Personal Information Protection in the Face of Crime and Terror: Information Sharing by Private Enterprises for National Security and Law Enforcement Purposes

A report prepared by Tamir Israel, Ali Mian, Aba Stevens, and Michelle Yau
Supervised by Andrea Slane

Centre for Innovation Law and Policy
March 2008

Funded by the Contributions Program 2007-2008
Office of the Privacy Commissioner of Canada

TABLE OF CONTENTS

Executive Summary

Approach of this Report

This report considers how information is shared by private entities with national security services and law enforcement, by engaging in a two layered research agenda: 1) to describe the context of information sharing by private enterprises with public bodies in four major industries where potentially sensitive personal information is typically held; and 2) to consider the statutory or *Charter* restrictions or questions that are raised by these information sharing practices. The report examines the telecommunications industry, the retail industry, the banking industry, and the airline industry in order to make recommendations.

Summary of Recommendations

Throughout analysis of information sharing in all four industries, the importance of balancing the privacy interests and rights of individuals with the investigatory interests of law enforcement and national security agencies has been a pervasive theme. The writers also considered important practical concerns of the industries. The following recommendations are the result of these efforts.

Recurring concerns include: 1) lack of clarity regarding the interpretation of s. 7(3) of *Personal Information Protection and Electronic Documents Act*; 2) the impact of technological development on the balance of relevant interests; 3) lack of transparency regarding informal information sharing, and 4) a tendency towards collection of increasing amounts of personal information identified in some of the industries. Some persistent constitutional issues are: 1) the departure from the principal of judicial authorization in the cases of information sharing without warrants or court orders, 2) lack of certainty regarding whether there is a reasonable expectation of privacy in various contexts and 3) the constitutional sufficiency of the standard for disclosure in instances where information is obtained notwithstanding a lack of reasonable probable grounds to believe that a crime has been committed. This last concern is particularly pressing where disclosure of information to national security agencies had been made mandatory.

The Executive Summary follows the structure of the report. It begins the telecommunications industry, which tended to reveal recommendations pertaining to generally applicable law, proceeds to discuss the retail sector and banking industries, and concludes with an analysis of the airline industry, with recommendations that are highly industry-specific.

➢ The Telecommunications Industry

The analysis shows that gaps and lack of clarity in the law have somewhat frustrated the attainment of a clear, satisfactory balance between the privacy interests of individuals, on the one hand, and the investigative interests of law enforcement and national security on the other. The problems posed by s. 7(3)(c.1) of *PIPEDA* and the discretion it seemingly gives telecommunications companies with respect to the disclosure of the personal

information of its customers were principle among the gaps in privacy protection and the privacy related controversies arising in the telecommunications industry. Making the disclosure mandatory rather then discretionary under the provision, however, would be an ineffective means of solving the problem considering the uncertainty concerning the reasonable expectation of privacy in Internet traffic data and the unclear *Charter* implications of such an amendment. Mandatory disclosure would, furthermore, be problematic due to the fact that it is a broadly applicable provision that does not circumscribe the types of personal information that may be disclosed and the fact that it would trench on the norm of judicial authorization in search and seizure law.

Even though the industry has shown itself to be responsive to the deficiencies of the law, both the state and individuals have important interests at stake with respect to disclosure under this provision and real consideration at a policy level should be given to whether Telecommunications companies are the appropriate entities to balance these interests. The report thus forwards recommendations that to a considerable extent pertain to generally applicable law but derive from the nuances and experiences of this industry.

Recommendations

1. Clarification is needed of the discretionary authority of private entities to disclose personal information of customers under s. 7(3) of *PIPEDA*, especially section 7(3)(c.1).
2. Section 7(3)(c.1) should not be amended to make disclosure to law enforcement mandatory absent a warrant, court order or other clear authority.
3. Disclosure of personal information in the absence of a warrant should be subject to consideration of the following factors: the seriousness of the crime being investigated, whether the nature of the crime is such that the inability of the state to access the information will foreclose the investigation, and whether the information is of a sort for which the privacy interest of the individual is relatively low.

- **The Retail Industry**

Analysis of the Canadian retail industry shows a current state of equilibrium between security and safety on the one hand and privacy rights on the other. However, the current regulatory scheme may be insufficient to maintain the current level of protection of individual privacy, especially given the likelihood of future technological developments which will make the compilation of personal information from a variety of sources increasingly sophisticated.

Recommendations

1. Customers should be informed when the information that they disclose to their retailer may be disclosed to public investigators, perhaps through the inclusion of this practice in the retailer's privacy policy.
2. The Privacy Commissioner should provide greater guidance to retailers regarding voluntary information sharing with law enforcement and national

security agencies. Given the likelihood of increased information sharing between public investigators and retailers, there should be clarification of the extent to which collaboration is permissible and desirable and under what circumstances it should take place. It may be appropriate to place certain types of personal information such as reading preferences or hobbies out of the bounds of non-consensual, warrantless disclosure.

3. Legislation compelling retailers to contribute personal information of consumers to a database similar to the Canada Border Services Agency's PAXIS database should be avoided.

➢ The Banking Industry

The section about banks shows an increasing tendency by the banks to retain more personal information, and that banks have not effectively indicated to clients the extent of personal information it needs to collect for many of their services. More specifically, it reveals that: major banks receive many informal requests from police to disclose bank records; even where banks keep a record of the nature and extent of informal police requests, their legality is often not assessed by an independent and publicly accountable authority; there remains uncertainty about under what circumstances bank records can be released without judicial authorization but in conformity with *PIPEDA*; and that the constitutionality of the 'reasonable suspicion' standard used by the Financial Transactions and Reports Analysis Centre in its disclosures of bank records to police is not yet certain.

Recommendations

1. Banks should provide clear guidelines to clients on what types of personal information can and must be collected for services such as investment advice.
2. All banks should keep track of the nature and extent of informal police requests for bank records, especially the authority under which these records are being sought, as well as the circumstances in which the records are disclosed.
3. An independent and publicly accountable authority, such as the Office of the Privacy Commissioner of Canada, should be tasked with assessing the legality of informal police requests for bank records.
4. Parliament should clarify terms in *PIPEDA* such as 'lawful authority' and 'national security threat' by providing examples of when personal information such as bank records can be disclosed without judicial authorization.
5. The Government of Canada or the Privacy Commissioner should bring a reference to the Supreme Court of Canada to inquire whether the standard of 'reasonable suspicion' can ever be justified to disclose personal information, such as bank records, to police in a criminal context.

- **The Airlines Industry**

Analysis of the airline industry shows that the balance of individual privacy interests with national security in current law and practice create the potential for infringement of privacy rights beyond what can be justified. There are a number of areas of concern. Even if an airline earnestly wanted to protect its customers' privacy, it will be hard pressed to do so when faced with the requirements of various legislative provisions which make disclosure of information mandatory absent any proof that the collection is justified. Another threat to privacy is the vagueness of the provisions of the *Customs Act* that establishes the PAXIS database. The continuous data streaming of Advance Passenger Information and Passenger Name Record information on all passengers entering Canada facilitates the authorities in fishing for information about individuals, results in a lack of transparency about police investigations, and does not accord with the plain meaning of the words in the *Aeronautics Act*. The Passenger Protect Program (no-fly lists), though helpful for protecting the safety of airplanes, would benefit from safeguards to better protect individual privacy and to reduce the probability of false listing and false matches. Given the mandatory disclosure requirements to which the airlines industry is subject, informal sharing of customer personal information with police should be limited or avoided altogether.

<u>Recommendations</u>

1. Legislated mandatory collection and disclosure requirements should be amended to clarify and specify conditions that must be met before an officer can compel an airline to disclose personal information of customers.
2. The legislative provisions relating to disclosure to the PAXIS database should be clarified to specify the conditions for disclosure.
3. Continuous data streaming should not be the norm.
4. Safeguards should be put in place to ensure the accuracy and minimize imprecision of the Passenger Protect Program.
5. Airlines should adopt policies to discourage informal information sharing between airline staff and government.

I. General Introduction

Recent privacy related controversies have contributed to concern amongst Canadians about the collection, use and disclosure of their personal information in the name of national security, and law enforcement more broadly. Meanwhile, current privacy legislation does not provide for oversight of the information practices of law enforcement and security services. The *Privacy Act* does not meaningfully restrict the sharing of personal information collected by one public entity with another, especially where national security or law enforcement is at issue. Moreover, while the *Personal Information Protection and Electronic Documents Act (PIPEDA)* regulates the collection, use and disclosure of personal information by inter-provincial businesses for commercial purposes, there are little to no restrictions on private entities disclosing personal information to public entities in the Act. The access that law enforcement and national security services may have to information held by private companies and the legal constraints defining it is consequently of particular concern to Canadians and will be the focus of the report.

The report was funded by the Office of the Privacy Commissioner of Canada and the research was conducted during summer 2007. It considers how information is shared by private entities with security services and law enforcement, by engaging in a two layered research agenda: 1) to describe the context of information sharing by private enterprises with public bodies in four major industries where potentially sensitive personal information is typically held; and 2) to consider what, if any, statutory or *Charter* restrictions or questions are raised by these information sharing practices. The report will consider the industry-specific concerns of four major industries (telecommunications, retail, banking and airlines) where the personal information held by private companies is of interest to security services and law enforcement and the information is potentially sensitive especially if it is compiled or combined with other information about an individual.

The report begins with a section explaining the law that is generally applicable to the sharing of information between private industries and law enforcement and national security. This section includes 1) an overview of *PIPEDA*, as the primary legislation shaping the practices of industry with respect to personal information and 2) a brief explanation of the protections against unreasonable search and seizure afforded by s. 8 of the *Charter of Rights and Freedoms*. The general section then provides 3) a description of the statutory, jurisprudential and constitutional law that regulates organizations in all four industries in relation to three activities that engage the privacy interests of individuals: a) the collection of information by the organization, b) the organization's use of information in its custody, and c) the potential disclosure of information by the organization. The general section is followed by sections describing and analyzing issues specific to telecommunications, retail, banking and airlines.

A) *PIPEDA* – Overview:

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) is a federal statute that applies in general to any private sector business that collects, uses and discloses personal information in the course of a commercial activity.[1] In addition, *PIPEDA* applies to all federal works, undertakings or businesses. Private businesses that operate strictly within British Columbia, Alberta and Quebec are covered by substantially similar provincial statutes instead of *PIPEDA*.[2] There are a few differences between these provincial Acts and *PIPEDA* but in matters regarding information sharing with law enforcement or national security organizations they are essentially the same.

