Office of the
Privacy Commissioner
of Canada

Commissariat
à la protection de
la vie privée du Canada

Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States

Backgrounder to the Standing Committee on Public Safety and National Security

Review of the Findings and Recommendations of the Internal Inquiry into the Actions of Canadian Officials in relation to Abdullah Almalki, Ahmad Abou-Elmaati and Muayyed Nureddin (Iacobucci Inquiry) and the report from the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar (Arar Inquiry)

May 7, 2009
Ottawa, Ontario

Jennifer Stoddart
Privacy Commissioner of Canada

TABLE OF CONTENTS

Executive Summary

The purpose of this survey is to examine the surveillance powers granted to government in several countries that have experienced recent acts of terrorism. The hope is that by examining the statutory basis for surveillance powers in the US, Canada, UK and France, a comparative picture of legal trends impacting state surveillance powers would emerge. Currently, there is much anecdotal discussion pitting the laws of one country against another, but little evidence-based analysis.

Since 2001, in all the countries reviewed, security concerns and an expanded role for police in combating terrorism has led to more investigatory, intelligence gathering and information sharing powers for police and intelligence agencies. However, legal and logistical approaches to intelligence gathering differ from country to country. Models for judicial oversight, administrative review and ministerial authorization also differ.

In the US, the *USA PATRIOT Act* (2001) significantly altered interception laws, extending the period of their applicability and placing less specific constraints on their use. Policing and intelligence agencies were also given a strong mandate to gather and share more intelligence across jurisdictions. In Canada, under the *Anti-Terrorism Act* (2001), restrictions on interception of communication in national security investigations were also loosened considerably. Canada's signals intelligence agency, the CSE, has been given a concrete mandate to assist police and security bodies in their investigations. In the UK, the *Anti-terrorism, Crime and Security Act* (2001) explicitly requires telecom companies to retain customer communications data for criminal investigations and national security purposes. Companies must assist agencies in carrying out interceptions. In France, the *Loi pour la sécurité quotidienne* (2003) entails broad anti-terrorism provisions, data retention provisions requiring companies to log customer activities and gives government access to encryption keys.

It is also important to note that each nation has its own system for authorizing surveillance. In the US and France, orders authorizing interceptions within the country are issued by judges. In Canada, depending on the purpose, surveillance is authorized either by the appropriate Minister or warrants issued in a Superior Court. In the UK, executive warrants are issued by the Home Secretary.

Finally, in each country examined, the administrative requirements for national security warrants are significantly less than those for criminal investigations. In the UK and France, the specific interests of national security that investigations seek to safeguard need not be defined. In the US, applications are not required to demonstrate probable cause in instances concerning national security. Similarly, in Canada, to issue law enforcement warrants, a court must consider whether surveillance is a last resort. This is no longer required for national security investigations.

Introduction

Purpose and scope of the review

The purpose of this survey is to examine the surveillance powers granted to government in several countries that have experienced recent acts of terrorism. The hope is that by examining the statutory basis for surveillance powers in the US, Canada, UK and France, a comparative picture of legal trends impacting state surveillance powers would emerge. Currently, there is much anecdotal discussion pitting the laws of one country against another, but little evidence-based analysis.

Given time constraints and to usefully limit the scope, this review will focus exclusively on a) laws governing the activities of state agencies as they monitor, intercept, collect, search and analyse communications, b) governments' ability to seize, collect and search for physical documents and other items, and c) the legal mandate of authorities to share that intelligence. Surveillance laws form the heart of these powers. While a whole range of inter-governmental instruments, internal regulations and administrative procedures also exist to provide for information gathering and sharing by state authorities – none of this is codified in law.

Finally, it is frequently the nature of individual national programs, not laws or treaties, which have the greatest visible impact upon citizens' privacy. To use only one example, both French and British police are entitled to check identification for any person without justification. Of 15 European Union member states, eleven have mandatory national identification card systems. These are long-standing normative differences that would likely bring public outcry if implemented in North America. Other monitoring programs and database (e.g. NSEERS in the EU or US-VISIT in the US) have generated controversy for their impact on travellers' privacy. However, detailed analysis of specific security programs (e.g. tracking terrorist financing, DNA collection, and national ID card programs) do not fall in the bounds of this review.

Historical context

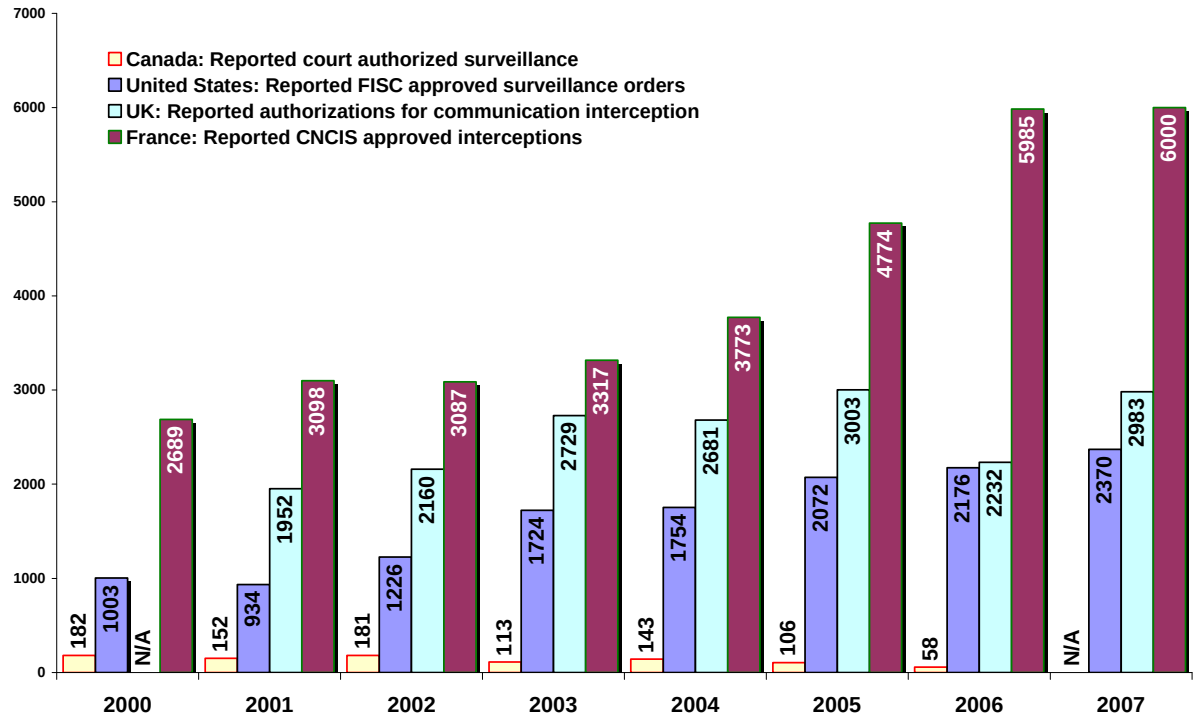
In reviewing laws governing surveillance in each of the countries selected, it is worth noting each nation has had significant (and traumatic) experiences with domestic and foreign terrorism over the past several decades. For example, the UK experience with violent ultra-nationalists (e.g. National Front) or independence movements (e.g. IRA), mirror North American concerns over political extremists in the United States and Canada (e.g. right-wing militias, FLQ). Similarly, the United States is not alone in having been targeted by international terrorism, as Canada (Air India), the UK (Pan-Am 103) and France (Paris bombings) all suffered deadly attacks in the 1980s.

