
[19] Ibid.

unrepresented minorities. In the United States and Canada Arab and Muslim men are the ones that fear that an entire society is willing to sacrifice someone else's rights for their sense of security.[20]

In *Mapp v. Ohio* the Supreme Court ruled that the Fourth Amendment applies to the states by way of Due Process Clause and that searches and seizures that violated the Fourth Amendment would be deemed unconstitutional.[21] The United States Supreme Court has the power to stop the Congress if they find that a specific legislation has gone too far in invading rights.[22] However, this power has yet to be exercised by the courts.

4. The Patriot Act

These are provisions that directly affect the United States Fourth Amendment. Section 215 of the Patriot Act permits government to obtain a court order providing access to tangible things and objects on the basis of certification by executive branch officials and orders the recipient not to divulge the government's request.[23] Section 505 allows the government to issue National Security Letters to retrieve customer records from Internet service providers otherwise necessary court order required by section 215.[24] Section 218 does require a court order to authorize electronic surveillance, but it diverges from the Fourth Amendment, as the rules on probable cause and notice are very relaxed. Lastly, section 213, the "sneak and peak" allows agents conducting search warrants to delay telling their targets that their property is being searched or even seized.[25]

Every single one of these provisions shows that government power has increased far beyond the temporary measures taken by Winston Churchill. Firstly, there is a clear enhancement of the executive discretion on when to conduct surveillance. Secondly, there has been an expansion of executive discretion to decide whether and when to divulge information. Thirdly, there has been a decrease in the role of the judiciary in approving surveillances before the fact. Finally, there has been a drastic decrease in the role of the judiciary in reviewing the constitutionality of the executive discretion.[26] The control of the executive to calibrate the dissemination of information and any search they conduct has as it primary goal secrecy and it ultimately avoids any challenge in court.[27] No judiciary system can properly adjudicate on theories and hypotheses, and that is what is available to anyone who wishes to challenge these new laws.[28] There is no tangible document that can be procured by those who have something to say about the effects of these provisions.[29] Secrecy for the sake of security is what has allowed the executive to simply ignore requests of accountability in their actions.

(a) Section 215

Section 215, titled "Access to Records and Other Items Under the Foreign Intelligence Surveillance Act," authorizes the government to acquire records, including educational or financial institutions, Internet service providers, or even librarians under court order.[30] The Patriot Act expediently increased the kinds of records the government could acquire in their efforts to fight the war against *terrorism*, and completely eliminated the

[20] Ibid.
[21] *Mapp v. Ohio* (1961), 367 U.S. 643, 81 S. Ct. 1684.
[22] Ibid.
[23] *USA Patriot Act*, s. 215.
[24] Ibid., s. 505.
[25] Ibid., s.218, s.213.
[26] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[27] Ibid.
[28] Ibid.
[29] Ibid.
[30] *USA Patriot Act*, s. 215.

requirement that the government demonstrate any form of suspicion. Section 215 prohibits anyone who is producing the tangible documents for the government to disclose the information to anyone other than the government official.[31] The government may procure medical, religious, or library records about anyone without the need to ever disclose to the public or to the person that such search was ever done. This search can be done even if there is no reason to believe to suspect that the person whose records are being sought has been involved in any form of misconduct or is affiliated with terrorists.[32] Since the court doesn't have much information to work with the issuance of such order has become arbitrary since the idea that there must be probable cause to release any search warrant has lost its fundamental constitutional value.[33]

This section also affects the First Amendment as it allows the gathering of information about reading habits, Internet searches, and religious practices. Individuals are not able to enjoy the privacy and freedoms associated with the First Amendment as they once could. Everyone could be searched, and there is little to zero accountability in the executive power, for any mismanagement results in political change not legislative repositioning.[34]

Section 505 surpasses section 215 in overstepping judicial oversight of government's collection of information from third parties. It permits government to extract records from a communications provider, including telephone companies, Internet service, and libraries with computer terminals by issuing its own administrative subpoena, called the National Security Letter ("NSL").[35] The only thing the government has to show in order to get the documents they require is that the information is relevant to a terrorist investigation. Section 505 prohibits anyone served with NSL to disclose to any person that the FBI has ordered or obtained records pursuant to this authority.[36] The *Washington Post* in 2005 published an article where it stated that over 30,000 National Security Letters had been requested a year.[37] However it is impossible to litigate such letters for its all a secret. "Essentially the Patriot Act is there to silence people who question the Patriot Act."[38]

(b) Section 218: Foreign Intelligence Surveillance

This section expands the power of the government in their Foreign Intelligence Surveillance ("FISA").[39] The power extension allows government to conduct electronic surveillance. The problem with this clause of the Patriot act just like with many of the clauses is that not electronic surveillance should be allowed unless it is found that probable cause exists in furthering the investigation. Attorney General Gonzales admitted that 74% applications to the FISA court and they all have been granted.[40] There is little room for contestation for all the orders granted to FISA are secret and are not available to the general public.

