FREEDOM AND THE WAR ON TERROR IN THE DIGITAL AGE

by

Juan Gabriel Estrada Alvarez

B.Sc. (Honours), Memorial University of Newfoundland, 2003

A THESIS SUBMITTED IN PARTIAL FULFILLMENT OF
THE REQUIREMENTS FOR THE DEGREE OF

MASTER OF SCIENCE

in

The Faculty of Graduate Studies

(Computer Science)

THE UNIVERSITY OF BRITISH COLUMBIA

March 2006

ABSTRACT

Advances in Computer Science continue to provide more tools, each time more efficient, to aid us in our everyday lives with everything from work to entertainment, from health to management of natural resources. Technology has made our lives better and continues to facilitate progress. But just as it can benefit us, it is only a tool. That tool itself is not ‘good’ or ‘evil’; it is only useful to achieve the ends of those who utilize it. And just as it has been used for benefit, there have been cases where its use had a detrimental impact to us. Given the benefits, who is to deny that a government can keep track of its citizens in the same way a business keeps track of all its assets? The discussion here will centre on this question, where we suspect that, given technological advances, governments are tempted to achieve this goal. The purpose is to present some of the policies that governments in North America and Europe have proposed and/or adopted with respect to technology and national security, and point out flaws that could allow the undue erosion of privacy and free speech in the electronic world as a consequence. We reflect upon those measures that seem unjustified and unnecessary even in the face of terrorism, and argue that none of them include adequate safeguards to minimize the risk of abuse. We hope the reader will realize that none of the measures discussed admit that technology can accommodate the protection of civil liberties as well as security. We also argue that at least in Canada’s case, not counting academia and civil rights groups, policies and laws introduced as a consequence of the events of 9/11 seem to receive little attention from the public at large. Citizens would appear to be unaware of what is being done to mitigate the terrorist threat. Indeed, amidst such legislative actions, we may be getting used to living in a permanent state of war. We hope our conclusions give an insight into the current landscape of privacy protection in

North America and, to some extent, Europe.

TABLE OF CONTENTS

GLOSSARY OF TERMS

ACLU	American Civil Liberties Union
BC	British Columbia
CAPPS II	Computer-Assisted Passenger Prescreening System II
CDT	Center for Democracy and Technology
CSIS	Canadian Security Intelligence Service
DARPA	U.S. Defense Advanced Research Projects Agency
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DOJ	Department of Justice
DOT	U.S. Department of Transportation
EC	European Council
ECPA	U.S. Electronic Communications Privacy Act
EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center
EU	European Union
FBI	U.S. Federal Bureau of Investigation
FIS Court	Foreign Intelligence Surveillance
FISA	U.S. Foreign Intelligence Surveillance Act
FOIA	U.S. Freedom of Information Act
GAO	U.S. Government Accountability Office
IRPA	Canada Immigration and Refugee Protection Act
ISP	Internet Service Provider
NASA	U.S. National Aeronautical and Space Administration

NGO	Non-Governmental Organization
NLC	U.S. National League of Cities
NSL	National Security Letter
PIPEDA	Canada Personal Information Protection and Electronic Documents Act
PNR	Passenger Name Record
RCMP	Royal Canadian Mounted Police
TIA	Terrorism Information Awareness
TSA	U.S. Transportation Security Administration
TSP	Telecommunications Service Provider
WP	Article 29 Working Party

PREFACE

Information is shared in volumes not possible just a few years ago. Before the new decade, most access to the internet relied on dial-up connections that made it difficult to transmit large quantities of data in a practical and non-time consuming way. At the same time, those connections that offered broad bandwidths were accessible only to a few with the resources and appropriate location. Today, just in North America, about half of the population connected to the internet do so through relatively new broadband technologies such as ADSL and Cable. With this immense penetration of broadband connections, terabytes of information flow through the internet per second. Add to this the spreading of the internet throughout the globe, and the network becomes a tool for facilitating information exchange and business transactions so important that we nearly rely on it as a vital part of our daily lives.

It follows then that governments can benefit from the amount of data that can be transmitted in a single unit of time to about anywhere in the world, something that could not be achieved just a few years ago.

Computational Power and Techniques now Enable Analysis of Data in Large Quantities

But the amount of data that can now be shared is not the only factor that has grown in the last few years. The computational power of a conventional home PC now surpasses its predecessors of two decades ago by hundreds of times. New algorithmic techniques can now handle tasks that would have taken years to complete in just days. It is not difficult to then imagine - as an example - that businesses now benefit by the staggering capacity of computer systems to keep control of everything that relates to their assets. But let us not forget that there are humans who are behind the design of these systems,

and as such they are not – and never will be – error free.

A Double Edged Blade

The accelerated advance in technology continues to provide us with more and more tools, each time more efficient, to aid us in our everyday lives with everything from work to entertainment, from betterment of nations to the more efficient use of natural resources. Technology has undeniably made our lives better and continues to offer potential for the progress of civilization.

But just as technology can and does benefit us in a significant way, it is no different from any other tool that the human race has held in its hands. The tool itself is not 'good' or 'evil'; it is only useful to achieve the ends of those who take advantage of it. And just as it has been used for benefit, there have been many cases where the objective was detrimental (one needs not look further than the warring history of the human race to make this realization).

So, who is to deny that a government can keep track of its citizens in the same way a business can keep track of all its assets? Our discussion will centre on this question and, given the record provided by history, we suspect that with the ease technology provides today governments are deeply tempted to achieve this goal.

Our purpose is to present some of the policies that governments in North America and Europe have proposed and/or adopted with respect to technology and national security, and point out many of the flaws that would allow the undue erosion of privacy and free speech in the electronic world as a consequence. We reflect upon those measures that seem unjustified and unnecessary even in the face of terrorism, and argue that none of them include adequate safeguards to minimize the risk of abuse. We hope

the reader will subsequently realize that none of the measures that we are going to discuss admit that technology can accommodate the protection of civil liberties as well as security, rather than supporting the fallacy that some balance or trade-off must exist between the two.

We will also argue that at least in Canada's case, not counting academia and civil liberties groups, policies and laws passed or proposed as a consequence of the events of 9/11 seem to receive little attention from the public at large. Most citizens appear to be unaware of what their government has been up to in order to mitigate the terrorist threat.

Indeed, in the face of counter terrorist laws and policies, we may already be getting used to living in a permanent state of war. We will argue that there is no clear need or justification for the measures presented here. We hope our conclusions give an insight into the current landscape of privacy protection in North America and, to some extent, Europe.

Finally, we want the reader to note that at times we have included opinionated statements to make the reader aware of where our concern for potential ethical issues may arise with the material being examined. As such, said statements should not be taken as conclusive and should, in fact, encourage the reader to draw his or her own opinion regarding these issues.

I. THE LEGAL AND TECHNOLOGICAL MEASURES THAT GOVERNMENTS CLAIM ARE NEEDED TO COMBAT TERRORISM – AND HOW THEY IMPACT CIVIL LIBERTIES

The discussion in this chapter centres on what we consider to be the most impact-bearing policies that have been introduced after the 9/11 terrorist attacks. Sections of this chapter are taken from or based on the author's previous works – [Estrada & Rosenberg, 2005a] and [Estrada & Rosenberg, 2005b] – as follows:

Sections I.1.1 – I.1.2.

Sections I.2.2.1 – I.2.2.2.

Sections I.3.1, I.3.2.1, I.3.2.3 – I.3.2.4, I.3.3.2 – I.3.3.4.

Some of those sections have been appended to so as to account for recent developments with government proposals, particularly with the USA Patriot Act and the Lawful Access [LA, 2005] proposals.

I.1. THE REACH OF THE LAW INTO CIVIL RIGHTS

I.1.1. In the United States of America

I.1.1.1. USA Patriot Act

The USA PATRIOT Act is a 342 page document that was passed by Congress just 45 days after the terrorist attacks of 9/11 [Patriot, 2001]. It remains a mystery how it was possible to draft such a complex law in that short an amount of time. But given the time frame, it comes as no surprise that the Act contains provisions that are of great concern to those who care about their constitutional freedoms. The provisions introduced here,

with the exception of section 805, were subject to a sunset clause in 2005 and it is imperative that U.S. citizens, no matter what their stance is, voice their opinion as soon as possible. Both the House of Representatives and the Senate of the United States have approved bills that would reauthorize these provisions,[1] and convened in the fall of 2005 to discuss both versions.

With that said, let us analyse the surveillance powers afforded by the Act that are relevant to electronic communications and have an impact on liberties; these can be found in Titles II, V and VIII of the Act [Patriot, 2001].

Sections 201 and 805

Section 201 amends the Wiretap Act,[2] which establishes the procedure under which law enforcement authorities may intercept wire, oral, or electronic communications. This procedure, however, is only available for the investigation of specific crimes designated as serious. Thus, section 201 adds various terrorism related offences to the list of designated serious crimes. In particular, two of these new offences are of concern:

- Material support of terrorists; and
- Material support of terrorist organizations.

The reason for concern arises when these offences are seen in context with the amendment made in section 805. This section adds ‘expert advice or assistance’ to the types of assistance that count as ‘material support’ of terrorists or terrorist organizations. Consider the example where an organization advocates and/or provides humanitarian assistance to a terrorist organization. Many organizations of this type may have also

[1] More details about the process can be found at the American Civil Liberties Union online at http://action.aclu.org/reformthepatriotact/ accessed 08.22.05
[2] United States Code, Title 18, s. 2510 *et seq*.

been designated as terrorist, and section 805 makes it illegal to offer expert advice and assistance for these legal, non-terrorist activities. Furthermore, consider Non-Governmental Organizations (NGOs) operating in countries where terrorist groups have a presence. Following a philosophy of compassion, such NGOs generally seek to provide humanitarian assistance, and may do so through other terrorist humanitarian organizations. Under the amendment, these organizations or individuals affiliated with them can be subjected to wiretapping under the suspicion of being criminals. Should a line be drawn so that individuals doing charity work are not considered criminals in this case? The question has already appeared before the courts, which while recognizing 'expert advice or assistance' as 'impermissibly vague' have nevertheless refused to order the government to repeal this provision.[3] Section 805 also potentially criminalizes a broad range of speech protected under the First Amendment.

Section 215

Before this section came into force, the Foreign Intelligence Surveillance Act (FISA)[4] allowed senior officials of the FBI to apply for a Foreign Intelligence Surveillance Court (FIS Court)[5] order, in connection with a foreign intelligence investigation, for access to records held by common carriers, hotels, motels, storage rental facilities, and vehicle rental agencies. In order to secure the order, the FBI had to present specific facts giving reasonable grounds to believe that the individual to whom the records pertained was an agent of a foreign power or a foreign power.

Section 215 rewrites those same provisions by extending an order to require 'the

[3] Humanitarian Law Project v. Ashcroft (2004), online at news.findlaw.com/hdocs/docs/terrorism/hlpash12304ord.pdf accessed 04.21.05
[4] United States Code, Title 50, s. 1801 *et seq* .
[5] *Ibid*. s. 1803 establishes a court that oversees applications for such orders.

production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.'[6] The orders can now be served to anyone, since the language specifying the possible recipients has been eliminated. It should be noted that as a consequence of the new language, the items sought need not be related to an identified agent of a foreign power or foreign power. Moreover, section 215 provides that the existence of an order, or that a disclosure under such an order has occurred, shall never be made known.[7]

This same section specifies that the FISA court must issue the order whenever the FBI has made the proper certification, regardless of whether there are facts to back it up. It provides an enormous amount of power to the FBI, and if it is abused, no one will ever know. That is what makes it potentially dangerous. Although an investigation must not be conducted 'solely upon the basis of activities protected by the First Amendment,' one could, in theory, be investigated partially based on religious beliefs or political affiliations, or even based on the websites and books one reads. This may chill free speech and access to information, as many may fear being targeted because of what they read or the opinions they express. Section 215 perhaps constitutes one of the most liberty-eroding provisions of the Patriot Act [Patriot, 2001].