The Act governs the collection, use and disclosure of personal information, defined as information about an identifiable individual, excluding the name, title or business address or telephone number of an employee of an organization.[3] The focus of the Act is to provide consumers with some measure of control over their own personal information. This is accomplished by installing informed consent as prerequisites to most uses an organization makes of such information.[4] Under *PIPEDA* an organization may only collect, use or disclose personal information for purposes that a reasonable person would consider appropriate under the circumstances.[5] In this way the Act nurtures an expectation of privacy with regards to personal information so that an individual can expect an organization to keep their information private or inform them of instances where this practice is not maintained.

In defence of these rights, the Privacy Commissioner is obliged to conduct an investigation when presented with a privacy complaint that is not trivial, frivolous, vexatious or made in bad faith.[6] The Commissioner releases findings based on these investigations. These findings are not binding on either party. However, a complainant may, after receiving the Commissioner's report, apply to the Federal Court for an enforceable ruling on their complaint or any matter relating to the report and certain key sections of *PIPEDA*.[7] The Commissioner may make such an application on behalf of a complainant if they consent, and has additional powers to initiate an audit of any organization the Commissioner has reasonable grounds to believe is contravening a

---

[1] Office of the Privacy Commissioner, Privacy Training Module: http://www.privcom.gc.ca/privacy_comm/which_laws_apply.asp (last accessed on January 29, 2008).
[2] British Columbia and Alberta have each passed a *Personal Information and Protection Act* (PIPA) and Quebec has passed *An Act Respecting the Protection of Personal Information in the Private Sector*. These acts replace *PIPEDA* for purposes of intra-provincial commercial endeavours while *PIPEDA* continues to apply to federal works, undertakings or businesses as well as to commercial activity that crosses provincial or international borders (http://www.privcom.gc.ca/fs-fi/02_05_d_26_e.asp) (last accessed on January 29, 2008).
[3] *PIPEDA* s. 2. This includes more than just personal identifiers such as an individual's name, address or telephone number: *PIPEDA* Case Summary # 370 (January 2007).
[4] *PIPEDA* Schedule 1, principle 4.3.
[5] *PIPEDA* s. 5(3). Principle 4.4 under Schedule 1 additionally requires that collection of personal information be limited strictly to those purposes that are disclosed to the individual in question.
[6] *PIPEDA* s. 12: "The Commissioner *shall* conduct an investigation in respect of a complaint…" (emphasis added). See also *PIPEDA* s. 13(d).
[7] *PIPEDA* s. 14.

provision of Division 1 of *PIPEDA*.[8] In these ways, the Commissioner ensures that privacy rights are maintained.

Although a strong expectation of privacy rights is established and a mandate is allotted to ensure these are maintained, there are exceptions that are deemed to be beyond the reach of the Act. Among these is the law enforcement and national security exemption, which holds that personal information can be collected, used and disclosed for these purposes without consent under the proper circumstances.[9] *PIPEDA* is permissive in this respect and the Privacy Commissioner has held that section 7 of the Act does not require cooperation but merely allows information sharing with public investigators in certain circumstances if a particular organization decides to do so. In many situations involving investigations into the contravention of a law, s. 7 of *PIPEDA* shifts control of personal information away from the individual consumer and places such control in the hands of businesses.

Section 7 reflects the tension between a general requirement of knowledge and consent of the individual for collection, use or disclosure of information and the needs of law enforcement and national security. On the one hand, it may seem that the provision runs counter to the expectations nurtured by the Act in most other situations. On the other hand, the Act contemplates limitations to the consent principle and specifically cites law enforcement as an instance in which seeking consent may defeat the purpose of disclosing the information and so be inappropriate.[10] Recognition of this consideration might lead a reasonable person to conclude that the exemption from the prior consent principle is appropriate in these circumstances, making the exemption in accordance with the purpose of the Act.[11] Of course, such a conclusion would not foreclose debate about the parameters that the provision places around the collection, use and disclosure of information in the absence of consent and the particular balance that it strikes between the needs of law enforcement and the individual's interest in privacy.

B) Section 8 of the *Canadian Charter of Rights and Freedoms* – Overview:

Considering that the balancing of precisely these interests has been at the core of the courts conceptualization of reasonable search and seizure a cursory look at the court's interpretation of s. 8 of the Canadian Charter of Rights and Freedoms, under which the court has constitutionalized the reasonable expectation of privacy in Canada, should be instructive. Section 8 of the *Canadian Charter of Rights and Freedoms* protects Canadian residents against unreasonable search and seizure by the state. In protecting people from unreasonable state interference, this section is protecting individuals' privacy. Section 8 protects privacy through safeguarding from the state "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state. This includes information

[8] *PIPEDA* s. 18.
[9] *PIPEDA* s. 7.
[10] *PIPEDA* Schedule 1, principle 4.3.
[11] *PIPEDA* s. 7.3.

which tends to reveal intimate details of the lifestyle and personal choices of the individual."[12] Section 8 is violated whenever there is (i) a search or seizure and (ii) that search or seizure is unreasonable.

1) Search or Seizure

For the purposes of s.8 of the *Charter*, a search occurs when law enforcement and national security services invade an individual's reasonable expectation of privacy[13] while a seizure occurs when something is taken from that individual against his or her will.[14] Accordingly, s.8 is not implicated every time police collect an individual's personal information. There is no search when police ask for personal information on an individual who is required to provide such information to them as a legal condition for the exercise of a right or privilege.[15] While a search may result in detention of an individual's property against his or her will, a seizure is more than detention of property, "there must be a superadded impact upon privacy rights occurring in the context of administrative or criminal investigation."[16] Since information sharing between police and private sector entities like banks, airlines, retailers and telecommunications companies only occurs for criminal, quasi-criminal or administrative purposes, information shared between them will generally involve a search and seizure of that information.

As indicated above, searches and seizures necessitate state interference of an individual's reasonable expectation of privacy. The inquiry into whether a search or seizure has taken place in any given circumstance is a contextual one; one's reasonable expectation of privacy will vary depending on the totality of the circumstances in which one finds oneself. In assessing the totality of the circumstances, a number of factors must be considered. These factors include facts such as a subjective expectation of privacy; the objective reasonableness of that expectation; a direct interest in the subject matter of the search; whether the police technique was intrusive in relation to the privacy interest; and whether the use of surveillance technology was itself objectively unreasonable.[17] In relation to informational privacy, certain factors are more pertinent in the analysis such as "the nature of the information itself, the nature of the relationship between the party releasing the information and the party claiming its confidentiality, the place where the information was obtained, the manner in which it was obtained and the seriousness of the crime being investigated."[18] There is a greater expectation of privacy in a private space than in a public space.[19] There is also greater expectation of privacy when the state collects or obtains personal information for a criminal or quasi-criminal investigation than when it collects or obtains such information for regulatory purposes.[20] Since reasonable expectation of privacy is a normative rather than a descriptive standard, an

---

[12] *R. v. Plant* [1993] 3 S.C.R. 281 at 293.
[13] *R. v. Wise*, [1992] 1 S.C.R. 527, at p. 533.
[14] *R. v. Dyment*, [1988] 2 S.C.R. 417.
[15] *R. v. Hufsky*, [1988] 1 S.C.R. 621; *R. v. Ladouceur* [1990] 1 S.C.R. 1257.
[16] *Quebec (Attorney General) v. Laroche*, [2002] 3 S.C.R. 708 at 740.
[17] *R. v. Edwards*, [1996] 1 S.C.R. 128; *R. v. Tessling*, 2004 SCC 67.
[18] *Supra*, note 10 at 293.
[19] *R. v. Mellenthin*, [1992] 3 S.C.R. 615.
[20] *R. v. Jarvis*, [2002] 3 S.C.R. 757.

individual does not lose a reasonable expectation to privacy merely because police have collected or obtained his or her personal information.[21] If he or she stores contents in a secure facility he or she will still have a reasonable expectation of privacy in those contents if there is no reasonable notice of a possibility of their inspection by police.[22]

Police will not invade reasonable expectation of privacy if they collect insignificant personal information, such as records of electricity consumption, which do not reveal intimate details of personal lifestyles.[23] Moreover, there is no reasonable expectation of privacy in anything one knowingly abandons.[24] There is, similarly, no reasonable expectation of privacy when one voluntarily consents to disclosure of personal information to the state.[25] Since disclosure of personal information can only be voluntary when one has sufficient information to make a meaningful decision about disclosure,[26] it is fair to say that most instances of personal information sharing between police and the private sector involves involuntary disclosure because those whose personal information is being shared are rarely in a position to make such a decision.

2) When is a Search or Seizure Unreasonable?

Section 8 of the *Charter* governs how the state may obtain personal information from private sector entities like banks, airports, retailers and telecommunication companies. Law enforcement and national security services must collect or obtain personal information reasonably or risk having it excluded from any court proceeding seeking to rely on it. A search or seizure will be reasonable if (1) it is authorized by law, (2) the law itself is reasonable, and (3) it is carried out in a reasonable manner.[27] A search will be unreasonable if any of these conditions are absent. A law will be unreasonable when it authorizes police to conduct a search or seizure without prior judicial authorization.[28] A search or seizure will be conducted in an unreasonable way when it is not in accordance with statutory requirements[29] or when a warrant is not obtained in circumstances that require it.[30]

It is important to note that there is less than perfect conceptual overlap as between the two sources of law reviewed thus far. Most notably, the judicial interpretation of what constitutes "a biographical core of personal information" is not coextensive with what *PIPEDA* refers to as "information about an identifiable individual" such that there are some types of information that may be covered under the Act although they do not engage the Charter.[31] There are, furthermore, instances in which information will clearly

---

[21] *Supra*, note 13 at 435.
[22] *R. v. Buhay*, [2003] 1 S.C.R. 631.
[23] *Supra*, note 10.
[24] *R. v. Evans*, [1996] 1 S.C.R. 8.
[25] *R. v. Borden*, [1994] 3 S.C.R. 145.
[26] *Ibid*.
[27] *R. v. Collins*, [1987] 1 S.C.R. 265; *R. v. Caslake*, [1998] 1 S.C.R. 51; *R. v. S.A.B.* 2003 SCC 60.
[28] *Hunter et al. v. Southam Inc.*, [1984] 2 S.C.R. 145.
[29] *R. v. Simmons*, [1988] 2 S.C.R. 495.
[30] *Supra*, note 18; *Supra*, note 21; *Supra*, note 27.
[31] *Supra*, note 3.

meet the test of being about an identifiable individual but a dearth of case law makes it less than clear that there is the requisite reasonable expectation of privacy in the information to engage the Charter.