(c) Section 213: "Sneak and Peak"

Section 213 applies in cases where the government has followed the rules of the Fourth Amendment and has been granted a warrant on probable cause.[41] Section 213 comes into play as it allows government to ask the court for permission to delay the notification of the target of the search because they believe that the notification might

[31] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[32] Ibid.
[33] Ibid.
[34] Ibid.
[35] *USA Patriot Act*, s. 505.
[36] Ibid.
[37] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[38] Ibid.
[39] Ibid.
[40] Ibid.
[41] *USA Patriot Act*, s. 213.

have an adverse result.[42] However, the Fourth Amendment requires that notice be given prior to search, and this section is completely ignoring the constitutional rights of American citizens. A letter from the Department of Justice stated that the deferred notification was used 153 and only 18 of those times were for terrorism investigations.[43]

The government is invading the public's privacy and infringing constitutional rights and yet there is no one to correct the problem. The courts are merely siding with the executive because there is no litigation over the constitutionality of this provision of the Patriot Act. This section does not only apply to terrorism, rather it applies to every citizen the government believes it has a probable cause in searching. The consequence of extending the application of section 213 to other areas of investigation is the ultimate fear for every clause in the Patriot Act. This invasion of privacy will no longer be an excuse to just investigate terrorism; rather it will be used and adopted as legislation that applies to every citizen. It seems that the government has taken a temporary fear of terror and replaced it with a permanent fight on terrorism and thus a permanent invasion of privacy.

The four sections illustrated above are a clear example of the secrecy that surrounds the fight against terrorism. However this fight has spilled over to include much more than just presumed terrorists. The public has put its privacy on the line and it cannot evaluate how the powers of the government have been used.[44] The media disclosed that over 30,000 NSL letters had been issued.[45] However, other than the sheer volume of the use of these provisions, no tangible document is given to reveal the true nature of the provisions in action. In a system where secrecy is the mode of action there can be little to zero accountability. In 1970s after the public learned that the FBI had wiretapped Dr. Martin Luther King, the government limited the discretion available to the Foreign Intelligence Surveillance.[46] A similar resistance is almost impossible to emerge in our days society because we have been indoctrinated to be afraid of anything and everything and in turn have become more willing to risk the rights of others for our perceived safety. However, that is not a universal view of how our society is progressing. Out there in the legal sphere there those hopeful ones that believe that courts power and actual governmental accountability is not such outlandish thought.

There have been some modest amendments to the Patriot Act by the Senate, however they have not been substantial, as the courts have unambiguously allowed deviations from the Fourth Amendment principles of judicial review, probable cause, and notice.[47]

The Fourth Amendment tests asks what expectations of privacy society is willing to protect, however the court has allowed government discretion to perform surveillance under conditions that the public would find unconstitutional and unreasonable.[48] In light of the terrorist attacks the court has been reluctant to go against the legislative power.[49] The balancing test on whether the governmental need to forego or tweak the Fourth Amendment outweighs the individual constitutional interest. The right to privacy is a merely an economic commodity in the United States.[50] And for now, it seems that commodity is being sold wholesale.

In order to comprehend the shift of the courts into a more subdued to the legislative power case law will be introduced to show the historical progression. In *Olmstead*, the court emphasized the need to protect the secrecy

[42] Ibid.
[43] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[44] Ibid.
[45] Ibid.
[46] Ibid.
[47] Ibid.
[48] Wayne N. Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy", 2006 43 Alta. L. Rev. 779 – 823.
[49] Ibid.
[50] Andrew Askland, "WHAT, ME WORRY? THE MULTI-FRONT ASSAULT ON PRIVACY", 2006, 25 St. Louis U. Pub. L. Rev. 33.