[6] *Ibid.* s. 1861-1862.
[7] *Ibid.*

Section 505

Three statutes authorize third parties to release confidential communication transaction records, financial reports, and credit information for intelligence purposes upon the written request of the Director of the FBI.[8] Prior to the enactment of section 505, these provisions allowed the FBI to request, through a National Security Letter (NSL), information and records about an individual. However, the FBI was required by those provisions to certify that there were 'specific and articulable facts' that the person or entity whose records were being sought was an agent of a foreign power or a foreign power itself.[9] The effect of Section 505 is to drop this requirement so that that the FBI now can issue NSLs by only certifying that the information sought is 'relevant to an authorized foreign counterintelligence investigation.'[10] Thus, NSLs can be issued to obtain information about anyone. Furthermore, according to section 505, even a special agent in a designated field office may issue such a letter.

The FBI can thus demand detailed information about an individual without court review or approval, without suspecting the individual of a crime, and without ever having to tell the individual that an investigation has been undertaken. The potential for chilling free speech and access to information is worrisome.

[8] These statutes are the Electronic Communications Privacy Act (ECPA), the Right to Financial Privacy Act, and the Fair Credit Reporting Act See United States Code, Title 18, s. 2701 *et seq*; Title 12, s. 3414(a)(5); and Title 15, s. 1681(u) respectively.

[9] Congressional Research Service, 'Terrorism: Section by Section Analysis of the USA PATRIOT Act' (Report for Congress RL31200) at p. 41 (December 2001). A copy can be found online at the Electronic Privacy Information Center's Patriot Act page (www.epic.org)

[10] *Ibid.*

I.1.2. In Canada

I.1.2.1. The Anti-terrorism Act of 2001

Canada's anti-terrorist measures were enacted not long after the Patriot Act [Patriot, 2001] was passed. Like its counterpart, it amended several statutes in order to afford law enforcement new powers for intelligence gathering and national security [ATA, 2001]. As this document is written, the Act is subject to review by the Canadian Parliament.[11] Canadians need to consider if the Act properly takes civil rights into account, and what the potential for misuse is. Our concern arises out of vague terms used in the legislation that could easily be interpreted by law enforcement in a manner leading to abuse. Let us consider some of the provisions relevant to our discussion.

An amendment to the Criminal Code provides for a new offence to make it a crime to knowingly participate in, contribute to or facilitate the activities of a terrorist group.[12] The participation, contribution or facilitation does not need to be a crime. Here, what 'facilitation' means is vague. Take for example, a person who provides an electronic forum for the communication of his ethnic group, which could be utilized by terrorists. A similar scenario has already occurred in the U.S. as discussed later in I.3.2.3, although at the moment, no similar case is taking place in Canada. But it is not unreasonable to expect that it could happen, and free speech online would be under attack. Further, certain charities that operate in the Middle East could also be criminalized.[13] These charities make no distinction between a terrorist and a person as a condition for providing the aid needed. Effectively, such restrictions could interfere with the ability of

[11] (ATA, 2001) ss. 145(1)-(2).
[12] Criminal Code of Canada, R.S.C. 1985, c. C-23, ss. 83.21-83.22.
[13] As we discussed earlier when analyzing section 805 of (Patriot, 2001).

individuals to show compassion for other human beings.

The Anti-terrorism Act also replaced the Official Secrets Act with a new Security of Information Act,[14] which created new classes of offences related to safeguarded information and information that if disclosed, released or stolen, would harm Canadian interests,[15] including espionage, leakage and 'harbouring or concealing' a person who commits one of the former offences. This legislation raises concerns as it bears an impact on freedom of expression, particularly for the press, where journalists have traditionally had a right to obtain information from confidential sources, especially on sensitive issues of public interest where the information is not publicly available.

I.1.2.2. The Public Safety Act of 2002

Assented to in May 2004, [PSA, 2004] is a controversial piece of legislation that expanded police investigation powers by allowing the Canadian Security Intelligence Service (CSIS) and the RCMP to require airlines and travel agents to disclose travelers' personal information for the purposes of transportation security or the investigation of 'threats to the security of Canada.'[16] A further provision amended the Personal Information Protection and Electronic Documents Act (PIPEDA),[17] Canada's major privacy legislation, to allow private sector organizations (not just airlines and travel agents) to collect personal information, without an individual's consent, for the purpose of disclosing it to law enforcement if required by law, or if requested in relation to national security or the conduct of international affairs, or if the organization suspects the information may be relevant for the purposes mentioned and intends to disclose it to

[14] Security of Information Act, R.S.C. 1985, c. O-5.
[15] *Ibid*. s. 3.
[16] (PSA, 2004) s. 5.
[17] R.S.C. 2000, c. 5, s.7(1)(e)(i)-(ii).

the authorities. The information could be used not only for these purposes, but also for the enforcement of outstanding arrest warrants for crimes punishable by 5 years or more of prison.

These amendments are troubling for a few reasons. First, private organizations in Canada can now collect and disclose personal information to the government without consent. Second, airlines and travel agents can be compelled to do so. Third, there are no limits on the amount or quality (source) of the information obtained. One could thus say that the government has enlisted the help of the private sector to act as an agent of the state. With our complete dependence today on services like telecommunications, we cannot be sure anymore of when we are under surveillance. The impact on our civil rights may cause many to choose to remain silent for fear that they are being watched. And those who do speak may be targeted. Not only does the potential for abuse exist, but also the amendments did not introduce a corresponding oversight mechanism.

I.1.2.3. Security Certificates under the Immigration and Refugee Protection Act (IRPA)

We begin by noting this measure is not a response to the events of 9/11, as opposed to others in this section. The power to issue these certificates has existed for a long time in Canadian law, but the latest incarnation appears in [IRPA, 2001]. It is relatively unknown, perhaps since it deals only with non-citizens. However, the provisions call for secrecy without a system of accountability and review which in our opinion is not compatible with the values of any democracy. The certificates are meant to provide an expeditious process to remove any unwanted or dangerous aliens (as well as permanent

residents) from Canada.[18] To see why, let us overview the procedure governing the issuance of a certificate as set forth in [IRPA, 2001]:

1. The Canadian Security Intelligence Service (CSIS) gathers information concerning some security risk and sends a brief to the Minister of Citizenship and Immigration and the Minister of Public Safety and Emergency Preparedness for their review.
2. If the Ministers are satisfied that a person is inadmissible to Canada on security grounds,[19] they must issue a certificate with their signature outlining the general grounds for inadmissibility. Foreign nationals are detained without a warrant, and permanent residents must be served with a warrant subject to judicial review periodically during detention of the permanent resident. The certificate is then filed with the Federal Court for its review. All other immigration proceedings against the subject must be suspended until the Court determines whether the certificate is reasonable or not.
3. The IRPA requires the Chief Justice of the Federal Court, or his delegate, to preside over the case. Throughout the process of determining the reasonableness of the certificate, at the request of the Ministers, the judge shall hear in camera all or part of the information or evidence in the absence of the subject or the subject's counsel. Upon review of the classified information, the judge will then determine how much will be included in an unclassified summary to be provided to the subject of the certificate and the subject's counsel, which must be sufficient to enable the individual to be reasonably informed of the circumstances giving rise to the certificate, but does not include anything which, in the opinion of the judge, would

[18] Proceedings of the Special Senate Committee on the Anti-terrorism Act, Issue No. 3, (March 7, 2005) p. 10-12. Online at http://www.parl.gc.ca/38/1/parlbus/commbus/senate/Com-e/anti-e/pdf/03issue.pdf accessed 03.12.2006

[19] In order to determine whether an individual is a threat to national security, both the Minister and the Solicitor General have to consider the factors set forth in ss. 34-37 of the IRPA.

be injurious to national security or the safety of any person. The subject has an opportunity to be heard in an open hearing.

4. During the proceedings, the subject may apply for protection to the Ministers if it is believed that deportation will result in death or torture. The judge suspends the proceeding until the Ministers make a decision on the application, and must determine the lawfulness of such a decision once it is made.
5. Finally, the judge must rule, based on all of the above, whether the certificate is reasonable or not. It must be noted that [IRPA, 2001] allows a judge to ignore the traditional rules of evidence. Any evidence that the judge deems 'appropriate' can be considered, and what 'appropriate' means is very vague and severely lowers the standard for admissible evidence. If the certificate is found reasonable, then it is conclusive proof that the detainee is inadmissible. It becomes an order for removal and may not be appealed.

The standard of review that must be met by the Ministers is merely to show that the decision to issue the certificate is 'reasonable'. [Gratl, 2005] argues that this standard may 'ensnare(s) any vocal political dissident,' with the potential of chilling political expression by non-citizens of Canada. [Gratl, 2005] also points out that the courts have held that subjects detained under the IRPA are entitled to a diminished level of protection under the Canadian Charter of Rights and Freedoms. Regardless of the level of protection to which they may be entitled, the amount of secrecy with which this process can be done, and the little judicial review that is provided – with no opportunity of appeal by any one – may hinder the individual's right to a fair open hearing guaranteed by the IRPA and leads us to conclude that it is a form of secret trial.

The government has invoked these powers 27 times between 1991 and 2005[20] and continues to hold individuals in confinement without charging them, as we will see in I.3.3.1. Democracy is based on the concept that the citizens as a whole rule themselves. This requires that we be able to observe, make decisions about and hold accountable those that we have elected as our representatives in government. Thus, the level of unaccountability and secrecy afforded by this statute may not be compatible with our democratic values.

I.1.2.4. A National Identity Card

A National Identity Card for Canada was proposed in 2002 by the then Minister of Citizenship and Immigration and was subsequently examined by the House of Commons Standing Committee on Citizenship and Immigration[21] (the Committee). There has not been any specific proposal for Canadians to respond to yet. However, the government has not stated that it would not consider a measure like this in the future either, and thus we must be prepared for the time when such a proposal appears.

In a speech to the Committee, the Minister argued that not only terrorism, but also growing identity theft are signs that Canada needs to consider a means of verifying that individuals are who they say they are since 'Canada does not have an explicit, official national identity policy' nor an identity system.[22] A use of biometric technologies and standardization of an identification policy were also advocated. As the Privacy

[20] See 'Certificates Under the Immigration and Refugee Protection Act (IRPA)' on the CSIS website online at www.csis-scrs.gc.ca/eng/backgrnd/back14_e.html accessed 06.06.2005
[21] See the House of Commons Standing Committee on Citizenship and Immigration news release, 'A national identity card for Canada?', online at www.parl.gc.ca/committee/CommitteePublication.aspx?SourceId=61004 accessed 06.09.2005
[22] Notes for an address by the Honourable Denis Coderre, Minister of Citizenship and Immigration (2003), 'Why Discuss a National Identity Card?', online at www.cic.gc.ca/english/press/speech/id-card.html accessed 06.09.2005

Commissioner of Canada [PCC, 2004] has argued, the financial costs and the privacy risks associated with setting up such a system are significant when viewed in contrast to the benefits sought. Our main concern arises with the magnitude of the database that such a system would require and the amount of information that it would hold about each individual. In addition to the challenge of preventing abuse of a system that keeps track of every individual in the country, the possibility of an identity disaster is real as the recent breaches of security in U.S. data aggregation companies cited by [Estrada & Rosenberg, 2005a] expose, making evident that such a solution could only make the problem it is trying to solve worse.

I.2. TECHNOLOGICAL RESOURCES AND THE CONFLICTS WITH CIVIL LIBERTIES

I.2.1. Knowledge Discovery and Data Mining

Right now, the main tool being used for surveillance measures in the U.S. is popularly known as data mining. However, a more appropriate term for what these programs seek to do would be *knowledge discovery*, as what governments plan to do is be able to identify and classify terrorist behaviour. Here we will treat data mining as the process where intelligent computational methods are used to extract patterns in databases for the purpose of knowledge discovery. Knowledge discovery has a number of applications in the private sector, for example finding the shopping habits of customers at a supermarket in order to stock more of the popular products. In the financial sector, it could be used to detect fraudulent credit transactions. Although not limited to information about individuals, for the purposes of this dissertation, knowledge

discovery entails gathering information about people and their everyday lives. Here we introduce the concept based on the work of [Han & Kamber, 2001].