Having provided an overview of two key sources of law shaping the information sharing context, it remains to explain more practically how these as well as other sources of law regulate information handling by private industry in relation to law enforcement. Specifically, the report will briefly cover how statutes applicable to all four of the industries considered, jurisprudence and constitutional considerations combine to regulate how the industries may collect and use personal information as well as disclose it to law enforcement.

C) Collection, Use and Disclosure of Personal Information

1) Collection

The collection of personal information by private industries is governed by s.5(3) and s.7(1) of *PIPEDA*, as well as various clauses in Schedule 1 of that Act. A number of clauses in Schedule 1 of *PIPEDA* have a direct bearing on information collection by private industries. Clause 4.2 requires organizations to identify the purposes for collection of information at or before the time of collection. Clause 4.2.3 requires organizations to specify the purposes for collection at or before the time of collection to the individual concerned, either orally or in writing. Quite significantly, in the context of law enforcement, clause 4.3 requires knowledge and consent for the collection, use, or disclosure of personal information, except where inappropriate (refer to s.7(1).) Clause 4.3.3 forbids organizations from requiring, as a condition for the supply of a product or service, an individual to consent to the collection, use, or disclosure of information beyond that required to fulfill the specified purposes. Clause 4.4 limits the collection of personal information (both amount and type, according to clause 4.4.1) to that necessary for the specified purposes, and requires collection to be by fair and lawful means. Clause 4.4.2 elaborates on the requirement of collection by fair and lawful means, indicating that organizations cannot collect information by misleading or deceiving individuals about the purposes for which the information is being collected. Clause 4.6 specifies that personal information shall be as complete, up-to-date and accurate as is necessary for the purposes for which it is used.

The two subsections that are most relevant to information collection in Part 1 of the Act are s. 5(3) and s. 7(1). Subsection 5(3) states that an organization may only collect, use, or disclose information for purposes that a reasonable person would consider appropriate in the circumstances. Subsection 7(1) permits the collection of personal information without knowledge and consent only in certain specified circumstances. The subsection provides as follows:[32]

> For the purpose of clause 4.3 of Schedule 1, and despite the note that accompanies that clause, an organization may collect personal information without the

[32] *PIPEDA* s.7.

knowledge or consent of the individual only if

(a) collection is clearly in the interests of the individual and consent cannot be obtained in a timely way;

(b) it is reasonable to expect that the collection with the knowledge or consent of the individual would compromise the availability or the accuracy of the information and the collection is reasonable for purposes related to investigating a breach of an agreement or a contravention of the laws of Canada or a province;

(c) collection is solely for journalistic, artistic or literary purposes;

(d) the information is publicly available and is specified by the regulations; or

(e) collection is made for the purpose of making a disclosure

(i) under subparagraph (3)(c.1)(i) or (d)(ii), or

(ii) that is required by law.

Subparagraph 7(1)(e)(i) is particularly notable as it allows organizations to collect information without the individual's consent specifically in order to disclose it for national security purposes. Likewise, subparagraph 7(1)(e)(ii) would serve more general law enforcement purposes in cases where disclosure is required by law, which in the context of law enforcement ordinarily suggests a warrant. On its face, s. 7(1)(b) appears to allow nonconsensual collection of personal information relating to law enforcement even in the absence of a warrant. The foregoing, however, is subject to the constitutional implications on such information collection if an organization is found to act as an agent of the state.

Where Private Organizations Act as Agents of the State

Although the *Charter* usually only applies to the actions of state entities, in some circumstances it may apply to the information collecting actions of private organizations if they are acting as agents of the state. According to the test from *R v. Broyles*, a private organization acts as an agent of the state if the exchange between the organization and the individual being investigated was altered by the intervention of the state. Thus, collection of personal information by private entities during routine business operations, and any subsequent disclosure of this information to government entities, does not engage s.8 of the *Charter*. However, where a private organization is collecting personal information for the purpose of disclosing it to state authorities, such as is envisioned by s.7(1)(e) of *PIPEDA*, the organization is an agent of the state and s.8 applies to the collecting activities of the organization. In such cases, s.8 restrictions apply to the collecting activities of the private organization, and any personal information collected in a manner violating s.8 may be inadmissible in court.

2) Use

PIPEDA regulates the possible uses that can be made of personal information by private organizations. In broad terms, *PIPEDA* restricts uses of information directly to those purposes for which consent has been acquired by the organization.[33]

PIPEDA restricts use of personal information by a private organization first of all to primary purposes, meaning to those purposes that are necessary for carrying out the transaction in question between the consumer and the organization. An organization can require consent as a precondition to a transaction if this is for a primary purpose use. An organization may make use of personal information for secondary purposes with the consent and knowledge of the customer in question as long as consent is in fact optional and not a requirement. In order to use personal information for secondary marketing purposes, for example, many private organizations make use of opt-out consent. As long as a reasonable effort is made to inform consumers of the opt-out option, consent can be assumed.[34] Many organizations accomplish this by including descriptions of such secondary marketing uses in their privacy policies and by including details of simple procedures in place to opt out of consent or by providing an opt-out option as part of any transaction. Organizations must then bring these procedures to the attention of the customer.[35] If personal information is especially sensitive, such as driver's license number or Social Insurance Number, then express consent may be required, where the consumer must sign a form clearly delineating the proposed secondary uses of the information at the time of collection.[36]

Opt-out consent is typically used by private organizations to make use of data brokers to aggregate information and create more detailed customer profiles to use for targeted and direct marketing campaigns. It is the responsibility of the private organization that initially collected personal information from a consumer to ensure that there is consent for all uses to which that information will be put.[37] In order to sell personal information to a data broker, an organization would have to first acquire consent for all uses the data broker intended to make of that information. This requirement restricts the ability of data brokers to purchase individualized personal information and to develop large aggregations of personal information in Canada. Canadian businesses have therefore tended to use data brokers for their own marketing purposes, but they have been hesitant to alienate potential customers through outright selling of their information.

A private organization may make use of personal information without knowledge or consent of the individual if the organization has reasonable grounds to believe that this information would be useful in the investigation of the contravention of a law of Canada,

---

[33] *PIPEDA* Schedule 1, principle 4.2.
[34] *PIPEDA* Case Summary # 260, http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040204_e.asp. (last accessed on January 29, 2008).
[35] *PIPEDA* Case Summary # 77, http://www.privcom.gc.ca/cf-dc/2002/cf-dc_021016_7_e.asp (last accessed on January 29, 2008).
[36] Office of the Privacy Commissioner, Privacy Training Manual: http://www.privcom.gc.ca/privacy_comm/pdf/A_primer_on_consent.pdf (last accessed January 29, 2008).
[37] *PIPEDA* Schedule 1, principle 4.1.

a province or a foreign jurisdiction. If such information is discovered during the regular course of an organization's activities, they may use that information for the purpose of investigating that contravention.[38]

3) Disclosure

PIPEDA generally requires an individual to know of and consent to disclosure of their personal information by private enterprise.[39] The Act however, makes an exception for circumstances in which seeking consent is impossible, impractical or defeats the purpose of collecting the information and specifically refers to security and law enforcement as examples.[40] However, since the Act specifies conditions that must be met in order for there to be such disclosure, *PIPEDA* does not provide a blanket exemption to the consent principle.[41] Section 7(3) of *PIPEDA* provides that disclosure without knowledge or consent may only take place if any one of a list of conditions is met. For instance, the Act contemplates such disclosure in cases of emergency that threaten the life, health or security of an individual; where disclosure is made pursuant to s. 7 of the Proceeds of Crime (Money Laundering) Act; where disclosure is required to comply with a warrant or subpoena; or where disclosure is "required by law."[42]

"Required by law" includes, inter alia, the following:

i) Warrants
ii) Subpoenas/Demands for information
iii) Court orders
iv) Warrantless Search or Seizures

a) Warrants

In most cases, unless expressly required by legislation, law enforcement and national security services will have to obtain a warrant to seek personal information held by the private sector. A warrant allows police to enter private premises and to seize personal information stored there. A warrant must be authorized (1) prior to a search or seizure, (2) by a person acting judicially in a neutral and impartial way, and (3) upon an oath that reasonable and probable grounds exist to believe that an offence has been committed and that evidence is to be found at the place to be searched.[43] A departure from these criteria for a warrant will only occur in rare circumstances. The requirements for warrants for a criminal investigation appear in various statutes. For example, search warrants are dealt with under s.487 of the *Criminal Code* and s.231.3 of the *Income Tax Act*. While regulators are permitted to conduct searches and seizures without warrants, they cannot do so when the predominant purpose of these searches and seizures is to further a

[38] *PIPEDA* s.7(2)(a).
[39] *PIPEDA* Principle 4.3, Schedule 1.
[40] *PIPEDA* note to principle 4.3.
[41] *PIPEDA* s. 7(3).
[42] Ibid.
[43] *Supra*, note 27.

criminal rather than a regulatory or administrative investigation. While the Canada Revenue Agency (CRA) is permitted to conduct searches and seizures to ensure a tax payer is complying with tax reporting requirements pursuant to s.231.1 and s.231.2 of the *Income Tax Act*, the CRA cannot do so if its predominant purpose is investigating penal liability.[44] Nevertheless, information obtained during the course of a regulatory investigation can be passed on to police if it is also evidence of a crime. If evidence of criminal activity is found using natural senses during the course of any *bona fide* investigation, it can be forwarded to police pursuant to the plain view doctrine.[45]

b) Subpoenas/Demands for Information

Subpoenas are judicial demands for information made pursuant to various statutes. Although commonly used in non-criminal contexts, subpoenas are also used in criminal investigations. Regardless of whether or not police use subpoenas to demand personal information from private sector entities, any police demand for personal information from them is a search and seizure within s.8 of the *Charter*.[46] However, the use of subpoenas is a more reasonable search and seizure and thus less likely to violate s.8 of the *Charter* than demands for information which are not judicially approved.

c) Court orders

A court order is a judicial order, other than a warrant or a subpoena, which allows for search and seizure of personal information under certain circumstances. These circumstances will usually be non-criminal in nature. For example, a court order known as a "CSIS warrant" can be issued pursuant to s.21 of the *Canadian Security Intelligence Service Act* to apprehend terrorists' personal information where there are no reasonable and probable grounds of a completed crime but where there are reasonable and probable grounds to suspect threats to national security.[47] Another circumstance in which a court order may be issued is pursuant to s.231.7 of the *Income Tax Act* where a court wants to ensure private sector entities comply with CRA demands of personal information made under s.231.1 or s.231.2 of the *Act*. A court order that directly assists regulators can indirectly assist police; as indicated above, regulators who discover evidence of a crime or a terrorist threat in the course of predominantly regulatory activities can provide this evidence to police.

d) Warrantless Search or Seizures

A warrantless search or seizure on private property in the context of a criminal investigation is *prima facie* unreasonable, thus a violation of s.8 of the *Charter*. However, the *Charter* permits warrantless searches and seizures for criminal investigations in rare and exigent circumstances. For example, where police are in "hot pursuit" of a criminal who is trying to elude police, they may enter premises without a

---

[44] *Supra*, note 19.
[45] *Supra*, note 18.
[46] *R. v. Mills*, [1999] 3 S.C.R. 668.
[47] *R. v. Atwal* (1987), 59 C.R. (3d) 339 (F.C.A.).

warrant to apprehend him or her.[48] It is unclear whether this power allows police to seek a suspect's personal information from private sector entities without a warrant in circumstances where there are sufficient grounds to indicate that the information would be imminently lost or destroyed if time was taken to obtain a warrant.