of telephone messages.[51] In addition, Congress passed the Federal Communications Act of 1934 where "no person not being authorized by the sender shall intercept any communication and divulge or publish the existence, contents, substance, purport, effect or meaning of such intercepted Communication to any person".[52] This was one of the first steps where the court took spearheaded the Congress for the protection of individual privacy. In *Katz v. United States*, the court decided that the Fourth Amendment protects individuals and not places. Katz could expect privacy even he was using a public phone booth.[53] The agents would have to convince the court that they had probable cause to believe Katz was committing a crime before they could be allowed to wiretap or intercept any of his conversations. The court in *Katz* rejected the previous *Olmstead's* narrow, property oriented approach and instead declared that the Fourth Amendment protects "reasonable expectation of privacy".[54]

However, *Olmstead* was adopted by the courts post *Katz v. United States* in cases where seizure of information held by third parties was at issue.[55] The court ruled that this form of information gathering is not a search and seizure within the meaning of the Fourth Amendment. The normative approach and what seems to be the rightful interpretation of the Fourth Amendment was inevitably narrowed.[56] The court decided to limit the scope of *Katz* by stating " a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[57] However it is impossible to survive in North America without voluntarily giving ones information to a doctor, a bank teller, a librarian and many other setting where we are required to divulge our information. The court seems to ignore that the information that we give to third parties is not so voluntary in the first place, for if we choose not to give such information than we would be shunned from leading a normal life.

In *United States v. Miller* is a clear example where the court found that handing over information "voluntarily" to third parties and then when government requested such information it was not found unconstitutional. In *Miller* the government acquired checks and other financial statements from his bank. Miller argued that the bank was required to keep the documents procured and not give them to the government as per the federal Bank Secrecy Act of 1970.[58] However, a majority of the Supreme Court ruled that Miller had no legitimate expectation of privacy once he voluntarily handed the information over to the bank.

Christopher Slobogin of the University of Florida Levin College Of Law created a questionnaire to test whether the public agreed with the Supreme Court in the government being able to extract bank information and the answer was an overwhelming belief that such action is highly intrusive and private.[59] There seems to be a disconnection between the popular belief and the courts siding with the legislative.

Legislation and whatever congress decided was reasonable it would be taken at face value and would pass the constitutional test.[60] There have been instances where U.S presidents like Richard Nixon believed that they could conduct surveillance of domestic dissidents without judicial approval. Nixon had authorized the FBI to wiretap Dr. Martin Luther King, Jr and other anti-war protesters solely on their political beliefs and

[51] *Olmstead v. United States* (1928), 277 U.S. 438, 43 S. Ct. 394.
[52] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[53] *Katz v. United States* (1967), 389 U.S. 347, 88 S. Ct. 507
[54] Ibid., Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[55] Ibid.
[56] Ibid.
[57] *Katz v. United States* (1967), 389 U.S. 347, 88 S. Ct. 507.
[58] *United States v. Miller* (1939), 307 U.S. 174, 59 S. Ct. 816.
[59] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[60] Dorothy J. Glancy, "The Twenty-Seventh Annual Law Review Symposium Privacy and Surveillance: Emerging Legal Issues: Privacy on the Open Road", 2004, 30 Ohio N.U.L. Rev. 295.

association.[61] The power Nixon used was arbitrary and it resembles the power of dictator more than it does that of a democratic leader. But that is another perfect example where the United States was found in a time of turmoil and in order to stabilize growing fear the government succumbed into the invasion of citizen privacy as the easiest choice to make people afraid of consequences.

5. Money Laundering

The U.S government is fighting the war on terrorism on many fronts and one of them is to shut down any money laundering scheme terrorist might be involved in, however this is a grand task and unfortunately it doesn't seem achievable. The Patriot Act passed many provision that would allow the government to become more efficient in their money laundering efforts. Section 314 of the Patriot Act has expanded the types of financial institutions that can be searched, including credit unions, futures commission merchants, commodity trading advisors and commodity pool operators and allows the government to prohibit any suspicious account.[62]

The new provisions in the Act require financial institutions to 1. verify the identity of any person seeking to open an account, to the extent reasonable and practicable; 2. maintain records of the information used to verify the person's identity, including name, address, and other identifying information; and 3. Determine whether the person appears on any list of known or suspected terrorist organizations provided to the financial institution by any government agency.[63] Prior to these new regulations the financial institutions were required only to 1. verify and record the name ad address of individual 2.when individuals purchased monetary instruments such as money orders and 3. in certain wire transfers.[64] The United States government prohibited financial institutions from holding any relationship with offshore banks.