However, since September 2001, there have been widespread legal developments in each country. Laws have moved either in increments (e.g. UK and France) or quickly (e.g. US and Canada) as politicians, bureaucrats and other officials have sought to restructure judicial and administrative oversight structures for surveillance operations.

In the US and Canada, these changes were largely effected by single pieces of omnibus legislation: namely the *USA PATRIOT Act* and *Anti-Terrorism Act*, respectively. Conversely, since 2000 in both France and the UK, a steady stream of new laws have modified or expanded surveillance powers already in place.

One crude indicator of these expanding surveillance activities is to track instances of authorized surveillance. Responding to demands for transparency by legislators, each country has in place some form of public reporting on the use of surveillance by state authorities (see below). Taking into account the relative size of each country, it is interesting to note the relative growth (or decline) in approved surveillance since 2000.

Federally reported interception authorizations, by country (2000-2007)



However, it is important to state these figures rarely encompass surveillance activities that require no judicial authorization, namely those interception powers used for counter-intelligence or combating terrorism. In the UK and France, details of these activities are still considered state secrets. As well, purely foreign interceptions take place in a grey area outside domestic reporting requirements. Since the beginning of the Cold War, global intelligence gathering has evolved from the premise that foreign-based interception falls outside national statutes governing the privacy of communications. Like international waters, interceptions of external communications are not subject to the same legal, judicial or administrative oversight that is found on home soil. Similarly, at least three of the four nations surveyed (US, UK and Canada) set in place the infrastructure to share intelligence information as allies, quite apart from national legal constraints.

Comparison of New Powers

Ease limits on intelligence operations

- In the United States, several laws passed since September 11, 2001 allow for expanded criminal and foreign intelligence gathering within the country.
- Most notably, the 2001 USA PATRIOT Act (PATRIOT) allows government agencies to gather "foreign intelligence information" from both U.S. and non-U.S. citizens, removed legal distinctions between criminal investigations and surveillance for the purposes of gathering foreign intelligence and eliminated statutory requirement that the government prove a surveillance target is a non-U.S. citizen. [1]
- In 2007, the US Congress amended the *Foreign Intelligence Surveillance Act* (FISA) permitting warrantless surveillance of US citizens when one party to the conversation may be outside of the United States. In addition, the Attorney General and Director of National Intelligence can 'can authorize jointly, for a period of up to one year the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information' even if all the communications to be acquired originate or terminate in the US. [2]
- In 2001, Canada's *Anti-Terrorism Act* (ATA) extended powers to Canada's signals intelligence organization, the Communications Security Establishment (CSE). Under particular circumstances, authorized under a revised section 273.65 of Canada's *National Defence Act*, the CSE can now intercept communications originating or terminating in Canada. [3]
- The United Kingdom has also greatly eased legal restraints on domestic surveillance operations, most notably in the 2000 *Regulation of Investigatory Powers Act* (RIPA). This Act allows the Home Secretary or a range of delegated officials directing criminal or national intelligence to issue warrants for the interception of communications and requires all Communications Service Providers to provide a "reasonable interception capability" in their networks for surveillance in national security investigations. [4]
- RIPA also allows senior members of the civilian and military police, customs, and members of the judiciary to demand that users hand over the plaintext of encrypted material, or in certain circumstances decryption keys themselves.
- In addition, the 2005 *Prevention of Terrorism Act* empowers the UK Home Secretary to issue data retention directives to all communications providers for the purpose of protecting national security or preventing or detecting crime that relates to national security.
- Under these data retention laws, communications data must be retained and made accessible to authorities for up to one year. Recently, the government has proposed modifying the Act (and RIPA) to make data retention mandatory and expanding its use to include serious crimes, not just terrorism offenses.
- France has followed a similar tack. The *Loi pour la sécurité quotidienne* (LSQ), while introduced prior to September 2001, was passed in 2003 and included certain "anti-terrorism" amendments regarding data retention. The LSQ requires ISPs to store log files on customers' activities for up to one year and gives

government access to private encryption keys.[5] Although the measures were initially to sunset in December 2003 and be limited to terrorism investigations, the subsequent *Loi pour la sécurité intérieure* (LSI) extended the provisions, giving them general and definitive application.

- The *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) imposes an obligation on ISPs, telephone companies and any organization giving the public access to the Internet to provide client information to anti-terrorism authorities upon request, including IP addresses, location where equipment was used, list of calls made, individuals involved and the date of communications. Following implementation of the Act, French media reported that police and intelligence services have established the technical platform allowing them to easily collect traffic data related to text messages, mobile or Internet.[6]
- As well, the *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* gives anti-terrorist intelligence services access to France's national administrative databases, to which they did not have access prior to 2006.
- Under French data retention statutes, security services can pinpoint who has contacted whom, when and where; they can also obtain from telephone operators calls lists from and to any subscriber, subscription documents, addresses and bank information, Internet sites and forum addresses the respective person has accessed.