In non-emergency cases in which there is not a warrant or court order, it is worthwhile to note that s. 7(3) of *PIPEDA* makes a distinction between non-consensual disclosure to government institutions that occurs on the initiative of the private entity and that which occurs as a result of a request by the government institution.[49] The Act is permissive towards disclosure to government institutions that take place on the initiative of the private entity if the organization has "reasonable grounds to believe that the information relates to … a contravention of the laws of Canada, a province or a foreign jurisdiction"[50] or if it "suspects that the information relates to national security, the defence of Canada or the conduct of international affairs."[51] Notably, the standard for disclosure in ordinary law enforcement contexts is higher than in cases of potential threats to national security.

When the government institution makes the request it must identify its lawful authority as well as indicating one of three things. According to s. 7(3)(c.1) it must indicate either that[52]

(i) it suspects that the information relates to national security, the defence of Canada or the conduct of international affairs,

(ii) disclosure is requested for the purpose of enforcing any law of Canada, a province or a foreign jurisdiction, carrying out an investigation relating to the enforcement of any such law or gathering intelligence for the purpose of enforcing any such law, or

(iii) disclosure is requested for the purpose of administering any law of Canada or a province.

The effect of this section appears to permit private entities to make disclosure to government institutions in response to requests for information for purposes of national security or law enforcement where lawful authority has been identified; it does not require disclosure. The foregoing has been the interpretation of the Office of the Privacy Commissioner who described *PIPEDA* as providing telecommunications service providers with a discretionary authority to provide personal information to law enforcement.[53] There is no apparent reason to believe that these observations would not apply equally to all organizations covered by *PIPEDA*. The OPC stressed that the government institution cannot compel production in the absence of a court order or warrant.[54] This interpretation is bolstered by the fact that the section provides that the organization "may disclose" and not that it shall.[55]

---

[48] *R. v. Feeney*, [1997] 2 S.C.R. 13.
[49] *PIPEDA* s. 7(3)(c.1) & (d).
[50] *PIPEDA* s. 7(3)(d)(i).
[51] s. 7(3)(d)(ii).
[52] s. 7(3)(c.1).
[53] http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp (last accessed on January 29, 2008).
[54] *Ibid.*
[55] *PIPEDA* s. 7(3).

A recent decision of the Ontario Court of Justice, however, potentially contradicts this interpretation. In *Re: S.C.*, Conacher P.J. denies a request for a search warrant after finding that some of the evidence in support of the application had been obtained by the police without lawful authority.[56] In a recent article in the *Canadian Privacy Law Review*, Howard R. Fohr interprets the judgment as indicating that s. 7(3)(c.1) requires that the "'lawful authority' to obtain information must first be established by the government institution, and that *PIPEDA* itself does not establish the authority for it to obtain the information."[57] Nor, according to Conacher P.J., is indication that the request is being made for a criminal investigation sufficient for establishing such authority.[58] Conacher P.J. concludes that as the enterprise had no basis to disclose the information, it was not lawfully obtained and could not be considered in the application for the search warrant.[59]

The ruling does not make it entirely clear how a law enforcement agency could sufficiently identify its lawful authority. Conacher P.J. does, however, write that "in the absence of express authority within the legislation, the Charter right not to have one's reasonable expectation of privacy interfered with, except through prior judicial authorization with all the protections that affords, must govern."[60] As a result, the ruling would seem to at least derogate from the ability of law enforcement to make use of information requested in the absence of a warrant or court order. Considering that the identification of lawful authority by the government institution is a precondition of disclosure by the private entity,[61] this ruling would significantly restrict the circumstances under which private entities are permitted to disclose information to law enforcement and national security. As s.7(3) already permitted disclosure when there is judicial authorization or disclosure is required by law,[62] this ruling would imply that there are rather few instances in which s. 7(3)(c.1) provides a unique basis for disclosure.[63]

Some of the implications of this ruling may be surprising to some members of the industries that were studied in this report and would have the effect of at least narrowing the "discretionary authority" of industry to disclose personal information. There are, undoubtedly, reasons to question the authority of this judgment: it is the interpretation of a federal statute by a justice of the peace in a low level provincial court in the context of an application for a search warrant. Further, there seems to be something substantively amiss in Conacher P.J.'s address of the s. 8 Charter issue. Conacher P.J. does not sufficiently acknowledge that all information collection by police does not require a

---

[56] *Re: S.C.* 2006 ONCJ 343.
[57] Howard R. Fohr, "Disclosure" Canadian Privacy Law Review.
[58] *Re: S.C.* at para 9.
[59] *Re: S.C.* at para 11.
[60] *Re: S.C.*at para 11
[61] *PIPEDA* s. 7(3)(c.1)
[62] s.7(3)(c) & (i)
[63] A finding of the Office of the Privacy Commissioner of Canada exemplifies a case in which another subsection of s. 7(3) could have provided the basis for disclosure. The Canada Customs and Revenue Agency made a request for information from a bank pursuant to s. 7(3)(c.1)(ii) citing s. 231 of the Income Tax Act as providing it authority. However, considering that s. 238 of the Income Tax Act obligated the bank to comply, the CCRA might equally have maintained that the disclosure was required by law thereby making s. 7(3)(i) the basis for the disclosure.

warrant and that unlike other government institutions, police have an inherent investigative authority. Moreover, although there is a norm of prior judicial authorization and warrantless searches are presumptively unreasonable, there must be a reasonable expectation of privacy in the information in order for obtaining the information to be considered a search at all. The fact that this case pertains to a commercial relationship, that the manner in which and place from which the police obtained the information was relatively unintrusive of privacy and that the offence under investigation was quite serious are factors which may count against a court finding the requisite reasonable expectation of privacy for there to be an infringement of s. 8.[64] Moreover, the information must be of a personal and confidential nature that "tends to reveal intimate details of the lifestyle and personal choices of the individual" and it is not clear that the subscriber data obtained by the police meets that standard.[65]

It is, nonetheless, difficult to simply dismiss the reasoning of *Re: S.C.* considering the dearth of jurisprudence that particularly interprets this section of *PIPEDA*; this dearth is even more pronounced as pertains to law enforcement and national security. Conversely, there is significantly more guidance for interpreting s.7(3)(c) and disclosure pursuant to prior judicial authorization is much less problematic. Section 7(3)(c) permits private sector entities to disclose personal information to police when police provide them with warrants, subpoenas and court orders.

D) Analysis of Industries

Throughout analysis of information sharing for all four industries, the importance of balancing the privacy interests and rights of individuals with the investigatory interests of law enforcement and national security agencies has been a pervasive theme. The writers also considered important practical concerns of the industries.

Each industry-specific section includes: a) an overview of the industry and how it is regulated by law; b) discussion of the personal information collected by the industry as well as analysis of the capacity for combining or compiling information in relation to the applicable privacy regime; c) discussion of the interest of law enforcement and national security in the information collected by the industry as well as the legal mechanisms that restrict or otherwise shape information sharing; d) discussion of formal and informal information sharing practices; e) discussion of gaps in privacy protection and privacy-related controversies; and, finally, f) conclusions regarding privacy protection and information sharing in the industry as well as recommendations for improving privacy protections. This analysis results in identification of a number of recurring as well as industry-specific concerns.

Recurring concerns include lack of clarity regarding the interpretation of s. 7(3) of *PIPEDA*, the impact of technological development on the balance of relevant interests, lack of transparency regarding informal information sharing, and an identified tendency

[64] *R. v. Plant* at para 32.
[65] *Ibid.* at para 27.

towards collection of increasing amounts of personal information identified in some of the industries. Some persistent constitutional issues are the departure from the principal of judicial authorization in many cases of information sharing without warrants or court orders, lack of certainty regarding whether there is a reasonable expectation of privacy in various contexts and the constitutional sufficiency of the standard for disclosure in instances where information is obtained notwithstanding a lack of reasonable probable grounds to believe that a crime has been committed. This last concern is particularly pressing should disclosure of information be mandatory.

1) The Telecommunications Industry

The analysis of the telecommunications industry shows that gaps and lack of clarity in the law have somewhat frustrated the attainment of a clear, satisfactory balance between the privacy interests of individuals, on the one hand, and the investigative interests of law enforcement and national security on the other. The problems posed by s. 7(3)(c.1) of *Personal Information Protection and Electronic Documents Act* and the discretion it seemingly gives telecommunications companies with respect to the disclosure of the personal information of its customers were principle among the gaps in privacy protection and the privacy related controversies arising in the telecommunications industry. Making the disclosure mandatory under the provision, however, would be an ineffective means of solving the problem considering the uncertainty concerning the reasonable expectation of privacy in Internet communications and the unclear *Charter* implications of such an amendment. Mandatory disclosure would, furthermore, be problematic due to the fact that it is a broadly applicable provision that does not circumscribe the types of personal information that may be disclosed and the fact that it would trench on the norm of judicial authorization in search and seizure law.

2) The Retail Industry

Analysis of the Canadian retail industry shows a current state of equilibrium between security and safety on the one hand and privacy rights on the other. However, the current regulatory scheme may be insufficient to maintain the current level of protection of individual privacy, especially given the likelihood of future technological developments facilitating data aggregation and data mining.

3) The Banking Industry

Analysis of the banking industry shows an increasing tendency by the banks to retain more personal information, and that banks have not effectively indicated to clients the extent of personal information it needs to collect for many of their services. More specifically, it reveals that: major banks receive many informal requests from police to disclose bank records; even where banks keep a record of the nature and extent of informal police requests, their legality is often not assessed by an independent and

publicly accountable authority; there remains uncertainty about under what circumstances bank records can be released without judicial authorization but in conformity with *PIPEDA*; and that the constitutionality of the 'reasonable suspicion' standard used by FINTRAC in its disclosures of bank records to police is not yet certain.