Knowledge discovery can be seen as a sequence of steps, each of which is essential to the process. We will propose our concerns with governments' handling of this tool along with each step:

1. Data cleaning and data integration: this is a pre-processing step where the data is prepared for mining. Integrating the data in this case means obtaining the sources from both government and private sector databases (typically travel, telecommunication and financial records).
2. Data selection: where the data considered relevant to the analysis is retrieved (in this instance it could include travel destinations and dates, types of financial transactions and dates). It is worth mentioning that governments have not been specific on where the data will come from or what types of data would be useful in order to identify potential terrorist behaviour. Although governments typically argue that such information should be secret, here the compelling reason for the unavailability of details may be that governments are still on an early testing stage and are not sure themselves which way to go, as will be evident later on.
3. Data transformation: in this step the data is consolidated or aggregated into a form appropriate for data mining. This step is crucial in the protection of privacy, as it is where all identifying information should be encrypted or anonymized, such that individuals can be identified only when a (justifiable) need arises. A privacy protection system was introduced into the U.S. government's knowledge discovery efforts as we will see in I.2.2.1. However, the system would have little meaning without appropriate oversight built into the regulations, especially in the face of the

FBI's unfettered access to information via [Patriot, 2001].

4. Data mining: as we previously noted, this is the step where computationally intensive methods are applied to the data resulting from 3 above in order to extract data patterns. Current methods have proved to work well in the private sector. We must point out, nonetheless, that private sector databases are typically not of the magnitude of the amount of information that the U.S. government is seeking to obtain for its programs. It is indeed a technical challenge to create efficient methods to mine data on every citizen's everyday life.
5. Pattern evaluation: out of the patterns extracted by step 4, this step identifies those that represent knowledge relevant to the analysis based on some *measure of interest*. Measures of interest are typically based on the structure and statistics underlying a pattern and the pattern will be interesting to the analysis if it meets the minimum threshold for the measure. We are concerned about how such a measure would be created for automatically uncovering potential terrorist behaviour. Moreover, as we will also see in I.2.2.1, the U.S. government has suggested that this step will be managed by human users, making a process that may involve a large number of interesting results highly subjective and hence prone to errors. None of these concerns have been fully addressed under the excuse that, as we will see in I.2.2.1, the programs are still under testing, and no details about what measures of interest are being used have been given. That can severely hinder the program's potential effectiveness in the absence of input by experts in the field.
6. Knowledge presentation: this is the final step where the discovered knowledge is presented to the user in a comprehensible form. In this particular case, the end users would be lawmakers making decisions on how to respond to terrorist threats.

The above overview should be enough for the non-technical reader to understand well enough the process of knowledge discovery so that our concerns with the programs reviewed in this work are clear.

I.2.2. Programs in Place or Being Developed to *Fight Terrorism*

I.2.2.1. Surveillance Measures in the United States

The Terrorism Information Awareness (TIA) Program

Originally called 'Total Information Awareness,' the TIA program was being developed by the Defense Advanced Research Projects Agency (DARPA). It aimed to integrate information technologies into 'a prototype to provide tools to better detect, classify, and identify potential foreign terrorists,' and was described as 'a program of programs' that would sit at the base of a counter-terrorism information architecture, as DARPA explained in [DARPA, 2003]. This was perhaps the first incarnation of such a controversial system that would have far reaching implications for personal information not only about foreign persons, but about U.S. citizens as well. To appreciate the intended scope of the TIA program, now terminated, consider a few of its objectives[23]:

- Unprecedented information coverage via access to and sharing of databases across governmental agencies that could be easily scaled, including (but not limited to) financial and medical records and transactions. This inevitably implies a virtually centralized national database of private information about individuals and their everyday behaviour.

[23] [Darpa, 2003] at p. 4.

- Produce warnings based on ‘triggering events’ or after passing some ‘articulated threshold.’ What these would be was not specified, and what the procedure would be after a false positive led to law enforcement action was not discussed.

The program would have employed data mining and pattern matching in order to do its job. Analysts would be cued based on ‘partial matches,’ providing them with a starting point for the assessment of potential threats to security; based on these assessments, decision makers could evaluate the impact of security policies . Given the legal framework provided by the Patriot Act [Patriot, 2001] and because of the nature of its information coverage, TIA would effectively become a tool not just to combat terrorism but also for everyday law enforcement. Nevertheless, the government tried to justify the creation of the system with the sole objective of countering terrorism by changing its original name (from Total IA to Terrorism IA). In practical terms, the system would have made the job of law enforcement undoubtedly much easier. Unfortunately, the magnitude of such a program would make it much more difficult for a proper system of checks and balances to be put in place.

At the time that TIA [DARPA, 2003] was under discussion, DARPA’s consideration of built-in safety procedures to protect civil liberties included a commitment from the Department of Defense (DoD) to ensure that activities would be ‘conducted in full compliance with relevant policies, laws, and regulations, including those governing information about U.S. persons,’ along with the ‘Genisys Privacy Protection’ system.[24] Genisys was to be an ambitious program that would sit on top of a database in order to control authorized access and make inferences about misuse. It would hide sensitive

[24] *Ibid*. at p. A-12.

information from users unless further investigation warranted it, and would provide it only upon proper authorization. Thus, it was to act as an automated audit system under the oversight of some 'appropriate authority.' There were no suggestions as to who this authority might be and what the criteria for obtaining authorization for further investigation would be. Regardless of any criteria, no matter how strict, the Patriot Act [Patriot, 2001] would already grant unfettered access to sensitive data to the FBI under section 215, as discussed in I.1.1.1.

DARPA's vision was to be able to access 'the massive amounts of data on potential foreign terrorists.'[25] Given the objectives and coverage of information, the question arises: Is it not the nature of such a strategy to simply assume then that everyone whose personal information exists in some database is a potential terrorist? As long as the algorithms that constitute the system assign a likelihood (and how this likelihood would be assigned has never been publicly disclosed) of criminal activity to each person whose information is in the system, that could potentially be the case.

Finally, it must be noted that at the time, the components of the system were in very preliminary stages and there were no results to report.[26] Furthermore, DARPA stated that it did not know if its proposed research program would be successful at all, especially given its ambition. But if it were to succeed, then an evaluation of the legal and policy implications would be conducted subsequently.[27] Such a strategy is a clear example of allowing the technological component to drive policy, which could lead to a very dangerous undermining of the principles of freedom and rights of individuals. Of course, any democratic government should be expected to protect these rights.

[25] *Ibid.* at p. 7.
[26] *Ibid.* at p. 17.
[27] *Ibid.* at p. A-5.

What we have described here is only part of what TIA was intended to be, without going into other potentially problematic components of the system such as the identification and tracking of unique individuals at a distance by using biometrics. The U.S. Congress terminated funding to TIA[28] shortly after its full potential was publicized [DARPA 2003]. This termination was by no means the end of knowledge discovery efforts by the U.S. government for the purposes of law enforcement, as we shall see.

The Transportation Security Administration's (TSA) Secure Flight as successor to CAPPS II

The Computer-Assisted Passenger Prescreening System (CAPPS) II was conceived in response to the terrorist attacks of 9/11 to evaluate all passengers of a domestic flight in the U.S. before boarding [GAO, 2004]. To do this, it proposed to make use of Passenger Name Records (PNRs) that airlines already keep in order to associate passengers with their itineraries and form of payment, among other items. Briefly, the system would operate in the following four steps[29]:

1. Require a passenger to provide his or her full name, home address and phone number, and date of birth, to be inserted in his or her PNR and sent to CAPPS II.
2. CAPPS II requests an identity authentication from one or more private sector commercial data providers which assess by a scoring method the level of confidence that the information provided by the passenger is authentic.

[28] House Report 108-283, 'Conference Report on H.R. 2658, Department of Defense Appropriations Act, 2004' (September 2003). A copy can be found online at the Federation of American Scientists page on Congressional Documents on Secrecy and Security – 2003 (www.fas.org)
[29] (GAO, 2004) at p. 6-7.

3. After obtaining an authentication score, CAPPS II conducts background checks (including criminal checks) for the passenger against government databases and intelligence data. It utilizes data mining techniques to identify potential terrorist behaviour from the passenger information available. This generates a 'risk score' that categorizes the passenger.
4. At check-in, the passenger's risk category is transmitted to the check-in counter. Depending on the category, a passenger might be required to go through additional security checks or possibly be detained by law enforcement.

By February 2004, the U.S. Government Accountability Office (GAO) had determined that the TSA had not fully addressed seven of eight issues that the U.S. Congress identified as areas of interest,[30] faced significant delays, and argued that the TSA did not have a clear picture of how much the system would cost in the long run. The TSA finally decided to postpone CAPPS II in July of 2004 under intense criticism over privacy concerns.[31]

The TSA decided to continue its plans for CAPPS II in September of the same year by creating Secure Flight. In terms of the steps above the system would be the same, except that data mining would not be used within Secure Flight, an expanded database provided by the Terrorist Screening Center[32] would be utilized for step 3 above, an and authentication process utilizing commercial databases would be conducted only if the

[30] *Ibid.* at p. 4-5. These included the verification of the accuracy of commercial and government databases, implementing security measures against abuse and unauthorized access, adopting policies for oversight of the operation of the system, identifying and addressing all privacy concerns, and a redress process for passengers erroneously categorized.
[31] The Washington Post, 'New Airline Screening System Postponed' (July 2004) online at www.washingtonpost.com/wp-dyn/articles/A53320-2004Jul15.html accessed 04.21.05.
[32] (GAO, 2005) at p. 11-14. The TSC database consolidates information from terrorist watch lists to provide government screeners with a unified set of antiterrorist information.

testing phase shows that it is effective [GAO, 2005]. It was reported in [GAO, 2005] that as of March 2005 the TSA still had not fully addressed all of the issues of interest that were present in its predecessor, and further noted other key concerns that remain unaddressed:

- The use of PNR data to check against watch lists to determine who is a threat does not, and will not, have any means of dealing with stolen identities.
- What the accuracy of the terrorists watch lists is.
- The TSA has not yet fully examined the privacy impacts of Secure Flight.

The magnitude of such a project is enormous. And unfortunately it may be subject to a proportional risk of failure. The possibility of such a failure is given substance from what has recently happened in the ChoicePoint and LexisNexis scandals, where the personal information of at least 455 000 individuals was put at risk of identity theft by individuals posing as legitimate companies seeking to get access to ChoicePoint's databases, which record the daily transactions of millions of people,[33] or using stolen passwords to gain access to personal information in LexisNexis' databases.[34] Seeing how easy it still is to perform ID theft, it is hard to argue how the TSA's programs will make the U.S. any safer given the high risk inherent in their proposed system. And also given how the Department of Homeland Security (DHS) is lacking proper security for its own computer systems,[35] we feel that this program poses not only a risk to civil liberties, but also to the security the U.S. government is trying to achieve for its nation.

[33] The New York Times, 'Breach Points Up Flaws in Privacy Laws' (February 2005) online at www.tuscaloosanews.com/apps/pbcs.dll/article?AID=/20050224/ZNYT01/502240326 accessed 04.21.05.
[34] ABC News, 'LexisNexis Breach May Be Worse Than Thought' (April 2005) online at abcnews.go.com/Business/wireStory?id=666708 accessed 04.21.05.
[35] MSNBC News, 'U.S. agencies flunk cybersecurity test' (February 2005) online at www.msnbc.msn.com/id/6981279/ accessed 04.21.05.

A system of redress for those who are wrongly categorized has been drafted but doubts exist as to how it can be implemented.[36] As can be seen from this section, each time the TSA is questioned it argues that it is too early in the testing phase to finalize policies, assess privacy impacts, and verify the accuracy of the databases it plans to utilize. This is an example of how the DHS is allowing *technology to drive policy*, a path that could lead the U.S. government to fail in its attempts to protect the nation and, as a consequence, to jeopardise individual liberties.

I.2.2.2. Lawful Access to Personal Information

Shortly after 9/11, the Convention on Cybercrime was introduced and signed by Member States of the EU along with Canada, Japan, South Africa and the USA on November 23, 2001 [CC, 2001]. It called for new expanded police powers for electronic evidence gathering in the investigation of crime. We will examine two proposals that have emerged in Canada and the European Union respectively, that are directly related to the Convention. In both cases, these proposals raise the question of lawful access to electronic traffic data as is defined in [E-PH, 2004].

The Proposal on Data Retention in Europe

Complementing the CyberCrime Convention [CC, 2001], there have been proposals by EU Member States to introduce data collection and retention of all internet communications as a preventative measure[37] (the interception of both traffic and content data would be similar to telephone wiretaps for internet communications). To

[36] *Supra* note 32 at p. 13-14.