It has been understood by Congress that this increase of power in accumulation of information could be overwhelming in collecting information, however it is a risk they have been willing to take.[65] The government has tried to expand the exemptions from filing Currency Transaction Report ("CTR").[66] CTRs must be filed for each deposit, withdrawal, exchange of currency, or other payment or transfer, by, through or to a financial institution, which involves a transaction in currency of more than $10,000.[67] This job was assigned to the Financial Crimes Enforcement Network ("FinCEN"). Since its conception FinCEN's mission has been to track proceeds of crime such as drug trafficking. Unlike terrorist funds, proceeds of crime are easier to follow because government focuses in intercepting the funds post-crime, whereas in terrorist finance the government is expected to intercept the funds prior to the crime. James Sloan, FinCEN director said that terrorist finance is much like "money laundering in reverse".[68]

There is an argument that terrorist attacks of September 11 could have been prevented if the government was able to link all the financial transactions of terrorists in order to prevent any crime however the problem does not rest in linking financial transactions but what financial transactions to link. Terrorist attacks are not expensive to fund. The FBI concluded that the operation of the terrorist attack on September 11 cost only $303,672.[69] This sum is insignificant when one considers the billions of dollars that are traded daily in the United States. In

[61] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[62] USA Patriot Act.
[63] *USA Patriot Act*., Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.
[64] Ibid.
[65] Laura K. Donohue, "Anti-Terrorist Finance in the United Kingdom and United States", 2006, 27 Mich. J. Int'l L. 303.
[66] Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.
[67] Ibid.
[68] Ibid.
[69] *USA Patriot Act*., Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.

addition, the $300 thousand dollars were not traded in one lump sum, rather they were dispersed in many different transactions to make it untraceable.[70] The majority of the funds that were used by the terrorists were in cash and only thirty four percent of the funds deposited were wire transfers and the remaining eight percent was in traveler's checks.[71]

The other issue that the United States government has to fight is identifying the sources of terrorist funding. These sources are often times legitimate businesses, travel agencies, constructions companies, that at face value could not be detected as providing funds for terrorism.72 The word terrorist is very complicated to define because one groups terrorist is another groups freedom fighter and many philanthropist give money to groups they believe are saviors of their country.73 The war that the western countries are fighting is as much religious and ideological as much as it is a political one.

The Islamic world functions in many different countries under the *hawala* traditional banking system.[74] This banking system is based on trust and it does not require the physical transfer of the funds from one place to the other, rather a hawala broker in one country instructs the other hawala broker in another country to make a payment to a beneficiary.[75] Under this banking system there is no possible way to trace the transaction. The Patriot Act applies to hawala but enforcement is unlikely by FinCEN since there is no way to control flow of money.

Much like organized crime groups work together terrorist groups co-operate together in reaching their goals. Money laundering is a phenomenon that does not recognize states and it can happen anywhere in the world.[76] Terrorists not only can use small sums of money to transfer to their cells and thus become untraceable but they can also use fake identities when they transfer money or open bank accounts.[77]

The problem with money laundering and terrorist anti finance in the United States is that it directly infringes the privacy of citizens. The efforts by the government to suppress terrorist finance are utopian and do not have tangible success in sight. The invasion of privacy for a goal that is not realistic is the conundrum that legislators are faced with. The provisions of the *Rights to Privacy Act* of 1978 and *The Gramm Leach-Bliley Financial Modernization Act* of 1999 have been overruled by the provisions of the Patriot Act.[78] Section 314 authorizes the sharing of information between financial institutions, regulators and law enforcement agencies.[79] This provision renders the powers of the *Right to Financial Privacy Act* and *Gramm Leach-Bliley Financial Modernization Act of 1999* inoperable and invalid. The sharing of information between financial institutions for marketing purposes was forbidden by these two acts, however with the Patriot Act these institutions have found a loophole in sharing information with each other which most of the time doesn't deal with terrorist situations.[80] The only way government can keep this section operable is if they keep fears of terrorism alive for many years to come because without the fear of terror people will start asking for their rights to be returned.

---

[70] Ibid.
[71] Ibid.
[72] Ibid.
[73] Laura K. Donohue, "Anti-Terrorist Finance in the United Kingdom and United States", 2006, 27 Mich. J. Int'l L. 303.
[74] Ibid.
[75] Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.
[76] Laura K. Donohue, "Anti-Terrorist Finance in the United Kingdom and United States", 2006, 27 Mich. J. Int'l L. 303.
[77] Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.
[78] *Right to Financial Privacy Act*, 12 U.S.C. 3401., *The Gramm-Leach-Bliley Act*, P.L. 106-102, *Financial Services Modernization*.
[79] *USA Patriot Act*., s. 314.
[80] Eric J. Gouvin, "Bringing Out the Big Guns: The USA Patriot Act, Money Laundering, and the War on Terrorism", 2003, 55 Baylor L. Rev. 955.