Allows intelligence gathering on country's citizens

- Since 9-11, the US has rolled back many of the legal and administrative protections that kept intelligence agencies from monitoring American citizens. Most notably, PATRIOT dropped statutory requirements that the government prove a surveillance target was a non-U.S. citizen and expressly allowed surveillance orders concerning a U.S. person in investigations related to international terrorism or clandestine intelligence activities.[7]
- Similarly, in the wake of the warrantless wire-tapping controversy in the United States, Congress amended FISA in 2008 to drop even this last stipulation. The government no longer has to demonstrate its targets are foreign agents or engaged in criminal activity or terrorism.[8]
- As mentioned, Canada's *Anti-Terrorism* Act allows the Minister of National Defence to authorize CSE interception of private communications under certain conditions.[9]
- In the past, CSE was prohibited from intercepting any communication in which one of the participants in the communication was in Canada. An example might be a communication in which a person of foreign intelligence interest in another country contacts a counterpart in Canada (e.g. a suspected terrorist financier in Pakistan emails an individual in Montreal).
- The statute does not expressly *exclude* interception of Canadian citizens or *limit* interceptions to those communications which occur outside Canada.

- As Canadian intelligence expert Wesley Wark comments, “This is a historic change in the CSE mandate, which since its birth at the dawn of the Cold War, has been exclusively targeted at foreign communications.” Since 2001, the staff complement of the CSE has increased from approx. 1000 employee to over 1700 in 2008.
- However, other Anglo-American countries appear to have embraced this change. As Stanley Cohen outlines, “Ministerial authorization now appears to be the norm in the countries of the common law world with which Canada is ordinarily compared … partners in the kinds of intelligence gathering exercises that the CSE would normally undertake.” As a public safety official explained before a Senate Committee in 2001, “The question is where there is a Canadian connection, i.e., the target is foreign but the call has been received in Canada or is coming from Canada, does that require a judicial authorization? In our view, quite clearly it does not.”
- The approach to surveillance and interception of communication in the UK is also coloured by tradition. Historically, interception of communications by government was a long established and publicly known practice. Before 1985, there was no statutory framework governing the practice, only localized provisions in various ordinances. Power was vested in the Secretary of State to authorize by warrant the interception of any postal and telegraphic communications, implying that the process was subject to executive control instead of statutory regulation.
- As a result, to this day surveillance conducted by British authorities under RIPA does not require a warrant to specify an individual or premises if it relates to the interception of communications external to the UK. [10]
- Even for domestic operations, interception of any specific individual or premises may be requested by the Security Service, Secret Intelligence Service, GCHQ, Serious Organised Crime Agency, the police, Customs and Excise, Defence Intelligence or other national government bodies as long as the purposes of the surveillance relate to national security, preventing or detecting serious crime, safeguarding the economic well-being of the United Kingdom; or to the provisions of any international mutual assistance agreement. [11]
- France’s LSI law (2003) give authorities the mandate to make new additions to the national criminal research database, including the national fingerprint database. Most notably, the LSI extends the list of infractions and the list of persons that may lead to a record in the national fingerprint database, including any individual whom police have plausible reasons to believe may have committed almost crime. [12]
- France’s *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) provides for the collection of personal information of all passengers either travelling to or from states outside the EU. The information collected comes from landing cards, scanning codes on travel documents and information collected through reservation systems.
- The same law extends video surveillance for anti-terrorism purposes and gives police access to surveillance tapes outside the context of an ongoing investigation and without a warrant. Under the law, public authorities can use video surveillance in public places for the purposes of “preventing terrorist acts”, and private organizations may install video surveillance to protect their premises where such premises are “at risk of being exposed to acts of terrorism”. Police and other

bodies overseeing public works and transportation can also put in place video surveillance for four months in cases of "emergency".

- As well, the same law provides for the *Lecture Automatisée des Plaques d'Immatriculation* (LAPI), which provides for putting into place fixed and mobile devices anywhere in France to prevent acts of terrorism and help in the fight against stolen vehicles. These devices can not only automatically read license plate information and compare data against the national stolen vehicles database and EU authority databases, but can also photograph occupants of vehicles.

Permit searches / surveillance without notification

- PATRIOT also dispenses with many traditional modes of judicial oversight in the US legal process relating to searches. The law permits 'sneak and peak' searches by federal authorities, as subjects of a warranted search are subject to delayed notification, they are not told what was searched, nor if anything was seized in the process. [13]
- Similarly, Canada's ATA added "terrorism offences" to the list of circumstances in which an Attorney General may delay notifying persons subject to wiretap of an interception for up to three years. [14]
- The ATA also eliminates the need to demonstrate surveillance is a last resort for terrorism-related investigations, though a Superior Court Judge must still approve most wiretaps.
- That said, the *Public Safety Act* (PSA) amended PIPEDA to allow private sector organizations to collect personal information without an individual's knowledge or consent if a) the collection is for the purpose of making a subsequent disclosure that is required by law; b) CSIS, the RCMP or another authorized government institution makes a request and the information relates to national security, the defence of Canada or the conduct of international affairs; and c) the organization suspects the information may be relevant to national security, the defence of Canada or the conduct of international affairs and the organization intends to disclose it to an investigative body or government institution.
- In additions to these legal revisions, Canada has set up a variety of 'passive' surveillance programs recently, most notably the Passenger Protect Program initiated under the PSA. The legislation added a section to the *Aeronautics Act* requiring airlines to disclose personal information about all passengers arriving or departing Canada to designated authorities for "transportation security" purposes and that will permit the Minister of Transport to require any air carrier or operator of an air reservation system to disclose specified information in its control for the purposes of transportation security or investigation of "threats to the security of Canada." [15]
- In the UK, the 2000 *Terrorism Act* broadly expands the discretionary search powers of authorities, allowing officials to search homes upon receipt of a warrant from a justice of the peace based upon 'reasonable suspicions'. [16] The Act also gives any police officer the authority to stop and search vehicles or individuals within previously authorized areas solely at their discretion and authorizes blanket

search power in any specified area for a period of time if considered 'expedient for the prevention of acts of terrorism'. [17]

- As a result of these powers, the entirety of Metropolitan London was declared a search zone by police in August-September 2003.
- The United Kingdom has also widely expanded monitoring and surveillance of its citizenry in the name of routine public safety and policing. In 2001, *Anti-terrorism, Crime and Security Act* allowed British Transport Police of the Defence Ministry to authorize the blanket search of areas for up to a 28-day period, while also allowing for much more invasive documentation of suspects by all police during detention, ranging from DNA sampling to detailed photographs of body features (e.g. tattoos, moles, scars). [18]
- In addition, the 2005 *Prevention of Terrorism Act* allows UK courts to impose 'control orders' on any suspect that place 'obligations on him for the purposes connected with protecting members of the public from a risk of terrorism'. Like restraining orders in the US and Canada, these delimit how a person may communicate, travel, interact, etc. Electronic tagging and continuous surveillance of untried suspects under this provision of the law has become increasingly common.
- As mentioned above, France's LSI allows for immediate access by law enforcement authorities to data of telecommunications operators and authorizes the warrantless search of any information system, provided that the system in question is connected to a computer that is being searched pursuant to a warrant.
- As well, the *Loi relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers* (2006) provides for an administrative procedure for accessing electronic information from ISPs without prior judicial authorization.