[37] The data retention proposal was first drafted by France, Ireland, Sweden and the U.K., and has evolved a little over time, and a copy of the latest version (EC document 6566/05) can be found at the Statewatch.org website online at www.statewatch.org/news/2005/apr/draft-data-retention-proposal.pdf accessed 04.17.05.

understand what that legislation seeks to do, we can look at the title of the proposal:

> 'Draft Framework Decision on the retention of data processed and stored in connection with the provision of publicly available electronic communications services or data on public communications networks for the purpose of prevention, investigation, detection and prosecution of crime and criminal offences including terrorism.'[38]

Not only would law enforcement authorities be given the power to straightforwardly access and monitor personal information, but they would be enlisting ISPs to carry out and pay for the surveillance on their behalf.[39] However, no one is charged to oversee that authorities go through the judicial process that applies to search and seizure warrants and wiretaps in order to get to the data.[40] The potential for abuse by states that do not provide the necessary safeguards is considerable; law enforcement abilities surely need to evolve with technological innovations, but we believe that so should the systems for checks and balances. Now the permanent element of non stop surveillance makes its appearance, rendering these provisions a matter of great concern. It may very well be, at a fundamental level, an action that represents a turn-around shift in our democratic societies where we are all presumed innocent until proven guilty. We believe that a world where we are presumed guilty until proven innocent, where no one can be

[38] *Ibid.*
[39] *Ibid.* Articles 3 and 4 provide for the logging and retention of traffic data by Internet Service Providers (ISPs) anywhere from 1 to 3 years.
[40] *Ibid*. Article 7(d) provides that access to such data shall be defined by each state in national law. This is a concern also found in (CC, 2001), where neither measure calls for specific and adequate safeguards for access and interception of the data. It should be noted as well that Directive 2002/58/EC on Privacy and Electronic Communications sets out the conditions for EU Member States to be able to implement these measures into law, but they do not provide an specific standard for a system of checks and balances either. Beyond that, we find the technical and practical challenges that ISPs would face unimaginable given the amount of data that would need to be logged.

trusted, may not be what our ancestors had in mind. And it may not what we want. Yet all the elements are slowly falling in place, arising from the legitimate concerns of some for the security of their countries and from others who are inevitably prepared to abuse their power. But none of these problems are unsolvable. We can, and indeed it is our responsibility, to engage in peaceful dialogue to ensure that the transition into the digital age will preserve our liberties, not diminish or erase them.

But how do we engage in fruitful debate when it seems that only a relatively few are trying to make the case? It may be a good time now to seek to educate the younger generations on issues affecting their basic rights to safety and freedom. And it is to be hoped that we have made it clear that what we mean by educating is not a campaign to brainwash people for an ideological cause but rather, to inform them of the choices they still have, and to demystify the repeated message from our governments that we must balance civil liberties with security needs. We perhaps should remind and encourage them to ask themselves: Can I say I am safe if I have diminished liberty?

The Lawful Access Proposal in Canada

The lawful access question was first posed in Canada in 2002,[41] but a more concrete proposal was not put on the table until 2005 when the government started touring the country to initiate a second round of debate.[42] The draft proposal was introduced until late 2005, and all we had previous to that were presentations from government officials outlining what they wished to do. Nonetheless, it was enough to review and evaluate the

[41] Department of Justice Canada, Lawful Access Consultation website online at www.canada.justice.gc.ca/en/cons/la_al/ accessed 06.09.05.

[42] A meeting was held in Vancouver, BC, in March 2005 as part of the consultation process. Present were representatives from the Department of Justice and civil liberties groups, as well as the provincial government.

proposals.[43]

The government wants, *inter alia*, to update wiretapping laws to reflect technological advances. Some of the terms in these updates, however, have not been specifically defined and remain vague, leading again to the need to question possible abuses. Otherwise, the proposal paves the road to fulfill the requirements for ratification of the Convention on Cybercrime. We focus here on two of these items.[44]

The first measure is preservation orders. The Convention [CC, 2001] calls for granting law enforcement the power to order a telecommunications service provider (TSP) not to delete information held by it about the target in the order for a period of 90 days so that authorities may have time to seek a warrant in order to legally obtain the data. In the proposal, the Canadian Department of Justice (DOJ) also wants to grant law enforcement the authority to issue a provisional order, without court approval, so that law enforcement may seek a formal order within two weeks without the risk of having the data needed deleted from the TSP's cache. Aside from the technical changes and costs required, the proposal does not compel TSPs to delete the data if it is never requested or after it has served its purpose. Notwithstanding, the proposed measure is relatively sound, and the potential for abuse is not as high as similar measures implemented or proposed elsewhere. But the Canadian DOJ has failed to justify adequately, as one should in attempting to establish the guilt of a suspect, why the measure is necessary at all. We remain unconvinced that it is permissible to introduce new law without sound justification, as previously mentioned.

We now focus on access to subscriber information held by telecommunications

[43] In the following discussion we have but the hard copy documents distributed by the DOJ to attendees as our only reference as of writing time of this document. The government plans to compile a report on the consultation process in the future, but until then, we do not have any official or electronic based materials to refer the reader to.

[44] These can be found in Articles 16 to 21 of (CC, 2001).

service providers (TSPs). To better understand what the Canadian government is doing, we shall first discuss a relatively unknown measure that is already law.

Bill C-13

Although not introduced as a response to terrorism, [C13, 2004] was passed in March 2004 and contains language that mirrors some of what was proposed during the first lawful access consultation of 2002.[45] Since the purpose of bill C13 was to make several other amendments to the Criminal Code as well, it may have been a convenient way of passing into law part of a proposal that had raised privacy concerns.

Section 487.012 of [C13, 2004] created a 'general production order' that would require a third party in control or possession of data or documents relevant to an investigation to produce them for their utilization in the case. [FIPA, 2002] notes that general production orders did not exist previous to the first lawful access proposal, and proposes that the existence already in the Code of search warrants and assistance orders in the execution of said warrants might be equivalent. The government has never explained how those two measures combined would not be adequate, rather than introducing a new power that can be used for the investigation of any crime as opposed to serious offences. This places the burden of conducting what in effect is a warrant on a third party, who then becomes an agent of the state doing work that corresponds to law enforcement. Additionally, a specific production order (section 487.013) was also created for financial information. It uses the same language as the general order, except that it lowers the standard that would otherwise be required to obtain a search warrant (or a

[45] The curious reader might wish to examine this old proposal *supra* note 41. However, the most recent version of the proposal, addressed elsewhere in this paper, differs enough to render the former obsolete.

general production order), making it easier for law enforcement to obtain this type of record.

Extending power

Going back to subscriber information, the proposal includes a provision to allow an authorized person to demand, on written or oral request, without judicial approval, from a TSP any information in its possession or control regarding the name, address and prescribed identifiers[46] of any subscriber to its service. Such a request would have to be kept confidential by the TSP. This is a departure that lowers even more the standard of the specific production order found in bill C-13 above for law enforcement to get information. The Canadian DOJ argues that law enforcement needs to access this information in pre-criminal investigations. We are extremely concerned with a measure that puts the right to anonymity of individuals on the internet at risk, possibly eliminating that right altogether. While a partial system of oversight has been proposed, it is not clear who would supervise it and, because TSPs have to comply with such an order within 72 hours (30 minutes in an emergency), it is not clear if or how a TSP will be able to verify that the request is legitimate at the time it happens. This type of order is an example of how to create a policy that could result in serious privacy invasion, identity theft, and perhaps even a risk to an individual's physical safety. This provision alone may be the most worrisome in the entire proposal, and it may be carrying an unacceptable risk. Here the government may have gotten itself into a paradox by trading both liberties *and* security to obtain security. It publicly announced that lawful access legislation would be introduced in the fall of 2005 along with many other bills to

[46] These include a subscriber's name, address, telephone numbers, usernames, and dynamic IP addresses.

expand police powers for the mitigation of other crimes,[47] in what appears to be a move by government to attempt and pass several worrisome provisions with as little scrutiny as possible given the latest terrorist bombings in London.

I.3. EVIDENCE OF THE EROSION OF CIVIL LIBERTIES

I.3.1. The Impact of U.S. Law Overseas

For the sake of the war on terror, the United States would appear to have chosen the path of surveillance of almost everything and everyone everywhere. One has to wonder then if that means overriding the laws of other sovereign nations and what the response from those nations would be when it comes to the rights and freedoms of their citizens. We examine here what we consider are good examples of that situation in Canada and Europe.

Impact of the USA PATRIOT Act for information in the Canadian Government's hands

This question was first brought up by the British Columbia (BC) Government and Service Employees Union in an effort to stop the BC Ministry of Health Services from outsourcing the administration of BC's health insurance program to a private company, that is a subsidiary of a company in the U.S.[48] As a result, the Privacy Commissioner of BC launched a public consultation seeking input, and subsequently issued a report, on whether section 215, discussed in I.1.1.1, of the USA PATRIOT Act would 'permit U.S. authorities to access personal information of British Columbians that is, through the

[47] Speech of the Hon. Irwin Cotler, Minister of Justice and Attorney General of Canada, online at http://canada.justice.gc.ca/en/news/sp/2005/doc_31604.html accessed 08.19.05

[48] National Union of Public and General Employees, 'B.C. ignores privacy to outsource medical data to U.S.' (November 2004) online at www.nupge.ca/news_2004/n05no04c.htm accessed 04.21.05.

outsourcing of public services, in the custody or under the control of US-linked private sector service providers' [ICBC, 2004].

The report found a general consensus that the U.S. FISA Court could order a U.S. based company to disclose records held in a foreign country that are under that company's control. The question then becomes whether contractual arrangements between public organizations and private companies could effectively nullify the issue of control over records held. This is not clear, as the report points out that there have been cases in which U.S. courts found, under U.S. law, that such control exists regardless of any contractual arrangement, but other cases suggest that such arrangements may influence a U.S. court's findings.[49]

Further, assuming that such control is found, we can ask whether a FISA Court would issue a subpoena if Canadian (or in this case, BC) law prohibited it. Unfortunately, the report notes, U.S. courts have upheld such orders even where a foreign law prohibited it. It thus concludes that the possibility of a FISA Court issuing a subpoena under section 215 ordering the disclosure of records located in Canada exists.[50]

The findings of the report are reasonable, and illustrate the far reaching impact of laws such as the USA PATRIOT Act, [Patriot, 2001] as utilized by world powers. It brings forth a global concern where, in order to comply with powerful nations, other nations might be willing to sacrifice the rights of their citizens that they had previously committed to protect. Such a possibility undermines the democratic principles on which our society is based. Supposing that the U.S. 'Big Brother' issues an order for disclosure, would Canada give in or resist, especially in an age where the transfer of information is

[49] [ICBC, 2004] at p. 18.
[50] *Ibid*.

but a daily occurrence? Given the intricate ties between Canada and the U.S., an ideal solution would be for the U.S. to be respectful of the protection afforded Canadians by our laws.[51] Otherwise, there is likelihood that under the perceived needs of the U.S. to ensure its security, we, Canadians and others, risk losing our privacy to another country.

The European Union's Sharing of Passenger Records with the United States

Since the second half of last decade, the EU citizens' privacy has been guarded by the Privacy Directive,[52] which became the role model for privacy protection laws in democratic societies elsewhere. This protection was tested when the U.S. adopted the Aviation & Transportation Security Act requiring airlines flying into the U.S. to disclose all PNRs in their possession for those flights.[53] The U.S. has further required, under the Homeland Security Act since May 2002[54] that airlines flying to and from the U.S. must disclose such data to its Bureau of Citizenship and Immigration Services. The European Council (EC) approved in May 2004 the transfer of PNRs from EU airlines' databases to the DHS.[55] In particular, this meant that the negotiated terms agreed to were viewed as adequate under the Privacy Directive. Initially, the Article 29 Working Party (WP)[56] considered that these U.S. requirements were problematic with respect to the Directive,

[51] In particular the Canadian Charter of Rights and Freedoms, Constitution Act, 1982, being Schedule B, Part I, of the Canada Act 1982 (U.K.) 1982, c. 11; the Privacy Act (R.S.C. 1985, c. P-21); and the Personal Information Protection and Electronic Documents Act (R.S.C. 2000, c. 5).