The traditional financial privacy rights have been extinguished under exigent circumstances of fear terrorism. However there is another fear the public should have and that is that Patriot Act provisions apply to every U.S citizen. Even thought it was initially conceptualized to for foreigners and aliens or suspected terrorists these provisions extended to include every U.S citizen in order to find suspects.[81] These new provisions will have limited effects in money laundering schemes for terrorist groups and to a lesser extent drug cartels but the biggest benefit will be the ability of the government to gain information about people who try to evade taxes.[82]

6. Canadian Privacy Laws post September 11

Much like the United States in Canada the government facilitated the surveillance of citizens and foreign individuals post September 11 terrorist attacks. The fears are the same in both countries; critics believe that legal and technological developments will inevitably undermine privacy rights unless restrictions are put in place.

In Canada, the surveillance powers of the Criminal Code have been amended since 2001 by the Anti-Terrorist Act to make it easier to use electronic surveillance against terrorist groups.[83] The legislation has also extended the period of validity of wiretap authorization from the previous 60 days up to one year if the police are investigating a terrorist group offence.[84] The requirement to notify a target after surveillance has taken place can also be delayed up to three years.[85] A judge of the Superior Court of justice has to approve the electronic surveillance however it is still not sufficient to properly assess that the power conferred is being used accordingly.

Canada has expanded the Anti-Terrorism legislation as it pertains to search and seizure. A police officer can arrest a person without if he believes upon reasonable grounds that their detention is necessary to prevent a terrorist activity.[86] The Attorney General must consent to the arrest unless exigent circumstances. In addition, the detention must be reviewed judicially within 24 hours.[87] This point is where the U.S legislation differs from the Canadian. Judicial reviews of terrorist arrests are not the primary concern post arrest in the United States. However, in Canada the Anti Terrorism Act has changed traditional Common law safeguards that required independent judicial authorization prior to the issuance of a search warrant.[88] For example, the Minister of Defence has the power to authorize international electronic surveillance without the need to seek prior judicial authorization.[89] It is stipulated that the Minister must be satisfied that his authorization would not encroach the privacy of Canadians. It is visible that the discretionary powers once reserved for the courts have been passed to the legislative powers.

The Canadian government often emulates the legislative decisions made by the United States. In 2003 the Canadian government introduced legislation that would permit courts to order third parties, such as Internet Service Providers, to produce documents for the government if there is reasonable doubt that an offence has or will occur.[90] The government officials hold more discretionary power as in previous years and the former Privacy Commissioner along with public interest groups were concerned that these laws do not have adequate privacy safeguards.[91] Abusive state surveillance power was the ultimate fear that people were concerned with.

---

[81] Ibid.
[82] Ibid.
[83] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[84] Ibid.
[85] Ibid.
[86] Ibid.
[87] Ibid.
[88] Ibid.
[89] Ibid.
[90] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[91] Ibid.

The relationship between the private sector and government surveillance has seen an exponential increase in since September 11. With the exception of Quebec, Canada has pursued a self-regulatory approach to private sector privacy protection until the passage of Personal Information Protection and Electronic Documents ("PIPEDA"). PIPEDA alongside the federal Privacy Act, are overseen by the Privacy Commissioner, an independent officer of Parliament.[92] In the United States there is no authority that oversees government in respect to laws that affect privacy rights. All companies that have business in Canada will have to get the explicit or implicit consent of an individual prior to collecting or distributing personal information.[93] The problem rests with banks where an individual doesn't have much choice but to give his information to the bank in order to survive in the modern world.

The general approach to PIPEDA is that the consent of an individual must be obtained before certain personal information can be collected, used or disclosed.[94] A subscriber might reasonably expect that a newspaper would have implied consent to solicit subscription renewal, however, if the newspaper wished to forward the persons information to a third party, this would require explicit consent by the subscriber.