4) The Airline Industry

Analysis of the airline industry shows that balance of individual privacy interests with national security in current law and practice creates the potential for infringement of privacy rights beyond that which can be justified in the name of national security. There are a number of areas of concern. Even if an airline earnestly wanted to protect its customers' privacy, it will be hard pressed to do so when faced with the requirements of various legislative provisions which make disclosure of information mandatory even absent any proof that the collection is justified. Another threat to privacy is the vagueness of the provisions of the Customs Act that establish the PAXIS database. The continuous data streaming of Advance Passenger Information and Passenger Name Record information on all passengers entering Canada facilitates the authorities in fishing for information about individuals, results in a lack of transparency about police investigations, and does not accord with the plain meaning of the words in the *Aeronautics Act.* The Passenger Protect Program (involving no-fly lists) though helpful for protecting the safety of airplanes would benefit from safeguards to better protect individual privacy to reduce the probability of false listing and false matches. This paper also takes the position airlines ought to avoid informal information sharing with police given the high level of mandatory reporting already required by law.

II. Telecommunications Industry

Written by Aba Stevens

Introduction

Privacy issues surrounding the interaction of law enforcement and national security agencies with telecommunications service providers (TSPs) has already received considerable attention from a policy perspective. The Council of Europe's *Convention on Cybercrime* articulates the interest of government agencies in personal data from TSPs. The proposed *Modernization of Investigative Techniques Act*[66] and the Lawful Access Consultation have respectively shown the shape that the requirements of the Convention may take in the Canadian context and some of the resulting controversies. This section of the report will take account of the special status of the telecommunications industry as an industry under the jurisdiction of an independent regulatory agency. The essay will consider the particular interest of law enforcement in the types of information collected by organizations in this industry, particularly as revealed by the Council of Europe *Convention on Cybercrime* and the Lawful Access Consultation. Ultimately, consideration of existing legal mechanisms will show that the current statutory and common law landscape leave much up to the contractual undertakings and the exercise of discretion by telecommunications companies.

This analysis of the telecommunications industry proceeds as follows: A) a brief overview of the industry points to the extensive reach of the industry, its asymmetric growth and the role that the industry's regulatory body has chosen to assume, which have resulted in a less settled landscape for Internet services and, to a lesser extent, mobile phone in comparison to other telecommunications services; B) consideration of the information collected by the industry reveals that telecommunications organizations have a unique capacity to access particularly sensitive personal information due to the nature of the services they provide, and that *PIPEDA* is the dominant regime governing that collection; C) discussion of recent law reform as an expression of law enforcement's interest in the information potentially accessible by these organizations also suggests that *PIPEDA* is the main statute circumscribing the ability of the police to obtain the information it seeks although the *Charter* may apply in some cases; D) consideration of the instances in which telecommunications organizations are likely to exercise discretion to disclose to law enforcement or national security agencies, especially a particular emerging practice that has developed in the industry which converges the realms of formal and informal information sharing practices; and E) identification of gaps and controversies, focusing on the uncertainties within the legal regime and the controversial proposals for law reform.

---

[66] The *Modernization of Investigative Techniques Act* was initially proposed as Bill C-74. It has been re-introduced as Bill C-416; it has not yet passed into law. See Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005. See also Bill C-416, *Modernization of Investigative Techniques Act*, 1st Sess., 39th Parl., 2007.

A) Overview of the Industry and How it is Regulated by Law

There has been a particular concentration on Internet services in recent policy and law reform discussion pertaining to the telecommunications industry. In this respect, mobile phone services appear to assume the position of a distant second place. The following overview of the industry mirrors this focus. This section posits that this phenomenon is likely owing to 1) technological development and asymmetric growth of the industry as well as 2) policy choices of the industry's regulatory body, which have resulted in varying levels of regulatory certainty amongst the industry's many services.

Although the telecommunications service industry has nearly universal reach in Canada with over 98% of households in Canada subscribing to phone service, it is an industry that continues to grow.[67] In 2006, the industry experienced a 4.5% increase in revenue over the previous year.[68] Significantly, Internet and mobile phone services accounted for the majority of this increase,[69] and these two categories of services are the source of the greatest controversy with respect to information sharing between law enforcement and national security.

Like other federally regulated industries as well as the retail sector, telecommunications companies are subject to *PIPEDA* in relation to the collection, use, disclosure and retention of personal information as explained above in the general section of the report. In addition, the general regulation of the telecommunications industry falls under the purview of the Canadian Radio-television and Telecommunications Commission (CRTC) through its jurisdiction under the *Telecommunications Act*.[70] The *Telecommunications Act* provides for at least some protection of privacy, as among the telecommunications policy objectives is the protection of the privacy of persons.[71] The effect of overlapping regulatory regimes on privacy protection will be discussed in greater detail below. It is, however, worthwhile to note that even though the *Telecommunications Act* defines the term "telecommunications" broadly as "the emission, transmission or reception of intelligence by any wire, cable, radio, optical or other electromagnetic system, or by any similar technical system,"[72] the CRTC in practice has been more vigilant in protecting the privacy of consumers of some types of services than others. The result is the likelihood that the *Telecommunications Act* and the CRTC's regulation of the industry more effectively remedies the shortcomings of *PIPEDA* for some types of telecommunications than others.

---

[67] Canada, Canadian Radio-television and Telecommunications Commission, *CRTC Telecommunications Monitoring Report 2007* (Ottawa: Canadian Radio-television and Telecommunications Commission, July 2007), available online: http://www.crtc.gc.ca/eng/publications/reports/PolicyMonitoring/2007/tmr2007.htm (last accessed on January 29, 2008).
[68] *Ibid.*
[69] *Ibid.*
[70] *Canadian Radio-television and Telecommunications Act*, S.C. 1974-75-76, c. 49, cl. 12(2).
[71] *Telecommunications Act*, S.C. 1993, c. 38, s. 7(i).
[72] *Telecommunications Act*, s. 2(1).

B) Information Collected by the Industry

Information collection by telecommunications companies reveals itself to be varied in terms of the types of information collected and the sources of law with the potential of shaping the collection. The following analysis will consider 1) the nature of information collection by Telecommunications companies and 2) the legal regime governing collection. The focus will once again be on Internet services. Note that for the purpose of the following analysis Internet Service Providers are Telecommunications Service Providers which provide the backbone service of connecting consumers to the Internet.

1) Nature of Information Collection

This section reveals that some of the most sensitive personal information in the custody of telecommunications organizations is not in a strict sense collected by the organization, or if it is collected is not retained for a substantial period of time. For some information it may be more apt to describe the telecommunications organization as having only transient access. This subsection will describe (a) active information collection for the purpose of providing the service and (b) the ability of telecommunications service providers to access information that passes over its network. For the latter consideration, particular attention will be given to electronic mail and will proceed by distinguishing the e-mail service provided by telecommunications service providers and providers of online e-mail accounts as well as highlighting the access of telecommunications companies to data pertaining to e-mail as quite ephemeral.

In accordance with *PIPEDA*, privacy policies of major telecommunications companies generally promise that collection of information will be limited to that which is necessary for the provision of the service.[73] Personal information - that is, information about an identifiable individual - may include such information as name, e-mail address, mailing address, telephone number, record of complaints, birth date, financial information, service and equipment.[74] Information pertaining to activity that takes place on the telecommunication service provider's network such as transmission and content of the communications themselves fall within the scope of personal information as well. Telecommunications companies have some capacity to monitor the activity that takes place over their networks. [75] However, the tendency of telecommunications service

---

[73] *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, cl. 1-4.

[74] See for instance *Frequently Asked Questions* at the Rogers website, available online: http://shoprogersfaq.custhelp.com/cgi-bin/shoprogersfaq.cfg/php/enduser/std_alp.php?p_sid=2NAKmcIh&p_lva=&p_li=&p_page=1&p_prod_lvl1=204&p_prod_lvl2=205&p_search_text=&p_new_search=1&p_search_type=4&p_sort_by=dflt.(last accessed on January 29, 2008).

[75] ISPs such as America Online already monitor for some offensive content. ISPs have the ability to retain web addresses which may reveal search terms entered by the user. Telecommunications companies providing mobile phone service can also track the geographical location of a mobile phone that is powered on in real-time. Stanley A. Cohen, *Privacy, Crime and Terror: Legal Rights and Security in a Time of Peril* (Markham: LexisNexis Butterworths, 2005) at 483. See also Dearbhail McDonald and Breda Heffernan, "Mobiles the key weapon in wave of new trials,"*Independent.ie* July 24 2007, online:

providers to collect these sorts of information is less clear. There are particular questions about the manner in which Internet Service Providers handle the content of communications such as electronic mail (e-mail).

E-mail service providers can be broken into two broad categories for present purposes. Telecommunication Service Providers which provide the backbone service of connecting customers to the Internet may also be called Internet Service Providers and usually provide e-mail accounts to their customers. Subscribers will generally download and store messages on their personal computers. On the other hand, providers of on-line e-mail service store messages on their servers and allow account holders to access them from any remote location with an Internet connection. Examples of online e-mail service providers include Yahoo, Microsoft's Hotmail and Google's G-mail. In the latter category, storage of messages is a key aspect of the service afforded to account holders. In this case, the e-mail service provider may have prolonged access to the content of the communication as well as data pertaining to the message's transmission. These service providers are, thus, the custodians of a large volume of information that may be of interest to law enforcement and national security and they promise varying degrees of protection for the privacy of account holders.[76] Nonetheless, companies that provide e-mail services in conjunction with facilitating consumer access to the Internet will be the focus of the present analysis not only because these companies are more readily understood as telecommunications companies but also because they have been the focus of attempts at law reform.

For e-mail accounts provided by Internet Service Providers (ISPs), messages are often stored on an ISP's server pending delivery to the recipient. This storage has the potential of being extremely transient. In fact, such factors as costs and technical demands on networks are disincentives to the retention of data by ISPs.[77] There are, nonetheless, numerous reasons which may cause an e-mail message to stay on an ISP server for longer periods of time including failure of the recipient to download the message into his or her inbox or an account being automatically disabled by the ISPs system security safeguards.[78] Another instance, in which the service providers tend to store communications for a period exceeding that which would ordinarily be required for a

---

http://www.independent.ie/national-news/mobiles-the-key-weapon-in-wave-of-new-trials-1043101.html (last accessed on January 29, 2008).