[52] Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, restricts transfers of personal data from EU Member States to other countries outside the EU where the legal regime does not ensure an adequate level of privacy protection for individuals (Articles 25 and 26).

[53] Aviation and Transportation Security Act, s. 115. Public Law 107-71, 115 Stat. 597 (2001).

[54] Homeland Security Act of 2002, Public Law 107-296, 116 Stat. 2135.

[55] European Council Decision 2004/496/EC of 17 May 2004, available in the 'Commission decisions on the adequacy of the protection of personal data in third countries' page of the EUROPA website online at europa.eu.int/comm/internal_market/privacy/adequacy_en.htm accessed 04.21.05.

[56] The Working Party on the protection of individuals with regard to the processing of private data, is a body in charge of interpreting the provisions of the data protection Directive, *supra* note 52, under which it was established at Article 29.

establishing that the transmission of the data could only happen in accordance with the legislation of the Member States,[57] and calling for caution in such transfers and for U.S. authorities to ensure respect of the Directive.[58] Further, the WP established the conditions under which the EC could adopt a decision recognizing the adequacy of protection that the DHS would afford to EU citizens' PNRs under U.S. law,[59] again raising concerns as to how all the procedures would take place and what safeguards would exist. In the end, the EC signed an agreement with the U.S. under a belief that the DHS will protect the records adequately.[60] There are reasons to doubt that belief. First, as we will see in I.3.2.1, the TSA repeatedly tried to hide its gathering of PNRs from U.S. airlines in order to test the former CAPPS II and now Secure Flight. The agreement was adopted at a sensitive time when the TSA was under fire for requiring the transfer of such data, making it look as if the DHS saw the agreement as a guaranteed way of obtaining the data it needed without problems. That kind of behaviour, whether dishonest or not, simply does not inspire trust. Second, the European Parliament expressed its opinion that the agreement was not adequate, that parts could be illegal, and has taken the EC to court on this matter.[61] The EC would then appear to have a convenient way of policy laundering – it is not difficult to imagine that the EU would require the same from its 'allies,' and the result would be a virtual global surveillance system of all people. This would not be the direction to go if we are to place trust in our governments to protect our rights.

[57] Within the limits of Article 13 of the data protection Directive, *supra* note 52.
[58] Opinion 6/2002 of the Article 29 Working Party, *supra* note 56.
[59] *Ibid*. Opinion 4/2003.
[60] The agreement was signed in Washington D.C. on 05.28.04 and can be found *supra* note 55.
[61] See the Note from Legal Service, document 11876/04 (August 2004) to the Council of the European Union re European Parliament v. Council of the European Union (European Court of Justice case C-317/04)

I.3.2. Problems in the United States

I.3.2.1. The Ruling of the DOT and the Disclosure of Personal Information to the TSA

In a complaint filed by the Electronic Privacy Information Center (EPIC) and the Minnesota Civil Liberties Union, the U.S. Department of Transportation (DOT) ruled in September 2004 that the privacy policy of a company does not preclude it from sharing data with the federal government, specifically when asked to do so - it is required by law to make records, including passenger data, available to federal agencies upon demand.[62] The government would thus have what seems to be a significant surveillance power. Furthermore, that power has been used extensively even though it is against the privacy policies of airlines.

The Office of the Inspector General of the DHS released a report [DHSIG, 2005] on the TSA's use and dissemination of airline passenger data. It states that the agency was involved in 14 transfers of data during 2002 and 2003, involving more than 12 million passenger records. It further notes that the 'TSA did not ensure that privacy protections were in place for all of the passenger data transfers. While TSA applied privacy protections in some contexts, shortcomings were also apparent in the agency's related contracting, oversight, and follow-up efforts.'[63]

Similarly on June 6 of 2004, U.S. District Court Judge Paul Magnuson of Minnesota issued his decision dismissing seven consolidated lawsuits in a case concerning a class action against Northwest Airlines for breaching its own privacy policy by providing the

[62] News.com, 'DOT dismisses privacy complaint against Northwest' (September 2004) online at news.com.com/2100-1029_3-5369677.html accessed 04.21.05.
[63] (DHSIG, 2005) at p. 6-9.

National Aeronautical and Space Administration (NASA) with passenger data records for an aviation security research project, after the 9/11 terrorist attacks, reported the Associated Press.[64] Northwest provided NASA with data from the last three months of 2001. The records included names, flight numbers, credit card data, hotel reservations, car rentals and traveling companies, among others. The plaintiffs claimed that in addition to having violated its own privacy policy, Northwest had also violated the Electronic Communications Privacy Act, the Fair Credit Reporting Act and Minnesota's Deceptive Trade Practices Act by disclosing the records. Judge Magnuson said that 'although Northwest had a privacy policy for information included on the Web site, plaintiffs do not contend that they actually read the privacy policy prior to providing Northwest with their personal information… Thus, plaintiffs' expectation of privacy was low.' This argument has the potential of rendering all privacy policies posted on web sites unenforceable because it may not be practical for the average adult to have the time to read the fine print on all the documents he or she comes across in a single day. The protections and guarantees of any policy posted on a web site are then called into question, while possibly sending at the same time a message to companies that guarantees made in such policies could be ignored without facing tough legal consequences, subsequently hurting the credibility of the private sector's self-regulation and its claims that as a result no legislation is needed for protecting online privacy. Furthermore, Judge Magnuson said that 'attorneys failed to show that the plaintiffs were harmed by the data sharing' and that the disclosure of the passenger information 'would not be highly offensive to a reasonable person' because the information was not provided to the general public but to a government agency in the efforts to fight

[64] Forbes.com, 'Judge Rejects Passenger Data Lawsuits' (June 2004) online at http://www.forbes.com/feeds/ap/2004/06/09/ap1405352.html accessed 04.17.05

terrorism.

The situation points out a serious flaw in privacy protection in the U.S. fair information practices, to which companies have committed themselves. They would appear useless in the face of law enforcement demands, and so far the government has shown no consistency in protecting personal information that it is trying to use to make individuals safer. We are concerned that if this trend continues, the terrorists could win when we get to the point that neither liberty nor safety exist.

Another worrisome picture is how the TSA's actions continue to undermine public trust in their government. In a letter from GAO to Congress, it was revealed that the TSA collected personal information through commercial data brokers on at least 200 000 people whose names were not in the data originally demanded from airlines, in order to proceed with tests of Secure Flight.[65] In essence, the TSA did what it said it would not do.

I.3.2.2. US v. Councilman

The U.S. Court of Appeals for the First Circuit issued a decision on Jun 29, 2004, in the case of U.S. v. Councilman. The Electronic Frontier Foundation (EFF) reports that the court held that 'it was *not* a violation of criminal wiretap laws for the provider of an email service to monitor the content of users' incoming messages without their consent.' [66] The decision states that defendant, Bradford C. Councilman, was vice-president of Interloc, an online rare and out-of-print listing service that provided certain book dealer customers with an electronic mail address and acted as the service

[65] Wired News, 'Congress: TSA Broke Privacy Laws' (July 2005) online at http://www.wired.com/news/privacy/0,1848,68292,00.html accessed 08.19.05
[66] Electronic Frontier Foundation news, 'Online Privacy 'Eviscerated' by First Circuit Decision' (June 2004) online at http://www.eff.org/news/archives/2004_06.php#001658 accessed 04.17.05

provider. Councilman was in charge of the management of the email service as well as the book dealer subscription list of the company.[67] Around January 1998, Councilman directed company employees to put in place a system to intercept and copy before delivery all incoming communications from Amazon.com to the dealers subscribed. The government charged Councilman with violating the Wiretap Act, alleging that he 'conspired to intercept the electronic communications, to intentionally disclose the contents of the intercepted communications… and to use the contents of the unlawfully obtained electronic communication' to 'exploit the content of e-mail from Amazon.com… to dealers in order to develop a list of books, learn about competitors and attain a commercial advantage.'[68] In arriving at its decision, the court reasoned that – and other courts in the U.S. agree – the Wiretap Act does not protect any *temporary* electronic storage of electronic communications at a middle point. While the definition for wire communications included storage at a middle point in that Act, the PATRIOT Act superseded that definition by erasing that wording. Thus, wire and electronic communications are not protected when residing in storage other than the sender's or the intended recipient's. So it is due to the wording of the wiretap laws, that it is not possible to intercept electronic communications while in transit when they are stored at a middle point because, e.g. e-mail stored at a middle point does not constitute an electronic communication. The court itself in its reasoning admitted that 'it may well be that the protections of the Wiretap Act have been eviscerated as technology advances.'[69] Some of the reasoning was based on a previous case where the Secret Service seized a computer used to operate a bulleting board system (bbs), but which also temporarily

[67] United States Court of Appeals for the First Circuit. U.S. v. Councilman, Case No. 03-1383, pp 2. Online at http://www.ca1.uscourts.gov/pdf.opinions/03-1383-01A.pdf accessed 04.20.05
[68] *Ibid.* pp 3-5.
[69] *Ibid.* pp 9-12.

stored private, unretrieved e-mail as a service that the owner provided to subscribers of the bbs. After seizure, the Secret Service read and deleted the private messages. The court also ruled in that instance that the seizure of sent but unretrieved e-mail did not constitute an intercept for the purposes of the Wiretap Act. It is evident that this is a loophole in the law that should be addressed as soon as possible. Moreover, the courts also agree that the U.S. Congress intentionally excluded the words 'any temporary electronic storage,' meaning to provide less protection to electronic communications. The government took the case to the full appeals Court for a review en banc, after several privacy groups joined with prosecutors to request that the decision be overturned. The case has now been reinstated and sent back to the District Court.[70]

The line of reasoning of U.S. v Councilman can already be seen in other cases. Five months after the ruling of the 1st Circuit Court of Appeals, federal judge Gary Feess in a Los Angeles District Court dismissed charges against a California resident accused of utilizing a *key logger*, a device that intercepts signals from a keyboard as an individual types and records them for later retrieval, in violation of the Wiretap Act. The man, Larry Ropp, is a former employee of an Anaheim, California insurance company and was found in 2004 using the surveillance device on a secretary's computer.[71] At the time he was secretly helping consumer attorneys gather evidence against his employer. The judge concluded that use of the device does not violate federal wiretap law - based in part on U.S. v Councilman – but also brought to light other loopholes in the law. Prosecutors in the case argued that the tapped computer, on which the secretary composed electronic mail, was protected under the Wiretap Act which made it illegal to

[70] Associated Press, 'Intercepted E-mail Indictment Revived' (August 2005) online at http://abcnews.go.com/Technology/wireStory?id=1030346&CMP=OTC-RSSFeeds0312 accessed 08.22.05

[71] The Associated Press, 'Judge rules law doesn't apply from keyboard to CPU' (Nov. 2004) online at http://www.msnbc.msn.com/id/6590614/ accessed 05.07.05

covertly intercept electronic communications transmitted 'over a system that affects interstate or foreign commerce,' since it was connected to the company's national network. Judge Feess stated the 'court finds it difficult to conclude that the acquisition of internal computer signals that constitute part of the process of preparing a message for transmission would violate the Act' and proceeded to rule that the interception of keystrokes between the keyboard and the machine did not meet the interstate or foreign commerce clause in the Act.[72] The reasoning behind this idea is that a computer could be isolated from any network connection, internal or external, and the transmission of signals between the keyboard and the CPU would still be possible; that is, the network connection is irrelevant. Indeed, the ruling could paint a picture where the government has significant surveillance power in this field. Consider that the court also cited a 2001 case in which a federal judge in New Jersey similarly concluded the FBI did not violate the Wiretap Act by installing a covert key logger on the computer of an organized crime suspect, where authorities claimed that they had configured the device to stop logging when the computer was connected to the internet. Once again, it was admitted by a judge that this gross invasion of privacy may be unfortunate, and that it is up to Congress to 'cover bases untouched.'[73] Being in court for being a whistleblower is, however, also unfortunate for Mr. Ropp, who was merely trying to help authorities expose improper anti-consumer practices of his employer, making this a very delicate case, perhaps more so than the Councilman case.