Expands duration of search / surveillance orders

- The United States, in a steady succession of legislative overhauls, has extended the time period during which a FISA search warrant may be used. Initially, PATRIOT allowed physical searches a) to 90 days (up from 45), or b) if agent of a foreign power (employee or member of a foreign power but not U.S. persons), to 120 days. [19]
- In 2005 with the *USA PATRIOT Improvement and Reauthorization Act*, pen registers and trap and trace device extensions were increased from 90 days to a year.[20]
- Finally, in 2008, amendments to FISA increased the time allowed for warrantless surveillance to continue from 48 hours to 7 days.
- In a similar vein, Canada's ATA enabled a wiretap order to be extended for up to one year when used to investigate suspected terrorist activities, instead of a 60 day time limit for most offences.
- As mentioned above, various laws in France impose retention requirements on ISPs and telephone companies to store customer identification and log information for up to one year. As well, the LSI allows for the immediate access by authorities to computer data of telecommunications operators and authorizes warrantless

searches of information systems where the system in question is connected to a computer that is being searched pursuant to a warrant. As well, the LEN requires ISPs to keep a log of subscriber data and individuals wishing to post content on the Internet must identify themselves to their host provider.

Allows inter-agency information sharing

- One of the most profound changes in intelligence and law enforcement since the September 11th attacks on the United States has been a global reformulation of how government agencies share and exploit information.
- One of the principle objectives of PATRIOT was to eliminate barriers to the flow of intelligence between various agencies. The Act allows for wiretap results, grand jury information and other information collected in criminal cases to be disclosed to intelligence agencies when the information constitutes foreign intelligence. [21]
- PATRIOT also allows the collection and sharing of intelligence information by law enforcement that is not directly related to criminal activity. This breaks down a significant legal barrier between law enforcement and intelligence organizations, erected in the United States in the late 1970s.
- Finally, foreign intelligence, counterintelligence or foreign intelligence information obtained as part of a criminal investigation can be disclosed to any federal law enforcement, intelligence, protective, immigration, national defence or national security official in order to assist the official receiving that information in the performance of his official duties.
- Then, in 2005, flowing from this historical change and in the wake of the 9-11 Commission report, the US Congress passed the *Intelligence Reform and Terrorism Prevention Act* (IRTPA). This Act authorized the creation of an "Information Sharing Environment" (ISE) to link "all appropriate Federal, State, local, and tribal entities, and the private sector."
- Most notably, for the purpose of sharing information in public and private databases, IRTPA contains no safeguards against data mining other than directing the President to issue guidelines.[22]
- As the Information and Privacy Commissioner of British Columbia noted in his 2004 report on the USA Patriot Act, “one of the defining characteristics of police states is the blurring of distinctions between law enforcement and national security functions, such that the rule of law eventually gives way to arbitrary decision-making by law enforcement authorities and the rights of ordinary citizens lose meaning. Democracies depend upon clear and effective rules that are suited to the state activities they are intended to govern and that reflect the essential values of a free society.”
- Similar trends are evident in the Canadian intelligence community, given the provisions of the PSA whereby passenger data collected by Transport Canada, can also be disclosed to the RCMP, CSIS, Citizenship and Immigration, Canada Revenue Agency and/or CATSA for the purposes of ensuring transportation security. Similar information sharing provisions have been extended to FINTRAC for the purposes of financial intelligence sharing among national security and law enforcement organizations.

- More broadly, the amendment to PIPEDA section 7 in *the Public Safety Act* which allows collection and use of information without consent for national security purposes further underscores the potential disclosure of sensitive information by private organizations to Canadian law enforcement.
- As Kent Roach wrote, several PSA provisions "authorize information sharing without enhanced review and oversight as to the necessity of the information sharing, the accuracy and reliability of the information shared, or the effects of the information sharing on privacy."[23]
- Legislators in the UK have also given authorities the legal mandate to share more intelligence information. The *Anti-terrorism, Crime and Security Act* offers public authorities broad discretion for information sharing in conjunction with any criminal investigation or proceedings against suspected terrorists, either within the UK or abroad, once approved in principle by the Home Secretary.

Allows inter-governmental information sharing

- PATRIOT also empowered the US intelligence community to reach out broadly to international partners, allowing that any information that "relates" to the ability of the U.S. to protect against an actual or potential attack, sabotage or international terrorism or clandestine intelligence activities, as well as any information that "relates" to the national defence or security or the conduct of foreign affairs can be disclosed to *any* other government official, including intelligence, national defence and national security bodies. [24]
- Subsequent provisions in IRTPA (2005) reinforce the disclosure of intelligence information to foreign government officials, where appropriate.[25]
- Along similar lines, Canada's ATA also allows that information obtained from a foreign government or international organization can be submitted by the government and considered by a judge in determining whether a decision to list a group as a terrorist organization. The affected persons may receive a summary of the evidence, but only if the information disclosed would not injure national security.

Wide production order powers

- Another extremely controversial aspect of PATRIOT allows the FBI to make an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities."
- This provision essentially provides for self-issued warrant, signed by any investigating officer, called National Security Letters (NSL), a form of administrative subpoena used by the FBI, and reportedly by other U.S. government agencies including the CIA and the Department of Defence. [26]
- The NSL amounts to a production order issued to a particular entity or organization to turn over various records and data pertaining to individuals. Under the legislation, authorities can require anyone to turn over records on their customers or clients. This gives the United States' federal government unparalleled power to

access and review individuals' financial records, medical histories, Internet usage, travel patterns, and other records.