[76] Professor Kerr's survey of the varying levels of privacy protection offered to consumers did not distinguish between service providers on the basis of whether it was a telecommunications company. See Ian Kerr, "Personal Relationships in the Year 2000: Me and My ISP" in Law Commission of Canada ed., *Personal Relationships of Dependence and Interdependence in Law* (Vancouver: UBC Press, 2002) 78 at 87.

[77] *Summary of Submissions to the Lawful Access Consultation* (6 August 2003), "Chapter 4: Comments by Industry", para. K-1, available online through the Department of Justice Canada: www.justice.gc.ca/en/cons/la_al/summary/4.html. (last accessed on January 29, 2008).

[78] In *R. v. Weir* the accused's account was disabled automatically due to the excessive size of file attachments. *R. v. Weir*, 2001 ABCA 181. See also Daphne Gilbert, Ian R. Kerr & Jena McGill, "The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers" (2006) 51 *Criminal L.Q.* 473 at 475.

message to reach its destination is when a client account has been suspended.[79] While this interim storage may not be the collection of the information per se, history has revealed the potential for the service provider to access and scrutinize information while it is in its possession.[80]

Even after an ISP may no longer have access to the content of a telecommunication such as the body of an e-mail, they may still have data pertaining to the transmission of the message including the origin, destination, route and size of a communication as well as the date and time at which it was sent.[81] Once again, this data may be ephemeral due to the same factors that act as disincentives against ISPs retaining content data. The forgoing demonstrates that for this industry some of the most personally sensitive data may not be that which is purposely collected, but the information to which it arguably has access due to its role as a conduit of communications.

2) Legal Regime Governing Information Collection

The following section explains the manner in which the various sources of law with the potential of bearing on the collection of information by telecommunications companies – including *PIPEDA*, the *Telecommunications Act*, contractual agreements between companies and their clients and the *Charter* – shape the information practices of the organizations. The following begins by a) highlighting *PIPEDA* as the dominant regime governing the information practices of Telecommunications organizations despite the jurisdiction of the CRTC in the area of privacy protection. It then discusses b) the crucial role of the contractual undertakings of companies in determining what consumers can expect of the information practices of their telecommunication service providers. It ends by suggesting c) the limited applicability of the *Charter*.

PIPEDA appears to provide the dominant legal regime governing the collection of information by telecommunications companies. Privacy policies of major telecommunications organizations refer to their compliance with *PIPEDA* and assume much of that Act's language while making little or no mention to the CRTC or the *Telecommunications Act*.[82] As detailed above, the tenor of *PIPEDA* is to restrict the

---

[79] *PIPEDA Case summary #66*, Office of the Privacy Commissioner of Canada, "Internet service provider accused of withholding e-mails sent to suspended account," (28 August 2002), online: Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020828_e.asp (last checked on January 29, 2008).

[80] *R v. Weir*, [1998] A.J. No. 155 at para. 4, 59 Alta. L.R. (Q.B).

[81] "Explanatory Report," *Convention on Cybercrime* (23 November 2001), at para. 29 available online at <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm> (last accessed on January 29, 2008).

[82] The *Bell Code of Fair Information Practices*, makes explicit reference to *PIPEDA* and does not mention the Telecommunication Act or the CRTC. See *Bell Code of Fair Information Practices*, available online at: http://www.bell.ca/web/common/en/all_regions/pdfs/bcfip.pdf (last accessed on January 29, 2008). COGECO's Privacy Policy similarly does not mention either the CTRC or the *Telecommunications Act*. See "Privacy Policy," available online at:. http://www.cogeco.ca/en/security_privacy_o.html (last accessed on January 29, 2008). It is likewise for Shaw. See also "Privacy Policy Principles," available online at: http://www.shaw.ca/en-ca/AboutShaw/PrivacyPolicy/Principles.htm#q10 (last accessed on January 29, 2008). Rogers, however, does state that its Privacy Policy is compliant with not only *PIPEDA* but also with the privacy rules of the CRTC where applicable. See "Privacy Policy," available online at:

retention of personal information except where there is the consent of the individual or retention is required by law. However, it is not apparent that *PIPEDA* will be used to restrict the purposes for which information can be retained. For instance, the Privacy Commissioner of Canada found that it was standard practice of ISPs to receive and store e-mail messages that were sent to clients with suspended accounts in order to make them pay their arrears and that this practice was not contrary to *PIPEDA* so long as the ISP adequately disclosed its suspension policy.[83]

This ruling of the Privacy Commissioner demonstrates that to a considerable extent the permissibility of collection of information and monitoring depends on the contractual relationship between Internet Service Providers and their customers. The level of confidentiality that Internet service providers promise their costumers varies from promises of confidentiality to the prospect of active monitoring and voluntary disclosure to law enforcement by the ISP.[84] The practices of the major Canadian telecommunications companies tend to fall in between these two extremes.

Rogers, Bell, Shaw Cable and COGECO provide Internet services to substantial numbers of Canadians.[85] All have Acceptable Use Policies, compliance with which is a condition of the terms of service outlining the contractual relationship between the company and the customer.[86] Prohibition of use of the service for illegal activity is standard though the terms of service go into varying levels of specificity in providing examples of illegal

---

http://www.shoprogers.com/privacy1.asp (last accessed on January 29, 2008) . The Telus Privacy Code does not mention the CRTC. but its Privacy Commitment makes several references to the CRTC's regulations. See "Telus Privacy Code," available online at: http://about.telus.com/legal/privacy/downloads/privacy_code.pdf (last accessed on January 29, 2008). See also "Privacy Commitment" available online at: http://about.telus.com/legal/privacy/brochure.html (last accessed on January 29, 2008).

[83] "Internet service provider accused of withholding e-mails sent to suspended account," *Commissioner's Findings*, available online at: Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020828_e.asp (last accessed on January 29, 2008).

[84] Ian Kerr, "Personal Relationships in the Year 2000: Me and My ISP" in *Law Commission of Canada ed., Personal Relationships of Dependence and Interdependence in Law* (Vancouver: UBC Press, 2002) 78 at 87.

[85] The top four providers of retail Internet service in Canada are Rogers, Shaw, Bell and Telus Communications Company. See Canada, Canadian Radio-television and Telecommunications Commission, *CRTC Telecommunications Monitoring Report 2007*, supra note 67. Telus Communications Company, however, provides its high speed Internet service to business customers. See Telus, available online at: http://www2.telus.com/cgi-ebs/jsp/homepage.jsp (last accessed on January 29, 2008).

[86] *COGECO CABLE CANADA INC. General Terms and Conditions* – Residential Services (20 May 2005) at para 25, available online at: http://www.cogeco.com/files/pdf/legal/Terms_and_Conditions_on_en_050520.pdf (last accessed on January 29, 2008). See also *Joint Terms of Service*, available online at: http://www.shaw.ca/en-ca/AboutShaw/TermsofUse/JointTermsofService.htm (last accessed on January 29, 2008). "Rogers Terms of Service," available online at: https://www.shoprogers.com/about/legaldisclaimer/TOS_Eng.pdf (last accessed on January 29, 2008). See also "Sympatico High Speed, High Speed Ultra, Basic and Basic Lite Internet Service," available online at: http://service.sympatico.ca/index.cfm?method=content.view&category_id=550&content_id=921 (last accessed on January 29, 2008).

use.[87] Use of the service to infringe copyright law, harass other users of the Internet or access or distribute child pornography are recurring examples of prohibited activities that are mentioned through the Terms of Service and Acceptable Use Policies. In addition, these contracts also prohibit activities that are likely to interfere with the company's network or the use of the Internet by other clients.

The telecommunications companies explicitly reserve the right to monitor such aspects of services and network to ensure compliance with their Acceptable Use Policy while stating that they are under no obligation to monitor. COGECO does so as follows in its Acceptable Use Policy: "Although COGECO has no obligation to monitor the Services and/or network, COGECO reserves the right to monitor bandwidth, usage, and content from time to time to operate the Services; to identify violations of this AUP; and/or protect the network and COGECO Customers."[88] Shaw's Acceptable Use Policy states that "Shaw has no obligation to monitor transmission made on the Services. However, Shaw has the right to monitor such transmissions and to disclose the same in accordance with Shaw's Privacy Policy."[89] Rogers states that it has "the right but not the obligation, to monitor or investigate any content that is transmitted using the Services or the Equipment; and to access or preserve content or information in accordance with the Terms."[90] Bell Canada's service agreement for its high speed as well as some other varieties of Internet service states that customers "agree that [their] Service Provider reserves the right from time to time to monitor the Service electronically, monitor or investigate content or [their] use of [their] Service Provider's networks."[91]

Subject to what is explained above in the introduction, monitoring by a private entity will ordinarily not fall under the purview of the *Charter*. It is nonetheless possible that monitoring by a private entity owner of facilities is an invasion of the privacy of an individual. In a case in which security guards of a bus depot opened a locker in order to investigate what they suspected was the odor of marijuana, the court found that the

---

[87] *COGECO High Speed Internet Service Acceptable Use Policy*, available online at: http://www.cogeco.ca/files/pdf/legal/HSI_PUA_on_en.pdf (last accessed on January 29, 2008). See also Acceptable Use Policy – Internet, available online at: http://www.shaw.ca/en-ca/AboutShaw/TermsofUse/AcceptableUsePolicyInternet.htm (last accessed on January 29, 2008). See also Acceptable Use Policy, available online at: Rogers https://www.shoprogers.com/about/legaldisclaimer/Unified_AUP_Eng.pdf (last accessed on January 29, 2008). See also "Sympatico™ High Speed, High Speed Ultra, Basic and Basic Lite Internet Service," available online: Bell at para. 2 http://service.sympatico.ca/index.cfm?method=content.view&category_id=550&content_id=921 (last accessed on January 29, 2008).

[88] COGECO High Speed Internet Service Acceptable Use Policy at 3, available online at: http://www.cogeco.ca/files/pdf/legal/HSI_PUA_on_en.pdf (last accessed on January 29, 2008).

[89] Acceptable Use Policy – Internet, available online at: Shaw http://www.shaw.ca/en-ca/AboutShaw/TermsofUse/AcceptableUsePolicyInternet.htm (last accessed on January 29, 2008).

[90] *Acceptable Use Policy*,available at 5 online: Rogers https://www.shoprogers.com/about/legaldisclaimer/Unified_AUP_Eng.pdf (last accessed on January 29, 2008).