[72] SecurityFocus News, 'Judge dismisses keylogger case' (Nov. 2004) online at http://www.securityfocus.com/news/9978 accessed 05.01.05
[73] U.S. v Ropp, Nov. 2004. (link currently unavailable)

I.3.2.3. US v. Al-Hussayen

This case illustrates the problem created by the amendments of sections 201 and 805 of [Patriot, 2001], as discussed in I.1.1.1. A jury in the case reached the verdict that Idaho student Sami Omar Al-Hussayen was not guilty of conspiracy to provide and conceal material support or resources to terrorists in the form of expert advice.[74] Al-Hussayen was a computer science graduate student at the University of Idaho and also the webmaster of several web sites and message boards serving the Muslim community, where many individuals that could be deemed to have controversial political or religious views gathered to exchange opinions. He was indicted by the U.S. and charged with having made false claims on his student visa application by engaging 'in computer web-site activities that exceeded his course of study… [including] expert computer services, advice, assistance and support to organizations and individuals… in the form of web-site registration, management, administration and maintenance,' claiming that many of these activities 'accommodated materials that advocated violence against the United States.'[75] The indictment did not state whether Al-Hussayen was the author of such materials, but cites such materials as being posted on his web sites by third parties.

The government clearly intended in that case to make the materials posted on a web site the responsibility of the webmaster. That could have made it a crime to provide a forum online for speakers, whenever the materials are not deemed appropriate for the interests of the U.S. We believe that providing space for others to voice their views is a service to the First Amendment of the U.S. constitution. Clearly the U.S. government thinks that it could count as assistance under section 805.

[74] Electronic Frontier Foundation news, 'Being a Webmaster for Controversial Islamic Websites Not a Crime' (June 2004) online at www.eff.org/news/archives/2004_06.php#001601 accessed 04.17.05

[75] See the Indictment, p. 6 in U.S. v. Al-Hussayen (2004), U.S. District Court of Idaho. Case No. 03-CR-48.

I.3.2.4. National Security Letters are Unconstitutional

Section 505 has already been found unconstitutional by a federal district court in New York.[76] The Amercian Civil Liberties Union (ACLU) joined an anonymous ISP ('John Doe' for the purposes of the litigation) in April 2004 in filing a lawsuit to challenge the government's authority to issue NSLs. In his opinion, the judge stated that the section violates the First and Fourth Amendments, finding the gag provision an unconstitutional prior restraint on free speech.[77] Moreover, the court believes that the statute, as it is currently applied by the FBI, 'exerts an undue coercive effect on NSL recipients.'[78] The NSL involved in this case, the judge reasons, directed John Doe to personally provide the information and prohibited him, his subordinates, agents or employees from disclosing the existence of the order to anyone, and further made no mention of the availability of judicial review for Doe to seek annulment or modification of the NSL or of the secrecy mandated by it, contrary to the government's contention that the statute can be interpreted to provide for litigation in order to enforce a letter or, conversely, for a recipient to seek judicial review of it. As it is worded, the statute makes no mention of these two factors, making it very vague. It is not clear whether a recipient could seek legal advice at all. The lack of procedural protections in the statute, in our view, renders it unconstitutional by violating the Fourth Amendment. The government's prosecution insisted, nonetheless, that an internet speaker 'relinquishes any interest in any anonymity, and any protected claim to that information, as soon as he releases his

[76] Press Release of the American Civil Liberties Union, 'In ACLU Case, Federal Court Strikes Down Patriot Act Surveillance Power As Unconstitutional' (September 2004), online at www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16603&c=282 accessed 04.21.05.
[77] American Civil Liberties Union, 'In ACLU Case, Federal Court Strikes Down Patriot Act Surveillance Power As Unconstitutional' (Sept. 2004) online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16603&c=282 accessed 08.22.05
[78] United States District Court, Southern District of New York. John Doe & ACLU v Ashcroft, et. al., Case No. 04 Civ. 2614 (VM) pp 38-45. Online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16596&c=262 accessed 08.22.05

identity… to his ISP.'[79] If we were to apply this line of reasoning, then anonymity would not be possible online any longer, contrary to what the constitution of the U.S. guarantees to its citizens, even if third party ISPs hold identifying information. The government sought to censor even non-sensitive information on almost every document the ACLU filed, including direct quotations from the *public law* in question.[80] In the meantime, it is not clear how frequently this new power has been used. Although blacked-out lists of NSLs have been obtained by the ACLU through Freedom of Information Act (FOIA) requests,[81] the FBI has not disclosed any statistical information about its usage.

I.3.3. Problems in Canada

I.3.3.1. Captives Without Charges

At the end of 2004, a three judge panel of the Canadian Federal Court of Appeal ruled that security certificates issued under [IRPA, 2001] are constitutional.[82] The appeal was made by Moroccan-born Adil Charkaoui, an international student at the University of Montreal pursuing a Master's degree in Teaching. He was accused of being a member of al-Qaeda and has been incarcerated for 29 months without being charged as of September 2005.[83] His case is one of five now known as the 'Secret Trial Five,' all of who are Muslim and none of which have been given the reasons for their detainment.

[79] *Ibid.* pp 73-83.
[80] American Civil Liberties Union, 'Government Gag Exposed' online at http://www.aclu.org/SafeandFree/SafeandFree.cfm?ID=16275&c=262 accessed 08.22.05
[81] See the section on documents obtained through FOIA litigations in the American Civil Liberties Union's webpage feature on the section 505 challenge, *supra* note 76, online at www.aclu.org/nsl accessed 04.21.05.
[82] See 'Security certificates constitutional: court' on CBC News online at www.cbc.ca/story/canada/national/2004/12/10/security-certificate-041210.html accessed 06.06.05
[83] According to the Coalition for Justice for Adil Charkaoui, online at www.adilinfo.org accessed 09.11.05

Charkaoui argues he was detained after having refused repeated requests by authorities to use his contacts in the Muslim community to become an informant for CSIS.[84] There have also been reports that the Canadian government has admitted that it does not have enough evidence to charge them of terrorism in a criminal court in Canada.[85] In 2005, these terror suspects are starting to get increased media attention thanks to the involvement of Canadian celebrity Alexandre Trudeau, who has stated he will testify on behalf of one of the suspects.[86] Due to increased coverage, we expect pressure on the government to mount and can only hope that given the review of anti-terrorist laws in Canada this year, Canadians will realize what we have argued in I.1.2.3.

I.3.3.2. Bullying of the Press

[ATA, 2001] raises concerns as it bears an impact on freedom of expression, particularly for the press, where journalists have traditionally had a right to obtain information from confidential sources, especially on sensitive issues of public interest where the information is not publicly available. These concerns are real, as a relevant case has already occurred in Canada, in January 2004.[87] In that instance, the Royal Canadian Mounted Police (RCMP) raided the home and office of journalist Juliet O'Neill in connection with leaked government documents relating to the case of Canadian citizen Maher Arar, of Syrian origin, who was deported from the U.S. to Syria where he was tortured. Mr. Arar was deported under allegations that he was linked to Al-Qaeda, and O'Neill published a story on his case in November 2003, citing a

[84] *Ibid.*
[85] The Toronto Star, 'Signs of sympathy for terror suspects' by Thomas Walkom (July 2, 2005) online at www.thestar.com (registration required). No-registration version online at www.zerra.net/freemohamed/news.php?extend.890 accessed 09.11.05.
[86] *Ibid*.
[87] Mapleleafweb.com, 'Journalist Raided by Royal Canadian Mounted Police' (February 2004) online at www.mapleleafweb.com/education/spotlight/issue_47/index.html accessed 04.21.05.

security source and a leaked secret government document. The RCMP used the provisions in the Act to obtain a search and seizure warrant, with the objective of obtaining evidence that might identify the source. Additionally, O'Neill was told she had been under surveillance for weeks, and that there were plans to charge her under the Act for concealing the source. To date, the charges have still not been laid, and it is not known whether the provision used will be included in the review of the Act.

Cases such as this could stifle freedom of expression and may intimidate journalists from publishing controversial stories from confidential sources. Thus, the legislation allows authorities to dissuade reporters from obtaining such information in the future.

I.3.3.3. Improperly Justified and Unused

None of the policies introduced in Canada has ever been adequately justified as necessary by the government, whereas all of them could be seen as convenient tools to make the job of law enforcement very easy and unchecked. The potential for abuse was never seriously weighed against the possible benefits. And to complete the picture, one of the measures in [ATA, 2001] has possibly never been used.

That provision would allow individuals to be brought to court for questioning when there are reasonable grounds to believe a terrorist activity will be carried out and to have supervisory conditions imposed on them.[88] Under certain criteria, an officer may simply arrest and detain a person *without warrant* if there are reasonable grounds to suspect detention of the person is necessary to prevent a terrorist activity.[89] A person could be compelled to testify and answer all questions, violating his or her right to avoid self

[88] Criminal Code, *supra* note 12, s. 83.3.
[89] *Ibid.* s. 83.3(4).

incrimination and the right to due process (and a fair and open trial).[90] The Canadian Department of Justice has reported in two consecutive years that these powers were not invoked.[91] We thus find the government not only failed to justify its quest for new powers, but it is in fact helping opponents of the legislation to argue against the necessity of such measures.

I.3.3.4. Are we safer?

In a submission to the Senate Special Committee in charge of the review of [ATA, 2001], the Privacy Commissioner of Canada 'called for the Government of Canada to carefully examine the continued need for the Anti-terrorism Act and to conduct an empirical assessment of the proportionality of the measures adopted in the interests of anti-terrorism' [PCC, 2005]. Furthermore, the Commissioner believes that there is a lack of evidence that the broad powers created by [ATA, 2001] have made us safer and that they may 'end up abolishing the very freedoms and democracy we claim to be defending' [PCC, 2005].

[90] British Columbia Freedom of Information and Privacy Association, submission to Canada's House of Commons Subcommittee on Public Safety and National Security, which is doing a review of (ATA, 2001).
[91] The reports on the use of these measures can be found on the Department of Justice Canada website online at canada.justice.gc.ca/en/anti_terr/impact.html accessed 04.28.05.

II. SECURITY AND CIVIL LIBERTIES – IS A TRADEOFF NEEDED?

In this chapter we examine the main arguments of both sides of the civil liberties debate and expose the opinion of civil society. We also present our concern with a possible lack of awareness by the Canadian public about their civil rights. Sections of this chapter are taken from or based on the author's previous works – [Estrada & Rosenberg, 2005a] and [Estrada & Rosenberg, 2005b] – as follows:

Section II.2.2.

Section II.4.

II.2.2. has been slightly modified for its inclusion here.

II.1. THE LAWMAKERS POSITION

II.1.1. No Adequate Tools to Fight Terrorism

On several occasions, the government of the world's power has justified the creation of laws with large potential to interfere with civil liberties by making claims that, prior to their enactment, legal tools were not available in the fight against terrorism.[92] Now, several years after 9/11, we begin to see the government claim that the fight against terrorism is being won because of those tools. In particular, former U.S. Attorney General John D. Ashcroft presented in mid-July 2004 a new report outlining the benefits that the USA PATRIOT Act has provided authorities by citing several examples, where controversial provisions of that law were used not only for anti-terrorism purposes but for common criminal cases as well.[93] The U.S. government claims that information can

[92] Prepared Remarks of Attorney General John Ashcroft on 'Report from the Field: The USA PATRIOT Act at Work' online at http://www.fas.org/irp/news/2004/07/ag071304.html accessed 04.20.05
[93] U.S. Department of Justice, 'Report from the Field: The USA PATRIOT Act at Work' (July 2004) online at http://www.fas.org/irp/agency/doj/patriot0704.pdf accessed 04.20.05

now be shared in ways that were 'virtually impossible' before the PATRIOT Act, and that the sunset clauses included in the act should be removed. U.S. President George W. Bush used this stance to promote his re-election.

Claims of this type are not new. The past 5 to 6 decades have often seen political statements of a strategic type to win the vote of citizens by inducing fear of foreign or domestic attacks on the nation.[94] This could lead many uninformed citizens to believe that they must give up certain freedoms in order to be safe.