In Europe there is more protection for the consumer. The European Data Protection Directive asserts that European Union consumers must provide "unambiguous consent" prior to the collection of their personal information.[95] In addition to the internet, there are many other technologies that encroach privacy rights including, cell phones that divulge the exact location of telephone calls, video or cameral surveillance to inhibit crimes, variety of electronic monitoring techniques in the workplace to monitor phone calls and computer usage.[96] Under the guise of national interest, a government employee, without the knowledge of the individual in question could scrutinize the information that has been gathered by the governmental agency.[97]

The anti-terrorism laws have subjected to open evaluation prior to their enactment in Canada, however not much attention has been paid to the technology developments that surround such policy changes.[98] Technology has produced many social changes that have escaped the traditional deliberation and review that govern these legal changes. The expanded powers of government increase the risk in racial profiling against minority groups such as Muslims. The Canadian Islamic Congress reports that hate crimes against Canadian Muslims have increased by more than 1,600% since September 11 terrorist attacks and there are cases of countless interviews and interrogations of individuals of Arab origin.

In Canada, the abusive state surveillance practice has been noticed by a recent case where a police wiretap expert is suspected to have given misleading information to five Ontario judges in order to secure wiretaps in drug trafficking cases.[99] The most shocking Canadian example of post-September 11 state abuses involves Syrian born Canadian citizen named Maher Arar. Mr. was traveling home to Canada and during a stopover in New York; U.S authorities apprehended then deported Mr. Arar to Syria due to alleged links to terrorist organizations.[100] In Syria, Mr. Arar was interrogated, tortured and imprisoned for over one year until he was released on October 6, 2003.[101] There were no charges laid against Mr. Arar in Syria, Canada, or the United States. The reason for Mr. Arar's arrest is yet to be clarified and one would assume it was only arbitrary detention. The U.S officials that questioned Mr. Arar in New York had private copy of a rental agreement signed

[92] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
[93] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[94] Personal Information Protection and Electronic Documents Act (PIPEDA), S.C. 2000, c. 5.
[95] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[96] Dorothy J. Glancy, "The Twenty-Seventh Annual Law Review Symposium Privacy and Surveillance: Emerging Legal Issues: Privacy on the Open Road", 2004, 30 Ohio N.U.L. Rev. 295.
[97] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[98] Ibid.
[99] Ibid.
[100] Ibid.
[101] Ibid.

by Arar in Ottawa in 1997.[102] It has not been clarified how Mr. Arar's rental agreement came to the hands of U.S officials however it is clear that his private agreement between him and the landlord was ignored.

7. Data Mining

The ultimate goal of the abovementioned legislations is to gather as much information as possible to primarily prevent terrorist attacks and other criminal activities. However, despite any benefits data mining might bring it could be as damaging as the threats it is deployed to fight.[103] It is a common statistic that citizens in the United States and in Canada are more susceptible to be injured by ordinary crimes and automobile accidents than they are to terrorist attacks.

While it is clear that most Muslims believe that violence is not the way of their religion, western governments have classified terrorists as those individuals that have been brainwashed to follow a certain political agenda of a few; that has been ultimately twisted as an ideological war. Firstly, modern terrorist groups tend to lack a formal structure.[104] Unlike organized crime groups such as La Cosa Nostra, terrorist groups do not have rigid hierarchies. Their organizational structure restricted the scope of informational scans.[105] Wiretaps could be placed at the home of a crime family boss. Al Qaeda and associate groups lack hierarchy.[106] Bin Laden undoubtedly holds a position of power however he has been described as a mediator or catalyst than a "boss" of lower level units.[107] Al Qaeda is not unified by command structure, rather there seems to be an ideological unity. Al Qaeda if it "is" anything at all—is a network of individuals, relatively anonymous cells and ideas not hierarchy.[108] Thus we know neither the target nor the terrorist. We do not know where to look. To be safe the government says we must look *everywhere*.

Secondly, terrorist use modern communication tools.[109] La Cosa Nostra belonged to an earlier technological age, where meetings and telephone calls were the only way they could transmit information to each other. Al Qaeda elements may communicate by email or through the use of Internet websites.[110] They literally can communicate from anywhere, everywhere routed through anywhere. The government believes this is another reason why they should look everywhere.

Thirdly, modern terrorist groups tend to be very secluded and it is rarity to produce informers, reducing information gathered by human intelligence.[111] It is equally as difficult to infiltrate groups like Al Qaeda because of the immense shortage of intelligence officials that do not have the adequate language requirements.[112] In contrast, it has been easier to penetrate organized crime and also turn members of the organized crime groups into informers. However, the fears that criminals have are not similar to the fears of Al Qaeda members. If a criminal gives up his boss to save his life that is a clear choice to make, however when a terrorist gives up his team he is facing repercussions in the afterlife, clearly a more aggravating factor in becoming an informer.[113]

---

[102] Ibid.
[103] Wayne N. Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy", 2006 43 Alta. L. Rev. 779 – 823.
[104] Ibid.
[105] Ibid.
[106] Ibid.
[107] Ibid.
[108] Ibid.
[109] Wayne N. Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy", 2006 43 Alta. L. Rev. 779 – 823.
[110] Ibid.
[111] Ibid.
[112] Ibid.
[113] Ibid.