[91] Sympatico™ High Speed, High Speed Ultra, Basic and Basic Lite Internet Service, available online at: Bell at para. 17 http://service.sympatico.ca/index.cfm?method=content.view&category_id=550&content_id=921 (last accessed on January 29, 2008).

security guards did not have a right to enter as the defendant had a contractual right to exclusive use of the locker and a reasonable expectation of privacy in its contents.[92] The court finds that "a reasonable person would expect that his or her private belongings, when secured in a locker that he or she has paid money to rent, will be left alone, unless the contents appeared to pose a threat to the security of the bus depot."[93]

The central issue in analyzing the right of the security guards to enter was the reasonable expectation of privacy of the individual and the court was notably unimpressed by the Crown's argument that the bus depot's possession of a key by which they could access the locker diminished the accused reasonable expectation of privacy in the contents.[94] What was more important than the ability of the private entity to enter was what constituted a reasonable understanding of the purposes for which the private entity would enter.[95] This focus highlights the importance of the contractual relationship between the Internet Service Provider and the customer. Arguably, where the Internet Service Provider explicitly reserves the right to monitor for the purposes of enforcing the terms of the agreement, a reasonable person would be alerted to the possibility that the ISP will do so. Further, as explained above what constitutes a reasonable expectation of privacy is a highly contextual inquiry and facilities provided by a bus depot for storage are not altogether analogous with the use of a Telecommunication Service Providers network by a customer.[96] While the storage locker cases are useful to the consideration of the impact of contractual arrangements on the accused's reasonable expectation of privacy, it is common to see the interception of data while it is being transmitted through the Internet as more analogous to wiretap, which has its own jurisprudence.[97]

C) Personal Information of Interest to Law Enforcement and Legal Mechanisms Shaping Information Sharing

1) Information of Interest to Law Enforcement and the Desire for Law Reform

The best evidence of the types of information that law enforcement would like to access emerges from substantial recent policy and law reform discussion that has sought to facilitate police access to information passing over the Internet. The following a) points to recent international and national initiatives as reflecting a desire for law reform, b) explains how the definitions of information passing over the Internet has been delineated nationally and internationally, and c) describes the expressed interest of law enforcement

---

[92] *R v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631 at para. 20.
[93] *Ibid.* at para. 21.
[94] *Ibid.* at para. 22.
[95] *Ibid.* at para. 22.
[96] The court has recognized a reasonable expectation of privacy in e-mail, which is only one form of Internet communication contemplated by the service agreements. The case that recognized this reasonable expectation was not concerned with the fact that the TSP accessed this information. Notably, however, Weir did not involve monitoring that was initiated by the TSP, but rather a TSPs response to the customer's request for repair.
[97] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 15, available online at: http://www.justice.gc.ca/en/cons/la_al/law_access.pdf (last accessed on January 28, 2008).

in these various types of information. The section ends by briefly discussing the likely interest of law enforcement in information accessible through wireless technology.

There has been activity at both the international and national level in recent years that reflects a desire on the part of law enforcement to alter the legal regime governing collection as well as disclosure of information by telecommunications companies. The Council of Europe's *Convention on Cybercrime* provides insight into the sorts of information potentially accessible by Internet Service Providers that is of interest to the state. Furthermore, both the Lawful Access Consultation and the proposed *Modernization of Investigative Techniques Act* articulate the interest of the Canadian law enforcement and national security establishments in such information more specifically.

The *Convention on Cybercrime* breaks the investigatory information sought by law enforcement into three categories: content data, traffic data and subscriber information.[98] Although the Convention does not describe content data, some examples are text of e-mail messages and search terms entered into search engines. The Explanatory Report of the Convention reflects particular alertness to the intrusiveness of the interception of content data.[99] Significantly, this form of data while arguably accessible by ISPs, at least intermittently, is the form of data that an ISP is least likely to collect. The Convention defines traffic data as "any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service."[100] The Convention describes subscriber data as[101]

> any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established:
>
> (a) the type of communication service used, the technical provisions taken thereto and the period of service;
>
> (b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;
>
> (c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement."

Examples of subscriber data may include name, address, telephone number, e-

---

[98] "Explanatory Report," *Convention on Cybercrime* (23 November 2001), available online at: Council of Europe <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm> at para 136 (last accessed on January 29, 2008).
[99] *Ibid.* at para. 142.
[100] *Convention on Cybercrime* (23 November 2001), available online at: Council of Europe <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm> at cl. 1 (last accessed on January 29, 2008).
[101] *Ibid.* at cl. 18-3.

mail address or IP address.[102]

Notably the Canadian government's delineation of personal information relevant to lawful access is somewhat different from those of the Convention, as are its definitions for the resultant categories. For instance, Bill C-74 describes subscriber data as "any information in the service provider's possession or control respecting the name and address of any subscriber to any of the service provider's telecommunications services and respecting any other identifiers associated with the subscriber."[103] The proposed and currently stalled *Modernization of Investigative Techniques Act* would have particularly served the interests of law enforcement and national security agencies in relation to subscriber data.[104] The Bill would have allowed investigative agencies to obtain customer name and address as well as other identifiers without a warrant by making a written request.[105] Alternative systems for access suggested by the Canadian Association of Chiefs of Police are a database that would be populated by communication service providers and accessible by law enforcement and national security or a data system that would allow information requests to be automatically directed to the systems of service providers.[106] The essential point is that law enforcement and national security agencies seek the ability to access this information without having to obtain judicial authorization.[107] While it is likely permissible under *PIPEDA* for communication service providers to provide such information to law enforcement, current law does not oblige them to do so in the absence of a court order; law enforcement proposes to change that situation.

However, law enforcement and national security agencies have demonstrated interest in the types of data covered in all three categories identified in the Convention. Law enforcement seeks a similar process for the acquisition of traffic data as that for dialed number recorders (DNR) in the *Criminal Code*.[108] The introduction of preservation orders into Canadian law whereby a communication service provider such as an ISP would be obliged to protect data pending the attainment of judicial authorization for seizure seems to particularly apply to traffic data. Not only was traffic data particularly linked to preservation orders in the *Convention on Cybercrime* but this measure's responsiveness to the volatility of electronic information also provides law enforcement

---

[102] "Lawful Access: Police Surveillance" Canadian Internet Policy and Public Interest Clinic (2 June 2007), available online at: http://www.cippic.ca/en/projects-cases/lawful-access/ (last accessed on January 29, 2008).
[103] Bill C-416, *Modernization of Investigative Techniques Act*, 1st Sess., 39th Parl., 2007, cl. 17(1).
[104] *Ibid.* at cl. 3
[105] *ibid.* at cl. 17(1).
[106] *Summary of Submissions to the Lawful Access Consultation* (6 August 2003), "Chapter 3 : Comments by Law Enforcement", at para. I-4&5, available online at: Department of Justice Canada http://www.justice.gc.ca/en/cons/la_al/summary/3.html (last accessed on January 31, 2008).
[107] *Ibid*. at I-2.
[108] Section. 492.2(4) of the *Criminal Code* defines a number recorder as "any device that can be used to record or identify the telephone number or location of the telephone from which a telephone call originates, or at which it is received or intended to be received." *Criminal Code, R.S.C. 1985, c. C-46, s. 492.2(4).* See also *Summary of Submissions to the Lawful Access Consultation* (6 August 2003), "Chapter 3: Comments by Law Enforcement", at para. H-1, supra note 106.

with a means of counteracting the ephemeral nature of traffic data. [109]

The proposed *Modernization of Investigative Techniques Act*'s focus on subscriber data can be seen as a way to limit the state's intrusion on the individual's reasonable expectation of privacy. However, although Canadian law enforcement agreed that the interception of communications, which would likely entail access to content data, should continue to be subject to judicial authorization,[110] they were less reserved in their advocacy for increased access to traffic data, which is alternatively called transmission data. Law enforcement advocates that "search warrants should only be required for information that tends to reveal intimate details of the lifestyle and personal choices of the individual affected by the order" at the same time as advocating a DNR-style process for accessing traffic data.[111] Yet, the government has acknowledged that the distinction between content data and transmission data is technically and analytically arduous.[112] As the DNR process only requires the court be satisfied of reasonable grounds to suspect an offence,[113] implementation of the provision could risk that some of the most sensitive data will be accessible to law enforcement at a relatively low standard.

Notwithstanding recognition by law enforcement and lawmakers of the sensitivity of content data from a privacy perspective, the interest of law enforcement in this sort of information is palpable, as is the increased access that will be afforded if Bill C-416 passes. Law enforcement advocates that all telecommunications services in Canada should be "interceptable" such that communication service providers will be technically capable of providing law enforcement and national security real time access to a broad range of content data including the entire telecommunications of the subject.[114] Corresponding to this interest Bill C-416 would impose obligations on telecommunications service providers with respect to intercept capability.[115]

The attempts at law reform also reflect the state's interest in wireless technology.[116] Notably, Bill C-416 applies to wireless as well. One telecommunications company indicated that in the past they have most frequently received court orders for information

---

[109] "Explanatory Report," *Convention on Cybercrime* (23 November 2001), available online at: Council of Europe <http://conventions.coe.int/Treaty/EN/Reports/Html/185.htm> at para. 161 (last accessed on January 31, 2008).

[110] *Summary of Submissions to the Lawful Access Consultation* (6 August 2003), "Chapter 3 : Comments by Law Enforcement", para. M-2, supra note 106.

[111] *Ibid.* at para. G-3.

[112] Part of the analytical difficulty arises from the fact that the term "content" has not been defined. For instance, "at a practical level, there are circumstances … where "content" is apparently not excluded" from traffic data. The difficulty with the word "content" led the government to conclude that some content may have to be included. The content that will be excluded is that attracting a reasonable expectation of privacy. See *Transmission Data: Considerations for Criminal Law Policy* (February 2005) Department of Justice Canada at 2-4, 9 available online at: www.cippic.ca/uploads/JC_TransData_4.pdf.

[113] *Criminal Code*, R.S.C. 1985, c. C-46, s. 492.2.

[114] *Summary of Submissions to the Lawful Access Consultation* (6 August 2003), "Chapter 3 : Comments by Law Enforcement", paras. B-1&2, supra note 106.

[115] Bill C-74, *Modernization of Investigative Techniques Act*, 1st Sess., 38th Parl., 2005, cls. 6-16.