Additionally, governments often insist that they have not committed any violations of the protections on civil liberties, and make strong use of speeches in the media to persuade citizens that they should not fear government actions, and to trust government to protect those liberties, ignoring that much of the information held in relation to the topic is classified. In fact, the U.S. Army has recently issued a report on the controversial disclosure of passenger data by JetBlue and other airline companies to the Transportation Security Administration.[95] The disclosure was against the privacy policies of the companies involved, but the report finds that 'technically' no privacy law has been violated since the information was not used other than for testing of controversial projects like CAPPS II.

Wiretapping of communications is seen as key in gathering evidence of criminal activity, and authorities believe it should be the responsibility of communications providers to implement easy wiretap access. Telephone networks are already accessible to authorities, but the internet infrastructure differs in that in its initial conception it does not include equipment to facilitate this task. Now governments want to have the

[94] Axis of Logic Critical Analysis, 'George W. Bush's Lasting Legacy to America: These Days of Fear' (July 2004) online at http://www.axisoflogic.com/cgi-bin/exec/view.pl?archive=65&num=10373 accessed 04.20.05

[95] Wired News, 'Army: JetBlue Data Use Was Legal' (August 2004) online at http://www.wired.com/news/politics/0,1283,64647,00.html accessed 04.20.05

accessibility they have with telephone lines, but do not wish to pay for the cost themselves.[96] Going further, the U.S. Department of Justice drafted a proposal for the 'Domestic Security Enhancement Act' to permit broader electronic surveillance – without court orders [Aden, 2003]. While the focus from enforcement officials is always on the threat posed by terrorists, all proposals and current legislation have been worded to extend to any type of potential criminal activity.

But some of the members of that government also feel a better job could be done without compromising civil liberties such as privacy, and that the extreme secrecy currently held should be revised.[97] Additionally, many government officials – as well as many observers and civil liberties activists – agree that a restructuring of the intelligence community is in order when we consider that its current modus operandi is not suited to today's global issues.[98]

Certainly many, including President Bush himself, have stated that a dictatorship would be much easier to manage than a democracy as it relates to national security.[99]

Although in the last four years and during the last decade of the 20th century the world has seen a decline in terrorist attacks [Human Security, 2004], the media attention to the latest high-profile cases such as the London bombings have helped governments pitch their argument that the current powers, and even extensions of them, are needed in order to continue the fight.

---

[96] The Washington Post, 'FCC Serves Up a Ruling Smorgasboard' (August 2004) online at http://www.washingtonpost.com/wp-dyn/articles/A42117-2004Aug5.html accessed 08.22.05

[97] Report of the Technology and Privacy Advisory Committee of the U.S. Department of Homeland Security, 'Safeguarding Privacy in the Fight Against Terrorism' (March 2004) online at http://www.epic.org/privacy/profiling/tia/tapac_report.pdf accessed 04.22.05

[98] The 9/11 Commission, 'The 9/11 Commission Report' (July 2004) online at http://www.epic.org/privacy/terrorism/911report.pdf accessed 04.22.05

[99] Moore, Michael (2004). 'Fahrenheit 9/11.' Lions Gate Films.

II.1.2. Fighting Crime in General

The Canadian government introduced the legislation [LA, 2005] discussed in I.2.2.2, in the fall of 2005.[100] In the announcement it was indicated that police needs to maintain the ability to lawfully intercept communications in the investigation of crime, so that they have the necessary tools to carry out their job.[101] It is, after all, law enforcement authorities who are requesting extended powers that have been granted in the U.S. and the Canadian government seems eager to comply. Together with the captivity of foreign nationals without charging them, it would seem the government does not want to appear to its neighbour in the south as doing nothing in the war on terror. With [LA, 2005] however, no consideration was given to limiting power only to serious crimes such as terrorism, nor to the possibility that the Criminal Code may have already provided the necessary tools for enforcement of the law, as we argued in I.2.2.2. In Canada, most new measures being introduced will cover crime in general, further emphasizing the desire of authorities to make their job easier and simpler and, unfortunately, that tends to negatively impact civil rights.

II.2. WHAT ARE CITIZENS THINKING?

II.2.1. Opposition to the USA PATRIOT Act

We must pay attention to the as-of-yet small but undeniable representation of a portion of the population's stance against government surveillance. More specifically, said people's stance against the controversial provisions of the PATRIOT Act.

[100] Speech of Hon. Irwin Cotler, Minister of Justice and Attorney General of Canada to the Canadian Association of Police Boards (Augus 18, 2005). Online at canada.justice.gc.ca/en/news/sp/2005/doc_31604.html accessed 09.08.05
[101] *Ibid.*

For the last few years, several municipalities in the U.S. have been passing resolutions opposing the PATRIOT Act. The movement began in 2001 with the Bill of Rights Defense Committee, with Ann Arbour, Michigan being the first community to oppose the act.[102] They argue that the Act gives law enforcement too much power and threatens civil rights.

But even before the Act was passed by Congress, the police department in Portland, Oregon, told the Justice Department it was not willing to cooperate with the FBI on investigations of Middle Eastern students in that city.[103] They argued that state law prohibited police from questioning immigrants not suspected of a crime. Similarly, City Councillors in Ann Arbor expressed their concern about the potential discrimination that could be carried on against members of that community.

As of August 2005, 386 cities and counties and seven states have passed resolutions declaring that "their communities will uphold the constitutional rights of their residents should federal law enforcement agents come knocking on the door of local authorities for assistance in tracking residents"; the population living in these communities amounts to 61,881,073 people or ~ 20.9% of the total U.S. population.[104] These resolutions have no power over the actions of the federal government since local governments do not posses authority over federal law enforcement.

Nancy Talanian, head of the Bill of Rights Defense Committee, has stated that the movements across the communities have acted and drafted their resolutions independently of her group, and consist of coalitions of very different demographic and politically inclined groups; from peace groups to veteran groups, from conservative

[102] The Bill of Rights Defense Committee online at http://www.bordc.org/ accessed 04.23.05
[103] ABC News, 'Patriot Revolution?' (July 2002) online at http://abcnews.go.com/sections/us/DailyNews/usapatriot020701.html accessed 04.23.05
[104] *Supra* note 102.

libertarians to liberal civil rights activists.[105]

This opinion has been growing since the end of 2003 when the National League of Cities (NLC), at its annual meeting, adopted a resolution calling for Congress to amend parts of the PATRIOT Act.[106] The NLC is the largest group in the U.S. of elected municipal government officials, representing 18,000 cities with approximately 225 million residents. Charlie Lyons, the NLC president, called for a partnership between cities and towns and the federal government regarding homeland security so as to perform that job efficiently while preserving civil liberties. The resolution also urged the President and the executive branch to 'review, revise and rescind executive orders and policies adopted since the terrorist attacks that limit or compromise the liberties guaranteed by the Constitution and the Bill of Rights.'[107] Among the concerns that the NLC stated in its resolution[108] are:

- 'Permit the FBI Director to seek records from bookstores and libraries including books of patrons based on minimal evidence of wrongdoing and prohibits librarians and bookstore employees from disclosing the fact that they have been ordered to produce such documents (Section 215);
- 'Permit law enforcement authorities to have broad access to sensitive mental health, library, business, financial, and educational records despite the existence of previously adopted state and federal laws which were intended to strengthen the protection of these types of records (Sections

[105] Wired News, 'Cities Say No to the Patriot Act' (June 2004) online at http://www.wired.com/news/privacy/0,1848,63702,00.html?tw=wn_story_related accessed 04.23.05
[106] The Washington Times, "Cities in revolt over Patriot Act" (Jan. 2004) online at http://www.washtimes.com/national/20040104-113441-7305r.htm accessed 04.24.05
[107] National League of Cities, 'Amend PATRIOT Act Urges National League of Cities' (Dec. 2003) online at http://www.nlc.org/nlc_org/site/newsroom/nations_cities_weekly/display.cfm?id=A67738D3-53FA-4D79-BCDB0AFE3000B99E accessed 04.24.05
[108] *Ibid.*

215, 218, 358, and 508);

- ‘Give the Secretary of State broad powers to designate domestic groups as ‘terrorist organizations’ and the Attorney General power to subject immigrants to indefinite detention or deportation even if no crime has been committed (Sections 411 and 412); and
- ‘Impose an unfunded mandate on state and local public universities that must collect information on students who may be of interest to the Attorney General (Sections 507 and 508).’

II.2.2. Lesser Coverage in Canada?

In contrast to all the media and public attention that civil liberties get in the U.S., Canadian citizens, with the exception of civil liberties groups, a few academics, and the Privacy and Information Commissioners of Canada, give the impression that they may not care as much as one might think, despite their close relationship with their neighbours to the south.

II.2.2.1. Lack of Awareness?

One must wonder whether measures are able to pass due to consent of the Canadian public, or due to a lack of awareness of what powers exactly law enforcement wants. What very little information is available on the subject seems to unfortunately point to the latter. [Roach, 2005] cites the Canadian Public Safety Minister as confident that the public is on the government’s side, quoting the results of a late 2004 survey on whether the public agrees Canada has responded appropriately to terrorism. Given the results (50% agree, 43% think Canada has *not gone far enough*, while only the remaining 7%

believe the government has gone too far), however, the articles raises a genuine concern for whether Canadians are aware of what is being done to counter terrorism.

In a small prelude to a study of electronic surveillance and privacy that is to be carried out internationally, [Zureik, 2004] notes that people do not place a high priority on protecting personal information, and that few know the basics about Canadian privacy laws and the technologies utilized to gather information on individuals. It finds the public is 'prone to accept or endorse by default current privacy practices with little awareness of the personal or societal implications of existing laws or the technology itself.' A further indicator of complacency from the public might be found in the remarks by Canada's Information Commissioner that 'Canadians have proven to be extremely, perhaps inexplicably, restrained in their use of the Access to Information Act.'[109]

It may be that the apparent lack of information regarding the public's awareness provides further anecdotal evidence that the Canadian public is not well informed on issues of privacy.

II.3. WHERE CIVIL LIBERTIES GROUPS STAND

The U.S. is probably the country where civil liberties groups are involved in the most lawsuits against government when it comes to privacy, freedom of speech and freedom of information access requests. Among the most popular and larger groups that take a significant focus on government policy with respect to technology, you can find the American Civil Liberties Union (ACLU), the Center for Democracy and Technology

[109] Remark by John M. Reid, Information Commissioner of Canada, to the 3rd International Conference of Information Commissioners in Cancun, Mexico in February 2005. Online at www.infocom.gc.ca/speeches/speechview-e.asp?intSpeechId=110 accessed 06.10.05

(CDT), the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC). What exactly is the issue according to them?

It is common knowledge today that history has provided several examples where at times of national crisis, civil liberties come under enormous pressure, with the opinion often being that a temporary restrain on such liberties is worth the benefit of overcoming a crisis.

The ACLU cites two examples illustrating this point: the thousands of deported civilians because of their political views during the 'Red Scare' of the early 1920s; and the infamous blacklisting during the era of U.S. Senator Joseph McCarthy that ruined lives and careers in the 1950s. The organization's general view is that the 'First Amendment exists precisely to protect the most offensive and controversial speech from government suppression. The best way to counter obnoxious speech is with more speech. Persuasion, not coercion, is the solution.'[110] The ACLU has been critical of several legislative measures taken and proposed by the U.S. government, e.g. the PATRIOT Act, citing concerns that such powers that extend the surveillance power of federal law enforcement chill speech protected by Amendment I of the U.S. constitution.

The EFF, EPIC and the CDT share this view, and have concentrated their resources on the analysis of both current and proposed legislation that has a direct impact on internet censorship. Censorship cannot only result from legislation designed for homeland security as can be seen in the controversial debate of how to regulate obscene speech on the internet. But for the purposes of this dissertation, there shall be little or no focus on that debate, as it is beyond the scope of our thesis on the trade-off between

[110] American Civil Liberties Union on Free Speech, online at http://www.aclu.org/FreeSpeech/FreeSpeechMain.cfm accessed 08.22.05

civil liberties and security.

The argument of these groups can be summarized nicely in the following excerpt from EPIC's PATRIOT Act website which states that the Act:

> 'introduced a plethora of legislative changes which significantly increased the surveillance and investigative powers of law enforcement agencies in the United States," and that it "did not, however, provide for the system of checks and balances that traditionally safeguards civil liberties in the face of such legislation.'[111]

The claim here is that the government authority to investigate has been increased specially with respect to the internet.