- In 2005, IRTPA began requiring senior officials' approval for NSL orders of library, bookstore, firearm sale, medical, tax return, and educational records. During 2005, the Government made requests for information concerning 3,501 different United States persons pursuant to National Security Letters. During this time frame, the total number of NSL requests for information concerning U.S. persons totalled 9,254.
- In 2006, 12,583 NSL requests were issued, concerning 4,790 different United States persons. The number of NSL issued has grown dramatically since the PATRIOT Act expanded the FBI's authority to issue them.
- In March 2007, the Department of Justice Inspector General determined that the FBI abused its National Security Letter authority in 22% of the cases examined. Also, the FBI did not report the actual number of issued Security Letters to Congress. Later that year, the U.S. District Court struck down the NSL provision of PATRIOT as unconstitutional.
- In Canada, there is also new legal precedent for production orders in national security investigations. The ATA amended the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to allow the Director of CSIS or any member of the Service to apply to a judge for an order for disclosure of any information where there are 'reasonably grounds' to investigate a threat to the security of Canada. The order empowers any CSIS employees named in the order to access and examine all information or documents to which the order relates.

Telephone communication access (content)

- Interception of communications by the government has a long history in the US. Law enforcement agencies have practised wiretapping since the invention of telegraph communication in 1844, and tapping of telephones since the early 1890s. In 1928, the Supreme Court ruled in the case of *Olmstead v. United States* that interception of telephone conversations by federal agents did not constitute a search or seizure under the meaning of the Fourth Amendment to the Constitution.
- Only in the 1960s did the US Supreme Court protect individuals from unreasonable searches and seizures by circumscribing prosecution based on interception of communications. In the landmark case of *Katz v. United States* (1967), the Court established the doctrine of reasonable expectation of privacy by ruling that interception without a warrant is against the Fourth Amendment.
- In addition, it is important to note, despite all that has been written about PATRIOT, that interceptions of telephone conversations within the United States still requires a warrant.[27] The 2008 FISA amendments only allow government to conduct unwarranted surveillance of any person for up to one week if the FISA court is notified when the surveillance begins, and an application for authorization is submitted within one week.
- In the United Kingdom, since RIPA came into effect in 2004 the number of communications intercepted has grown. Over 200 agencies, police forces and prisons are now authorized to intercept communications. In 2005-2006, there were

2,407 warrants for interceptions of telephone and mail issued in England and Scotland under RIPA, up from 1,466 in 2002. There were also 5,143 modifications of warrants. The government refuses to disclose the number of national security interceptions.

Electronic communication access

- PATRIOT allows law enforcement to install devices that can intercept e-mail and internet activity (with FISA order) and extends scope of wiretap to include packet and recipient data. The law "significantly increased the type and amount of information the government can obtain about users from their Internet Service Providers (ISPs). [28]
- In the UK, the *Anti-terrorism, Crime and Security Act* (2001) allows the Home Secretary to issue a code of practice for the retention of data by communications providers for the purpose of protecting national security or preventing or detecting crime that relates to national security. It only applies to data that is already being held by the communications service providers for business purposes. [29]
- Communications data can be retained for up to one year. The government has proposed modifying the Act (and RIPA) to make data retention mandatory and expanding its use to include serious crimes, not just terrorism offenses. [30]
- In France, the *Loi pour la sécurité intérieure (LSI)* extended lawful access provisions to all stored data of telecommunications operators (including ISPs), as well as of almost any public or private institute, organization or company. It authorizes searches of data without warrant of any remote system, provided its data is accessible via a network from a computer being searched with a warrant. If the data is stored in a computer located in a foreign country, its access remains subject to applicable international agreements.

Communication records access

- PATRIOT permits ISPs to hand over any transactional data to law enforcement without court order or subpoena. Data can include not only "the name, address, local and long distance telephone toll billing records, telephone number or other subscriber number or identity, and length of service of a subscriber" but also session times and durations, types of services used, communication device address information (e.g. IP addresses), payment method and bank account and credit card numbers. [31]
- The 2008 amendments to FISA also the Attorney General and Director of National Intelligence to direct any electronic communication service provider immediately to 'provide the Government with all information, facilities and assistance necessary to accomplish acquisition.' This development has led to numerous media stories of US intelligence agencies 'piggybacking' their own monitoring devices on privately operated networks by installing the devices on a permanent basis. [32]
- Provisions covering the CSE in Canada's ATA stipulate the organization is broadly empowered to 'acquire information from the global information infrastructure for the purpose of providing foreign intelligence through means including interception of

communications of foreign targets abroad, and to ensure the security of electronic information and government computer networks'.

- This intelligence is to be acquired for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities; to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada; and to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. [33]
- Data retention provisions following passage of RIPA in the UK also provide British authorities with broad access to communications records. These provisions allow any public authority designated by the Home Secretary to access "communications data" without a warrant.
- Accessible data includes subscriber information, records of calls made and received, e-mails sent and received, websites access, the location of mobile phones, identity information relating to a person, apparatus or location e.g. calling line identity and mobile phone cell site location details, data identifying or selecting apparatus e.g. routing information.
- Communications data can be accessed for the following purposes under s.22(2) RIPA: (a) in the interests of national security; (b) for the purpose of preventing or detecting crime or of preventing disorder; (c) in the interests of the economic well-being of the United Kingdom; (d) in the interests of public safety; (e) for the purpose of protecting public health; (f) for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; (g) for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health. [34]
- In 2005-2006, there were over 439,000 requests for communications data. According to the Home Office, most of the requests were for address information. There has been considerable controversy about who has access to communications data.
- Again, following trends in the UK, French authorities have made widely accessible transactional data for investigatory purposes. The LSQ sets retention for up to one year for the purpose of prevention, investigation, detection and prosecution of criminal offences.
- While data should not reveal the content of communication, be it e-mail content or the content of the visited web site. The penalty for non-compliance ISPs is one year jail and 75,000 Euros fine.
- The AFA (French association of ISPs) has published a document evaluating the requests for data that they have received from the judicial authorities, and it is stated in this public document that they received approximately 500 requests monthly.
- French provisions on data retention and disclosure may be extended. A draft version published in April 2007 would require webmasters, hosting companies, fixed and mobile telephony operators and Internet service providers to retain all information on Internet users and telephone subscribers and to deliver it to the police or the State at a simple request, and would even require retaining the

passwords supplied when subscribing to a telephone service or an Internet account or payment details such as amount, date or type.