Some persons, corporations, have a vested interest in selling information technology tools and in advancing their careers, and therefore maintaining terrorism hysteria. In addition to problem with the gathering of information there is also a problem with the way it is shared. The American Civil Liberties Union ("ACLU") declared "you don't find a needle in a haystack by bringing more hay" referring to the data mining that governments have indulged themselves with post September 11 terrorist attacks.[114] The U.S department of Justice and the Federal Bureau of Investigation ("FBI") purchased and used information from ChoicePoint, a U.S data mining firm. Google Corporation has been another corporation that has collaborated with government in third party information release.[115]

Data mining faces the inevitable database problem: garbage in, garbage out. The data accessed for mining could suffer from many weaknesses. The data may be incomplete, missing fields or records, it could be incorrect, involving non standard codes, incorrect calculations, duplication, linkage to the wrong individual or other mistaken inputting, it may be incomprehensible, it could have bad formatting or the inclusion of multiple fields in one field.[116] It may be inconsistent involving overlapping codes or code meanings that change over time. If the United States and Canada are going to rely on data mining as an important source for finding about and preventing terrorism problems could arise. If data mining produces unreliable information, there will be individual costs and national security itself will be threatened.

The other argument is that by providing information to a third party privacy is not entirely lost. The individual need does not need to maintain a property or a possessory interest in the information or the records that he has given to a third party. It is this point which creates an essential difference between U.S and Canadian jurisprudence. As stated before, In *United States* v. *Miller* the Supreme Court held that once information had been disclosed to third parties the subject ceases to have a constitutionally protected privacy right.[117] Canadian jurisprudence differs itself because the Charter still protects the interests of information disclosed to third parties including health information disclosed to physician, information provided by sexual assault complainant made to the Crown as an example.[118] However, Canada has come on board with the U.S with the efforts in the fight on terrorism. Thus, legislation has been passed to allow Canadian governmental officials to gather more information from third party agencies than before.

8. Effects of Counter-Terrorism legislation

In the United States it is visible that any battle with security, Fourth Amendment claims of a right to privacy will lose. The government believes that at this moment in history it is more important to fight for security than to fight for your privacy rights. It is impossible to know whether any terrorist or other criminal actually has been or will be caught through the use of a particular power that has been enacted post September 11 terrorist attacks.[119] It could be that one of these surveillance technologies has impeded a grave terrorist attack from occurring. However, since everything is submerged into secrecy we are not really sure as to the percentage of its success. The problem with the legislations that have been enacted does not stem from a complete rejection of the legislation; rather, it is about the lack of the use of the judiciary.[120] There is an immense lack in seeking justification before engaging in surveillance, when and to whom notice must be provided, how broad the veil of secrecy should be, and how extensive or minimal the role the courts are to play.[121]

---

[114] Ibid.
[115] Ibid.
[116] Ibid.
[117] *United States v. Miller* (1939), 307 U.S. 174, 59 S. Ct. 816.
[118] Wayne N. Renke, "Who Controls the Past Now Controls the Future: Counter-Terrorism, Data Mining and Privacy", 2006 43 Alta. L. Rev. 779 – 823.
[119] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[120] Ibid.
[121] Ibid.

Marc Rotenberg has noted that the critical analysis should be made on how much secrecy and lack of accountability we are willing to tolerate in the government's use of its surveillance powers. The role of the courts should not be minimized and as it was stated in *Hamdi v. Rumsfeld* there is need for the courts to play a role in curbing excessive executive discretion to detain people in connection with the war on terror, despite its conclusion that Congress had authorized the executive execution in question.[122]

There always seems to be a clash between privacy and security. Perhaps another problem rests in our understanding that you can't have one without infringing the other. Thus, the solution rests in redefining either security or privacy; an evolving of the terms will move us from the traditional clash between the understanding of privacy and security. The definition of security and security measures around the world won't change unless world peace is at sight, until then governments and terrorist groups will continue with their political and for some religious agenda. Governments believe that measures must be taken domestically and internationally to protect their citizens. In order to protect the society one must make sure that every member of the society follows its rules. Countries like the United States and to a lesser extent Canada have thrived on ideologies that allow individuals to pursue an independent life where the government has little to zero intrusion on ones private life. However with the introduction of two components - Terrorism and Technology- the world governments are playing the once feared role of the Big Brother. There is an eye watching at all times, and much like the propaganda in the cold war where the United States criticized the Russians for intrusion into the private sphere; it seems they are on the same path themselves. If the government wants to, they can use surveillance on our homes without our knowledge, check every electronic subscription to any agency; our life has entered the grey zone of immense government discretion.