II.4. RHETORIC OF WAR AND FEAR

To end this discussion, we would like to present a few quotations from U.S. President George W. Bush in his 'Address to a Joint Session of Congress and the American People' delivered a few days after 9/11[112] (except one that is from a subsequent address). We propose that they can be categorized according to a rhetoric, and thus possibly reveal two victories for *terrorism warriors*. Part of the motivation in identifying these quotations is to explain the drive to restrict basic civil liberties by politicians and bureaucrats alike. We find it is important to respond to their efforts with a renewed commitment to support basic civil liberties and to resist their erosion.

First there is a rhetoric of permanent war:

- '… enemies of freedom committed an act of war against our country.'

[111] Introduction to the EPIC USA PATRIOT Act page, Electronic Privacy Information Center. Online at http://www.epic.org/privacy/terrorism/usapatriot/ accessed 04.24.05

[112] Delivered on September 20, 2001. The address can be found in the White House website online at www.whitehouse.gov/news/releases/2001/09/20010920-8.html accessed 04.25.05.

- ‘Our war on terror begins with al Qaeda, but it does not end there. It will not end until every terrorist group of global reach has been found, stopped and defeated.’
- ‘Americans should not expect one battle, but a lengthy campaign, unlike any other we have ever seen.’
- ‘… the only way to defeat terrorism as a threat to our way of life is to stop it, eliminate it, and destroy it where it grows.’
- ‘I ask for your patience, with the delays and inconveniences that may accompany tighter security; and for your patience in what will be a long struggle.’

We believe that by declaring a war on terrorists, and labelling their acts as acts of war, President Bush granted these individuals, who before were mere criminals, a status of soldiers fighting for a cause. Furthermore, not only does he affirm that this will be a long battle, but also gives evidence that it is a permanent war, since it may not be possible to eliminate every single terrorist on the planet. Consider the following quotations illustrating a rhetoric of retaliation:

- ‘Our grief has turned to anger, and anger to resolution.’
- ‘These demands are not open to negotiation or discussion. The Taliban must act, and act immediately. They will hand over the terrorists, or they will share in their fate.’
- ‘They are the heirs of all the murderous ideologies of the 20th century.’
- ‘Every nation, in every region, now has a decision to make. Either you are with us, or you are with the terrorists.’

Here he made clear that the U.S. would have its way, and anyone who objected

would also be punished. We believe such a rallying cry serves to contribute to the pressure to constrain civil liberties in order to supposedly satisfy the goal of apprehending terrorists thereby increasing the security of the nation. However, it may be that the hope of witnessing an end to the war on terror is diminished under such a philosophy.

Finally, consider additional instances of a rhetoric of fear:

- 'Tonight we are a country awakened to danger… '
- 'There are thousands of these terrorists… to plot evil and destruction.'
- 'These terrorists kill not merely to end lives, but to disrupt and end a way of life. With every atrocity, they hope that America grows fearful…'
- 'Terror, unanswered, can not only bring down buildings, it can threaten the stability of legitimate governments.'
- 'Thousands of dangerous killers… are now spread throughout the world like ticking time bombs, set to go off without warning.' [113]

With seemingly never ending statements of this kind, that constantly remind citizens that there exist individuals who commit atrocious crimes, can we expect that citizens will not continue to live in fear? As long as this fear is fuelled, people may find it difficult to recover from the events of 9/11. And consequently, they may be willing to give up certain liberties in order to feel safe. But as long as they feel fear, they may never feel truly safe and free, resulting in another vicious circle. As Bush himself said in the address, 'freedom and fear are at war.' We believe they do not need to be.

It is important to be clear that the present purpose is not to speculate whether this is a strategy by governments to coerce their citizens. That does not matter, for the

[113] The President's State of the Union Address, January 29, 2002, can be found at the White House website online at www.whitehouse.gov/news/releases/2002/01/20020129-11.html accessed 04.25.05.

statements have already been delivered. We believe it is important to bring attention to the results this campaign has had both in the short and long run. Finally, one last quotation by President Bush that we agree with is ironically also part of the address discussed above:

> ‘*We are in a fight for our principles, and our first responsibility is to live by them.*’

III. CONCLUSION

This dissertation includes some of what we consider to be the most relevant legal and technological measures, as they relate to cyber space, that North America and Europe have adopted or are proposing in order to evaluate their impact on our liberties. Indeed, there seems to be a premise that the more information governments have about everyone the safer we will all be. This premise would illustrate that governments' fear of the unknown has resulted in the creation of measures such as lawful access and total surveillance systems such as Secure Flight, as a response. But governments cannot implement these alone and wish to compel the private sector to act as agents of the State in the fight not only against terrorism, but crime in general.

Nevertheless, we remain unconvinced that all of the measures are necessary. Terrorism has always been a fact of life and resources were already available to deal with it. New measures have not always been adequately justified and, even if some of them have been, there are no adequate built-in systems of checks and balances in order to repair any mistakes or abuses that may occur during their use. Furthermore, governments are walking a dangerous path in allowing technology to drive policy as appears to have been the case with DARPA in the development of programs such as Secure Flight. Similarly, the Canadian government appears to walk a thin line in utilizing policy laundering as could be the case with their proposal on lawful access with the alleged objective of ratifying the Convention on Cybercrime. These actions and the examples of the erosion of freedom given in this work have only served to undermine public trust and further exacerbate our concerns with governments' handling of security.

We are therefore not convinced that reducing the rights and freedoms of individuals

is going to prevent further threats to their safety by terrorists. This observation is particularly important when we consider the rhetoric of fear. We are concerned that individuals will give away some of their freedoms in exchange for what is essentially a false sense of safety, resulting in a 'lose-lose' situation. Our governments may have engaged us in a war between freedom and fear, and unless society's fear is healed, freedom could continue to erode.

What concerns us even more is that Canadians (and citizens around the world, for that matter) may face an enemy that is virtually invisible in the possible lack of awareness to what our government is exactly doing to combat crime. We would in effect be blind to that enemy. We need to be educated on our rights and obligations. Otherwise, tomorrow our children may no longer know the difference between liberty and 'liberty subject to surveillance.' The government should seriously consider the effect of laws that were not drafted with only temporary crisis in mind, before they become the established norm for our future generations.

There does not need to be a balance or trade-off between civil rights and security. We believe technology can accommodate and facilitate both the freedom and safety of individuals without necessarily sacrificing one for the other. We are not opposed to improving security. We encourage its development insofar as adequate safeguards to our freedoms are put in place at the same time and adequate responses to abuses are seen to be effective. A general intelligence overhaul would be preferred to passing legislations such as the USA PATRIOT Act.

Our stance is that, if we hope to have any meaningful security, then it is time to stop the campaign of war and fear. As James Madison, 4th president of the United States once stated in 1793:

‘Of all the enemies to public liberty, war is, perhaps, the most to be dreaded, because it comprises and develops the germ of every other. War is the parent of armies; from these proceed debts and taxes; and armies, and debts, and taxes are the known instruments for bringing the many under the domination of the few. No nation could preserve its freedom in the midst of continual warfare.’

IV. REFERENCES

[Aden, 2003] Aden, Steven H. (2003), Taking Liberties in the War on Terror: The Justice Department's 'Partriot Act II,' The Rutherford Institute. Online at www.rutherford.org/articles_db/legal_features.asp?article_id=36 accessed 04.22.05.

[ATA, 2001] Bill C-36, An Act to amend the Criminal Code, the Official Secrets Act, the Canada Evidence Act, the Proceeds of Crime (Money Laundering) Act and other Acts, and to enact measures respecting the registration of charities, in order to combat terrorism (Anti-Terrorism Act). 1st Session, 37th Parliament, 2001. R.S.C. 2001, c. 41.

[C13, 2004] Bill C-13, An Act to amend the Criminal Code (capital markets fraud and evidence-gathering). 3rd Session, 37th Parliament, 2004. R.S.C. 2004, c. 3.

[CC, 2001] Council of the European Union (Budapest, November 23, 2001) Convention on Cybercrime. Online at conventions.coe.int/Treaty/en/Treaties/Html/185.htm accessed 04.17.05.

[DARPA, 2003] United States Defense Advanced Research Projects Agency (May 2003) Report to Congress regarding the Terrorism Information Awareness Program. Copy online at www.epic.org/privacy/profiling/tia/may03_report.pdf accessed 04.21.05.

[DHSIG, 2005] Department of Homeland Security Office of Inspector General (March 2005) Review of the Transportation Security Administration's Role in the Use and Dissemination of Airline Passenger Data. Office of Inspections, Evaluations, & Special Reviews, report OIG-05-12.

[E-PH, 2004] Escudero-Pascual, A. and Hosein, I. (2004) Questioning Lawful Access to Traffic Data. *Communications of the ACM*, Vol. 47, No. 3, 77-82.

[Estrada & Rosenberg, 2005a] Estrada, J. G. and Rosenberg, R. S. (2005), The assault on civil rights in the international fight against terrorism. Proceedings of the 6th International Conference of Computer Ethics: Philosophical Enquiry, July 17-19, 2005, The Netherlands.

[Estrada & Rosenberg, 2005b] Estrada, J. G. and Rosenberg, R. S. (2005), Invisible Enemy? Canada's Blindness in an Age of 'War on Terror.' To appear in Proceedings of the 8th ETHICOMP International Conference on the Social and Ethical Impacts of Information and Communication Technologies, September 12-15, 2005, Sweden.

[FIPA, 2002] British Columbia Freedom of Information and Privacy Association (2002), Comments on the Lawful Access Consultation Document, online at fipa.bc.ca/library/Reports_and_Submissions/Lawful_Access_Submission-Dec_16_2002.doc accessed 06.09.05

[GAO, 2004] United States Government Accountability Office (February 2004) Aviation Security: Computer-Assisted Passenger Prescreening System Faces Significant Implementation Challenges. Report to Congressional Committees GAO-04-385.

[GAO, 2005] United States Government Accountability Office (March 2005) Aviation Security: Secure Flight Development and Testing Under Way, but Risks Should Be Managed as System Is Further Developed. Report to Congressional Committees GAO-05-356.

[Gratl, 2005] Gratl, J. (2005), Security Certificates, online at www.bccla.org/positions/antiterror/05Security Certificates.htm accessed 06.06.05

[Han & Kamber, 2001] Han, J. and Kamber, M. (2001). *Data Mining: Concepts and Techniques*. Morgan Kaufmann Publishers. San Francisco.

[Human Security, 2004] Human Security Centre (2004). The Human Security Report. To be published by Oxford University Press, USA.

[ICBC, 2004] Information & Privacy Commissioner of British Columbia (October 2004) Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing. Online at www.oipcbc.org/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf accessed 04.17.05.

[IRPA, 2001] Immigration and Refugee Protection Act. 1st Session, 37th Parliament, 2001.R.S.C. 2001, c. 27, s. 76-87.

[LA, 2005] Report on the second round of Lawful Access consultations (2005). Not yet available for release.

[Patriot, 2001] Bill H.R.3162, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT) Act of 2001. U.S. Public Law 107-56, 115 Stat. 272 (2001).

[PCC, 2004] Privacy Commissioner of Canada (2004), Annual Report to Parliament 2003-2004, pp. 12-14, online at www.privcom.gc.ca/information/ar/200304/200304_e.pdf accessed 06.09.05

[PCC, 2005] Privacy Commissioner of Canada News Release (2005), Contained surveillance and increased oversight needed in Anti-terrorism Act to protect against loss of privacy rights, online at www.privcom.gc.ca/media/nr-c/2005/nr-c_050509_e.asp accessed 06.10.05

[PSA, 2004] Bill C-7, An Act to amend certain Acts of Canada, and to enact measures for implementing the Biological and Toxin Weapons Convention, in order to enhance public safety (Public Safety Act, 2002) 3rd Session, 37th Parliament, 2004. R.S.C. 2004, c. 15.

[Roach, 2005] Roach, K. (2005), Should Canadians be concerned with Canada's anti-terrorism efforts?, online at www.opinion-canada.ca/en/articles/article_147.html accessed 06.10.05

[Zureik, 2004] Zureik, E. (2004), What Canadians Think about Privacy, The Surveillance Project at Queens University, online at www.queensu.ca/sociology/Surveillance/home.htm accessed 06.10.05