- The draft text also proposes data retained by ISPs and hosting companies and obtained by the police can be kept by the latter for a period of three years in the automatic processing systems provided by the Ministry of Interior and the Ministry of Defence.
- As mentioned above, the LEN provides for additional data retention requirements in telecommunications, namely stipulation of personally identifying information (including name, address, and log data) that must be collected on users by all operators of electronic networks. The LEN also requires all persons wishing to post content on the Internet to identify themselves, either to the public, by publishing their name and address on their website (in the case of a business), or to their host provider (in the case of a private individual).
- In both the UK and France, these data retention provisions for telecommunications providers have since been supplemented by an EU directive on data retention for law enforcement and national security purposes. This requires communications companies throughout Europe to retain and make available traffic data "for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law" for periods up to two years.
- Only Germany, Denmark, Italy and Ireland have implemented the Directive to date. In some case, they require retention for 24 months. However, the European Commission has formally written to 19 EU member states about their failure to meet the deadline for implementing the directive. This approach has been sharply resisted in both the US and Canada.

Financial records access

- In the US, PATRIOT has also modified laws for the protection of individuals' financial privacy by granting investigators broad authority for compelling business records. [35]
- Under previous law, only records of common carriers, public accommodation facilities, physical storage facilities and vehicle rental facilities could be obtained with a court order. Act now allows application to FISA court for an order to compel the production of any business record or tangible thing from anyone for any investigation to protect against international terrorism or clandestine intelligence.
- PATRIOT also broadened the scope of the *Bank Secrecy Act* to focus on terrorist financing as well as money laundering, giving Financial Crimes Enforcement Network (FINCEN) new monitoring and reporting authority.
- To some degree, monitoring of individuals' financial affairs has also become wide-spread in Canada. The ATA amended Canada's anti-money laundering legislation, adding terrorist financing to its list of offences and title, the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act.* [36]
- Subsequent legislation in 2005 also authorized the lead agency, the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), to query suspicious transactions, accounts and individuals by sharing information with CSE, CSIS and police authorities across Canada. [37]

- Likewise, in the UK under the 2000 *Terrorism Act*, police can compel any financial institution to disclose a customer's current and previous addresses, financial account numbers and date of birth for the purpose of freezing / seizing suspect assets providing material support to terrorist activities. There are also powers to monitor account activity pursuant to judicial warrant. [38]
- As each country in this study was a member of the Financial Action Task Force (FATF), all jurisdictions reviewed have established a financial intelligence unit similar to Canada's FINTRAC. The United States established FINCEN in 1990, Britain established the Serious Organized Crime Agency (SOCA) in 2000 and France established the Traitement du renseignement et action contre les circuits financiers clandestins (TRACFIN) in 1990.

Sources consulted

- Abele, Robert P. A user's guide to the USA Patriot Act and beyond (2005).
- American Civil Liberties Union, "Surveillance Under the USA PATRIOT Act" (updated Apr. 2003) URL: http://www.aclu.org/safefree/general/17326res20030403.html
- Bazan, E. B. The Foreign Intelligence Surveillance Act (2002)
- Beckman, James. Comparative legal approaches to homeland security and anti-terrorism (2007)
- Brown, Ian. "UK government surveillance powers" (2006) URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1026974
- Canada. Solicitor General. "Annual Report on the Use of Electronic Surveillance" (1996-2006)
- Canada. "Office of the Communications Security Establishment Commissioner Annual Reports" (1997-2008)
- Canada. Senate. "Special Senate Committee on the Subject Matter of Bill C-36" (Oct. 29, 2001)
- Centre for Technology and Democracy, "PATRIOT Act Overview" (updated Apr. 2008) URL: http://www.cdt.org/security/usapatriot/overview2005.php
- Chalk, Peter. Confronting "the enemy within" : security intelligence, the police, and counterterrorism in four democracies (2004)
- Cohen, Stanley. Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril (2005)
- Cousens, Michael. Surveillance law (2004)
- Electronic Frontier Foundation, "Analysis Of The Provisions Of The USA PATRIOT Act" (updated Oct. 2003) URL: http://w2.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php
- Electronic Privacy Information Centre, The USA PATRIOT Act (updated Nov. 2005) URL: http://epic.org/privacy/terrorism/usapatriot/default.html
- Electronic Privacy Information Centre and Privacy International, Privacy and Human Rights (2006) URL: http://www.privacyinternational.org/article.shtml?cmd[347]=x-347-559458
- Forcese, Craig. National security law: Canadian practice in international perspective (2008)
- France. « Commission nationale de contrôle des interceptions de sécurité rapport annuel » (2000-2008)

- Friedland, Martin L. “Police powers in Bill C-36” in The Freedom of Security: Essays on Canada’s Anti-Terrorism Bill (2001)
- Guide to Homeland Security: 2005 edition (2005)
- Hubbard, Robert W. Brauti and Fenton. Wiretapping and Other Electronic Surveillance: Law and Procedure (2008)
- Information and Privacy Commissioner of British Columbia, Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing (2004)
- Information and Privacy Commissioner of Ontario, National Security in a Post-9/11 World: The Rise of Surveillance … the Demise of Privacy? (2003)
- Jacobson, Michael. The West at war: U.S. and European counterterrorism efforts, post-September 11 (2006)
- Lyon, David. Surveillance after September 11 (2003)
- Marzouki Meryem. “Cybercrime and Data Retention : French Situation and Articulation with the International Context” (2002) URL: http://www-polytic.lip6.fr/article.php3?id_article=77
- Moore, John Norton, Robert F. Turner. National Security Law (2005)
- Patriot Debates: Experts debate the USA PATRIOT Act, Stewart A. Baker and John Kavanagh, editors. (2005)
- Perelman, Marc. “How the French Fight Terror,” *Foreign Affairs* (January 2006) URL: http://www.foreignpolicy.com/story/cms.php?story_id=3353
- Roach, Kent. September 11: Consequences for Canada (2003)
- Roach, Kent. “Must We Trade Rights For Security? The Choice Between Smart, Harsh or Proportionate Security Strategies in Canada and Britain” (2006) URL: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=899280
- Solove, Daniel J., Marc Rotenberg, Paul M. Schwartz. Information privacy law (2006)
- Terrorism, Law and Democracy: How is Canada changing following September 11? (2002)
- United Kingdom's legal responses to terrorism / Yonah Alexander and Edgar H. Brenner, editors (2003)
- United States. Department of Justice, “FISA Annual Reports to Congress” (1979-2007)
- United Kingdom. Office of the Interception of Communications Commissioner. “Report of the Interception of Communications Commissioner.” (2001-2007)
- Wark, Wesley. “Intelligence requirements and Anti-Terrorism Legislation” in The Freedom of Security: Essays on Canada’s Anti-Terrorism Bill (2001)
- Weiner, Eric. “Wire-tapping, European style” *Slate* (February 2006) URL: http://www.slate.com/id/2136147/
- Westby, Jody R. International Guide to Privacy (2004)
- Williams, Victoria. Surveillance and intelligence law handbook (2006)
- Wispinski, Jennifer. “Access to information and privacy rights: changes introduced by the Anti-Terrorism Act and the Public Safety Act, 2002” (2006) URL: http://www.parl.gc.ca/information/library/PRBpubs/prb0535-e.html
- Wispinski, Jennifer. “The USA PATRIOT Act and Canada's Anti-terrorism Act: key differences in legislative approach” (2006) URL: http://dsp-psd.pwgsc.gc.ca/Collection-R/LoPBdP/PRB-e/PRB0583-e.pdf
- Wolfson, S.M. “The NSA, AT&T, and the Secrets of Room 641A” *I/S: A Journal of Laws and Policy for the Information Society* (Winter 2007-2008) pp. 411-441.
- Wong, Thomas. “Regulation of Interception of Communications in Selected Jurisdictions” (February 2005) URL: http://www.legco.gov.hk/yr04-05/english/sec/library/0405rp02e.pdf