It is a difficult task to quantify the success that the United States and Canada has had in the fight against terrorism, since most things are wrapped in secrecy.[123] And most criticism comes from the failures of prevention of terrorist acts. Thus, we can only advise on the failures for we don't see the success. However, cases like Mr. Arar demonstrate that complete secrecy infringes our rights of privacy. We as people have entered into a social contract and we lose part of our sovereignty to a government or other authority in order to receive or maintain social order through the rule of law. The rule of law has not been followed by governments in their attempts to fight terrorism because the rule of law implicitly and explicitly protects our rights, especially our privacy rights. Legislation should be implemented that protects government use of resources in their combat of terrorism.

It could be argued that in order to be completely free we must enter into another social contract whereby we have the traditional privacy settings as in the past. However, in circumstances where government feels that our privacy is to be altered by the threat of security to the person than we lose control over our privacy rights temporarily.[124] The aforementioned scenario would be any government's idealistic solution to the problem of privacy but there is a better solution one which would simply put procedural safeguards to every decision that is made that directly or indirectly invades our rights. In addition, it is that most information that you will be giving to third parties will be and is being shared in with the government.

We cannot risk government and its workers gaining power and using it without any sense of accountability.[125] There is a danger that government agents and other individuals will misuse the information

[122] *Hamdi v. Rumsfeld* (2004)124 S. Ct. 2633, 159 L. Ed. 2d 578.
[123] Susan N. Herman, "The USA PATRIOT Act and the Submajoritarian Fourth Amendment",2006, 41 Harv. C.R.-C.L. L. Rev. 67.
[124] Arthur J. Cockfield, "Protecting the Social Value of Privacy in the Context of State Investigations Using New Technologies", 2007) 40 U.B.C. L. Rev. 41 – 67.
[125] Hale E. Sheppard, "U.S. Actions to Freeze Assets of Terrorism: Manifest and Latent Implications for Latin America", 2002, 17 Am. U. Int'l L. Rev. 625.

they gather and harm privacy rights and target certain individuals for illegitimate reasons.[126] The U.S and Canadian government could pass legislation that would govern how the state agents may use technologies to collect and store personal information. The government officials could store sensitive information in files that require prior judicial review.[127] The law could mandate the tracking of information on database searches performed by government agents. By maintaining logs of searches by government personnel, authorities and wrongly accused individuals will have access to an audit to determine whether the surveillance was done legally.[128] These records will allow citizens to correct errors through the surveillance that was done. In addition, the searchers will be aware that their computer usage is being monitored and this should serve as a disincentive for abuse of surveillance practices.[129]

It is argued that an independent committee should be created to provide oversight to these changes to ensure that abusive state practices are not taking place. Ultimately, we are individuals that are constantly dependent on other people's choices about our livelihood, and we all want to make sure that any decision that is made by a third party does not have negative consequences on our self identity and livelihood.

9. Conclusion

In conclusion, privacy rights have always seen a clash with security. A government cannot protect you without infringing your privacy rights. As a result privacy rights have let security take a primary role in the fight against terrorism. Privacy rights have been traded as a commodity in the market by the U.S and to a lesser extent the Canadian government because no information other than your mind is completely secluded from society. The cynical remedy to protect your privacy is to keep everything in your mind; however, no social contract should inhibit people from their freedoms. Ultimately it is necessary to protect your privacy rights by introducing regulations that control every breach of privacy. For the time, being fear of terror is greater than the fear of privacy invasion. However, governments should still be responsible and accountable for every wrong decision because after all the U.S and Canada are democratic countries and we would like to believe that as a society we still have influence over what happens with our privacy and in broader context, our lives.

Acknowledgement

Professor Crowne wishes to acknowledge the generous funding provided by the Law Foundation of Ontario in support of this work.

[126] Arthur J. Cockfield, "The State of Privacy Laws and Privacy-Encroaching Technologies after September 11: A Two-Year Report Card on the Canadian Government", 2003-2004, 1 UOLTJ 325 – 344.
[127] Ibid.
[128] Ibid.
[129] Ibid.