Endnotes

[1] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 218.*
[2] Under section 702(a), the Attorney General and the Director of National Intelligence can 'can authorize jointly, for a period of up to one year the targeting of persons *reasonably believed* to be located outside the United States to acquire foreign intelligence information' even if all the communications to be acquired originate or terminate in the US.
[3] Section 102 of the *Anti-Terrorism Act* amended *The National Defence Act* (section 273.65.1-4), allowing the Minister of National Defence to authorize the Communications Security Establishment (CSE) to intercept private communications if satisfied that: the interception will be *directed* at foreign entities located outside Canada; the information to be obtained could not reasonably be obtained by other means; the expected foreign intelligence value of the information that would be derived from the interception justifies it; and satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.
[4] Part 1, section 5, of the law requires all Communications Service Providers to provide a "reasonable interception capability" in their networks for surveillance in national security investigations. Part III compels production of plaintext of encrypted material, or in certain circumstances decryption keys themselves.
[5] Provisions in the LSQ deal with the use of cryptography and set conditions for decrypting encrypted data: public prosecutor or a judge may ask any expert to decrypt data. If they suspect a crime or an offence which penalty is more than two years jail, cryptography tool providers must provide decryption keys to authorised agents (authorised by the Prime Minister) upon request, with the penalty for not complying with this obligation is two years jail and 30,000 Euros fine. Encryption keys should be provided upon judicial request when cryptography has been is used for commission, preparation, or facilitation of a suspected crime or offence.
[6] According to media reports, French security services can pinpoint who has contacted whom, when and where; they can also obtain from telephone operators calls lists from and to any subscriber, subscription documents, addresses and bank information, Internet sites and forum addresses the respective person has accessed.
[7] With caveat that such investigation are not conducted solely upon the basis of 1st Amendment activities: religious worship, free speech, free assembly and protest. See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 214.*
[8] In fact, it does not quire to identify specific targets at all. The law expressly provides that government application need only specify the facilities, telephones lines, email addresses, places, premises or property at which the surveillance will be directed.
[9] The Canadian legislative approach to surveillance was not dramatically altered by the Act, as in most cases, judicial authorization is still required. However, new powers introduced in the Act eliminate the need to demonstrate surveillance is a last resort for terrorism-related investigations. As Kent Roach outlines in a review of the ATA, the state can invade privacy once it shows it has reasonable grounds to believe a serious offence has been committed and that surveillance will reveal evidence of the offence. Specifically, sections 6 and 133(8) of the Act gave law enforcement and national security agencies new investigative tools by amending the *Criminal Code* to eliminate the need to demonstrate that electronic surveillance was a last resort in the investigation of terrorism (this requirement was also dropped for investigation of organized crime). The Act amended section 186 (1.1) of the *Criminal Code* to permit wiretap investigations into terrorism offences without compliance with the usual investigative necessity threshold. A Superior Court Judge must still approve the surveillance.
[10] Interception of content (what is said in a letter, phone call or e-mail) is authorised for three or six months (depending on the purpose) by the Home Secretary under Part I Chapter 1 of the Act.
[11] A warrant need not specify an individual or premises if it relates to the interception of communications external to the UK.
[12] The issue of national databases in France continues to divide. France has explored the idea of creating a national health database, and more recently, has proposed "EDVIGE", a new database to be used by French intelligence services and the administrative police which will file "individuals, groups, organisations and moral persons which, due to their individual or collective activity, are likely to attempt to disrupt public order", whether or not the individual has committed an offense. EDVIGE will contains data on "civil status and occupation; physical addresses, phone numbers, email addresses; physical characteristics, photographs and behaviour; identity papers; car plate numbers; fiscal and patrimonial information; moves and legal history", and data on sexual orientation and health. Filing under EDVIGE starts at age 13.
[13] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 213.*
[14] It also allows police powers of preventative arrest and to bring subjects before an investigative hearing in which the right to remain silent is forfeit. The Act also allows that information obtained from a foreign government or international organization can be submitted by the government and considered by a judge in determining whether a decision to list a group as a terrorist organization. The affected persons may receive a summary of the evidence, but only if the information disclosed would not injure national security.
[15] The legislation adds a new section (4.81) to the *Aeronautics Act* requiring airlines to disclose personal information about all passengers arriving or departing Canada.
[16] Article 42 allows officials to search homes 'reasonable suspicions'. Section 44 of the Act gives any police officer the authority to stop and search vehicles or individuals solely at their discretion. Article 44 (subsection 3) authorizes blanket search powers.
[17] Section 33-36 give police the power to demarcate a certain area as cordoned for the purpose of a terrorist investigation, in which they have broad discretionary search and seizure powers.
[18] Part X, section 98-101 of the Act allows British Transport Police of the Defence Ministry to authorize the blanket search of areas for up to a 28-day period. Also reinstates a 'bystander cooperation rule' effectively compelling witnesses to assist police investigating, even to the detriment of peers or family members, or face prosecution. This effectively eliminates any right to remain silent. Part X, section 90 and 96 of the Act allows for documentation of suspects during detention: DNA sampling to detailed photographs of body features.
[19] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 207.*
[20] Duration of surveillance and physical search orders increased, with surveillance performed against "lone wolf terrorists" under section 207 of the Patriot Act increased to 120 days for an initial order, while pen registers and trap and trace device extensions

were increased from 90 days to a year, with an expiration date set to December 31, 2009. See *USA PATRIOT and Terrorism Prevention Reauthorization Act of 2005 (U.S. H.R. 3199, Public Law 109-177), Title I, Sec. 107*

[21] The USA PATRIOT Act allows any Federal agency to share information with law enforcement; any official who acquires information through electronic surveillance or physical searches can consult with Federal law enforcement to coordinate investigations or protect against potential attacks, sabotage, terrorism or intelligence activities by an foreign intelligence service; see *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 203* and *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title V, Sec 503. Amended 50 U.S.C. § 1825*. Regarding collection and sharing of intelligence information by law enforcement that is not related to criminal activity, see *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 218.*

[22] Section 1016 authorizes the creation of an "Information Sharing Environment" (ISE) to link "all appropriate Federal, State, local, and tribal entities, and the private sector."

[23] Roach, Kent, "Must We Trade Rights for Security? The Choice between Smart, Harsh or Proportionate Security Strategies in Canada and Britain," *Cardozo Law Review*, Vol. 27, pp. 2157-2221 (2006), 2161.

[24] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 203*

[25] Section 6501 incorporates revisions for sharing of grand jury information relating to foreign intelligence or counterintelligence with any other Federal official (from section 203 of the *USA Patriot Act*) and provisions in section 895 of the *Homeland Security Act* which further authorize the disclosure of that information to foreign government officials, where appropriate.

[26] Allows the FBI to make an order "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities" under *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 215*. Related to these powers were one of the most controversial powers under the Patriot Act, called National Security Letters (NSL), a form of administrative subpoena used by the FBI, and reportedly by other U.S. government agencies including the CIA and the Department of Defence. The provision was reauthorized in 2005 but amendments were made to specify a process of judicial review of NSL and to allow the recipient of an NSL to disclose receipt of the letter to an attorney to comply with or challenge the order. However, in 2007 the U.S. District Court struck down the provision as unconstitutional. See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title V, Sec 505. Amended 18 U.S.C. § 2709(b*).

[27] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 204 & 209.*

[28] Allows law enforcement to install devices that can intercept e-mail and internet activity (with FISA order) and extends scope of wiretap to include packet and recipient data; see *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 216.* As the Office of the Information and Privacy Commissioner of Ontario concluded in her 2003 report on the USA Patriot Act, the law "significantly increased the type and amount of information the government can obtain about users from their Internet Service Providers (ISPs). It permits ISPs to voluntarily give law enforcement all "non-content" information without requiring a court order or subpoena. It also expanded the records the government may seek with a simple subpoena (no court review required) to include records of session times and durations, temporarily assigned network (IP) addresses, means and source of payments, including credit card or bank account numbers."

[29] See Part XI, section 102-107.

[30] Chapter XI gives the Home Secretary the power to require the retention of communications data (but not the content of communications) by phone and Internet companies for periods specified. Subsequently, the *Code of Practice on Data Retention* approved by Parliament in December 2003 set the period for up to 12 months, and to include the following elements: subscriber details relating to the person (e.g. Name, date of birth, installation and billing address, payment methods, account/credit card details); contact information (information held about the subscriber but not verified by the CSP) e.g. Telephone number, email address; identity of services subscribed to (information determined by the communication service provider) e.g. Customer reference/account number, list of services subscribed; telephone number(s), IMEI, IMSI(s); email address, IP at registration; Internet Message Handle, IP at registration; ISP - dial-in: Log-in, CLI at registration (if kept); ISP - always-on: Unique identifiers, MAC address (if kept), ADSL end points, IP tunnel address; Date and time of start of calls, Duration of call/date and time of end of call, Type of call (if available), Location data at start and/or end of call, in form of lat/long reference; Cell site data from time cell ceases to be used; etc. Content of email would be retained for 6 months – both sent email (authentication user name, from/to/cc email addresses, date and time sent) and received email (authentication user name, from/to email addresses, date and time received). ISP data would be retained 6 months e.g. Log-on (authentication user name, date and time of log-in/log-off, IP address assigned). Finally, Web activity logs would be retained 4 days with data including e.g. Proxy server logs (date/time, IP address used, URL's visited, and services).

[31] See *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 212*. Act also allows for the disclosure of electronic communications to law enforcement as well, as companies who operate a "protected computer" can allow authorities to intercept communications routed through the machine, bypassing warrant requirements, under *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 217*. For expanded subpoenas issued to Internet Service Providers, see *USA PATRIOT Act (U.S. H.R. 3162, Public Law 107-56), Title II, Sec. 210*.

[32] Once authorized under the Act, the Attorney General and Director of National Intelligence may direct any electronic communication service provider immediately to 'provide the Government with all information, facilities and assistance necessary to accomplish the acquisition'; see *H.R. 3773: FISA Amendments Act of 2008, sec. 702(h)(1)(A).*

[33] These activities shall not be directed at Canadians or any person in Canada; and shall be subject to measures to protect the privacy of Canadians in the use and retention of intercepted information. See section 273.64 of the *National Defence Act*.

[34] Access to data related to the use of communications service may be self-authorised by a wide range of government bodies under Part I Chapter 2. In June 2002, the Home Office announced that the list of government agencies allowed under RIPA to access communications data was being extended to more than 1,000 different government departments including local authorities, health, environmental, trade departments and many other public authorities.

[35] Section 215 grants broad authority for compelling business records. Under previous law, only records of common carriers, public accommodation facilities, physical storage facilities and vehicle rental facilities could be obtained with a court order. Act now allows application to FISA court for an order to compel the production of any business record or tangible thing from anyone for any investigation to protect against international terrorism or clandestine intelligence. Library records, bookstore purchases

and other transactional logs are all obtainable – without judicial approval or oversight. Section 505 allows the FBI to request telephone toll and transactional records, financial records and consumer reports in any investigation to protect against international terrorism or clandestine intelligence activities, if the investigation is not conducted solely on the basis of activities protected by the first Amendment. This power is subject to Congressional review in 2010.

[36] Section 72 of the Act amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to allow the Director of CSIS or any member of the Service to apply to a judge for an order for disclosure of any information where there are 'reasonably grounds' to investigate of threat to the security of Canada. The order then allows any employee of CSIS named in the order to have access to and examine all information and documents to which the application relates.

[37] Part IV, sections 47-75 of the legislation amended the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to authorize the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to collect and disclose information about financial transactions that may constitute threats to Canada's security to CSIS and other law enforcement agencies.

[38] Under Schedule Six (par. 7); also powers to monitor account activity pursuant to judicial warrant (section 38a).