[116] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 7.

about calling history and the location of calls.[117] The utility of such information as location tracking in real-time and mobile phone records to law enforcement has been exemplified in other jurisdictions. The Australian government is hoping that the proposed *Telecommunication (Interception and Access) Bill* will facilitate criminal and terrorist investigation by allowing agencies to track the geographic location of individuals through their mobile phones without a warrant.[118] Mobile phone records were key evidence in a high profile murder conviction in Ireland.[119] The states interest in mobile phone records as evidence has impeded the efforts of the Irish telecommunications industry to reduce the required retention period from two years.[120]

2) Legal Mechanisms Shaping the Sharing of Information

The same legal mechanisms that set parameters around the collection of information shape the sharing of information by telecommunications organizations with law enforcement and national security agencies. This subsection a) explains in greater detail the overlapping statutory regimes of *PIPEDA* and the *Telecommunications Act*, suggesting that *PIPEDA* is once again dominant largely due to the actions of the CRTC. It furthermore b) explains the possibility of the *Charter*'s applicability to information sharing as exemplified by a case from the Alberta Court of Appeal, *R. v. Weir*.

a) Relationship between *PIPEDA* and the CRTC's protection of privacy under the *Telecommunications Act*

Related to the question of the type of information law enforcement seeks is the level of access that current legal mechanisms afford. The presence of two regulatory regimes with the mandate to protect privacy of consumers of telecommunications leaves room for uncertainty as to how the regimes coincide. In addition to *PIPEDA*, telecommunication companies are subject to the particular regulatory regime of the *Telecommunications Act* which confers powers to oversee the industry to the CRTC.[121] The court has found that the regulatory regimes of *PIPEDA* and the *Telecommunications Act* overlap[122] meaning that CRTC has the potential to play a role in protecting privacy as part of its regulation of the industry. It would nonetheless appear that *PIPEDA* has come to dominate the privacy landscape in the eyes of service providers.

---

[117] Interview conducted by the author with Drew McArthur, Corporate Affairs and Compliance Officer for TELUS on September 10, 2007. Hereinafter referred to as "Interview 3".
[118] "Mobiles to become tracking devices," *Australian IT*, (23 July 2007) available online at: http://www.australianit.news.com.au/story/0,24897,22116627-15306,00.html (last accessed January 31, 2008).
[119] Dearbhail McDonald and Breda Hefferman, "Mobiles the key weapon in wave of new trials, " *Independent.ie* (24 July 2007) online: http://www.independent.ie/national-news/mobiles-the-key-weapon-in-wave-of-new-trials-1043101.html?service=Print (last accessed on January 31, 2008).
[120] *Ibid*.
[121] *About the CRTC*, CRTC, available online at: http://www.crtc.gc.ca/eng/about.htm#mandate (last accessed on January 31, 2008).
[122] *Englander v. Telus Communications Inc*., 2004 FCA 387.

This section will focus on the CRTC, as an industry-specific regulatory body, to consider what it adds to the privacy matrix under which telecommunications organizations operate. It will i) demonstrate that the role of the CRTC in protecting privacy is less transparent than that of *PIPEDA;* ii) explore the manner in which the CRTC has asserted its jurisdiction over privacy; iii) compare, in a limited fashion, the protection of privacy by the CRTC with that of *PIPEDA* by reference to what each regime mandates about the disclosure of Local Service Provider Identification Information to law enforcement and iv) suggest that the CRTC has chosen not to exercise its jurisdiction over privacy to the greatest extent possible particularly with respect to new technologies.

As detailed above *PIPEDA* establishes conditions under which private entities such as telecommunications companies may disclose information in response to requests by government institutions such as law enforcement and national security agencies. However, as a reasonable interpretation of the provision is that telecommunications companies are not required to make disclosure even when these conditions are met,[123] *PIPEDA* likely makes disclosure to law enforcement permissible though not mandatory.

Of the two regimes the role of the CRTC in protecting privacy is arguably even less transparent. Whereas, *PIPEDA* articulates numerous standards against which the personal information practices of individuals can be scrutinized, the *Telecommunications Act* merely states that "to contribute to the protection of the privacy of persons" among the objectives of the telecommunications policy of Canada.[124] It thus falls to the CRTC to define what the protection of the privacy of persons means in a regulatory as opposed to a statutory context.

The CRTC has asserted its jurisdiction in the area. In its decision "Provision of subscribers' telecommunications service provider identification to law enforcement agencies" the CRTC describes itself as not being bound by *PIPEDA*.[125] The CRTC made this decision following an argument by Bell Canada that as the *Telecommunications Act* pre-dates *PIPEDA*, specifically deals with telecommunications and is the source of the CRTC's authority over privacy concerns in the industry, the *Telecommunications Act* has priority in this area.[126] In another decision "The Commission notes that the [*PIPEDA*] sets out regulations and standards relating to the privacy of personal information. However, the Commission also notes that its jurisdiction in this matter stems not from the [*PIPEDA*], but from the *Telecommunications Act*, and that in exercising its discretionary powers pursuant to the *Telecommunications Act*, it may apply different standards than those contemplated by the [*PIPEDA*]."[127]

---

[123] The OPC appears to have interpreted the provision in this manner. It also appears to be the dominant interpretation in the industry.
[124] *Telecommunications Act,* R.S.C. 1993, C. 38 cl. 7(i).
[125] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 August 2002) at para. 23, available online at: http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm (last accessed on January 31, 2008).
[126] *Ibid.* at para. 14.
[127] "Confidentiality provisions of Canadian carriers" *Telecom Decision CRTC 2003-33* at para 23, http://www.crtc.gc.ca/archive/ENG/decisions/2003/dt2003-33.pdf (last accessed on January 31, 2008).

The CRTC, nonetheless, used similar wording to describe the provisions contained in s. 7(3)(c.1) and (e) of *PIPEDA* concerning the conditions under which a law enforcement agency can obtain a Local Service Provider Identification (LSPID) and acknowledges this similarity.[128] There are some differences, however. Unlike the CRTC's conditions, *PIPEDA* s. 7(3)(c.1)(i) does not specify that the government authority must have "reasonable grounds" for suspecting that the information may be relevant to national security in order for there to be disclosure in response to a request by a government institution.[129] The requirement of reasonable grounds for suspicion under the CRTC's conditions for disclosure of LSPID sets a higher standard for disclosure than *PIPEDA*. However, by essentially combining s. 7(3)(c.1)(i) & (ii) into a single condition the CRTC would potentially allow Bell Canada broader power to disclose in relation to the administration (as opposed to the enforcement) of laws than *PIPEDA* does. Whereas *PIPEDA* allows for disclosure to government institutions including law enforcement agencies for the purpose of administering a law of Canada or a province;[130] the conditions of the CRTC also deem administration of the laws of a foreign jurisdiction to be a suitable purpose for disclosure.[131] The CRTC conditions further deem gathering intelligence for the purpose of administering a law to be a suitable purpose;[132] whereas, under *PIPEDA* intelligence gathering is only a suitable purpose for enforcing a law.[133] *PIPEDA* requires that organizations that disclose personal information due to an emergency inform the individual in writing without delay.[134] The CRTC condition relating to emergencies does not state such a requirement.[135]

Perhaps the most significant distinction between the relevant provisions of *PIPEDA* and the CRTC decision on LSPID associated with particular phone numbers is that following its statement of the conditions that a law enforcement agencies must satisfy in order to obtain LSPID information, it states that "LSPID *is to be released* to LEAs requesting it

---

[128] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, (12 August 2002) at para 23, available online at: http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm (last accessed on January 31, 2008).

[129] *PIPEDA*, s. 7(3)(c.1)(i). See also "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 April 2002) at para 22, available online at: http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm (last accessed on January 31, 2008).

[130] *PIPEDA*, s.7(3)(c.1)(i).

[131] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 April 2002) at para 22.

[132] *PIPEDA*, s. 7(3)(c.1)(ii).

[133] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 April 2002) at para. 22.

[134] *PIPEDA*, s. 7(3) (c.1)(e).

[135] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 April 2002) at para. 22.

for any of the reasons set out above."[136] This statement contrasts with that of *PIPEDA* which states that "an organization *may* disclose personal information"[137] only if particular conditions are met. Whereas, *PIPEDA* leaves disclosure within the discretion of the telecommunication service provider; the CRTC decision would at least seem to encourage disclosure even if it does not create an obligation to disclose.[138]

On the one hand, it seems likely that the tendency to develop the concept of privacy under the *Telecommunications Act* in accordance with the standards of *PIPEDA* would be even greater following the subsequent pronouncements of *Englander*. [139] Among the issues in *Englander* was whether *PIPEDA* permitted fees to be charged to customers who wished to not have their personal information listed in telephone directories. In *Englander*, contrary to the ruling of the Federal Court, the Federal Court of Appeal ruled that as the *Telecommunications Act* would require explicit wording to oust the jurisdiction of the Federal Court acting under *PIPEDA* and there was no such wording, there was a concurrent or overlapping jurisdiction on this issue between the CRTC and the Federal Court:[140]

> "Should the Federal Court, or this Court in appeal, decide that fees cannot be charged, the CRTC would have to revise its tariff in the same way it would have had to revise its tariff had it decided on the merit that the fee could be legally imposed and its decision on that point had been reversed on an appeal to the Court made under the provisions of the *Telecommunications Act*."[141] This ruling could provide an incentive for the CRTC to continue to approach privacy in a similar manner to *PIPEDA* in order to avoid judicial intervention whereby *PIPEDA* would take precedence.

In reality, there is considerable scope for the CRTC to regulate information sharing of telecommunications organizations with law enforcement and national security agencies. In *Englander*, the CRTC received judicial support for its role in regulating the protection of privacy in the telecommunications industry. Essentially, *PIPEDA* can overrule the *Telecommunications Act* only where there are contradictory provisions in the two Acts.[142] Considering that *PIPEDA* does not provide the clearest guidance about under what circumstances information may be shared with law enforcement, there is arguably considerable scope for the CRTC to regulate in this area without contradicting *PIPEDA*. Further, the Privacy Commissioner of Canada recognizes the CRTC mandate to establish

---

[136] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 April 2002) at para. 23.
[137] *PIPEDA*, s. 7(3).
[138] Although the language could be seen as creating an obligation to disclose, the *Lawful Access - Consultation Document* takes the view that law enforcement would not have a means of compelling disclosure when faced with non-cooperation by a custodian of information. *Lawful Access – Consultation Document*, (25 August 2002) at 15, online: Department of Justice Canada http://www.justice.gc.ca/en/cons/la_al/law_access.pdf (last accessed on January 31, 2008).
[139] *Englander v. Telus Communications Inc*., 2004 FCA 387 at para. 1.
[140] *Ibid*. at para. 78.
[141] *Ibid*. at para. 79.
[142] *Ibid*. at para. 83.

rules pertaining to the use or disclosure of personal information by the telecommunications industry.[143]

The CRTC does require telecommunications companies to file tariffs outlining confidentiality provisions. Although the definition of confidential information may vary somewhat by service, both large telecommunications companies interviewed saw the CRTC's regulation of privacy as applying to all telecommunications services. Both suggested that the CRTC's regulation resulted in telecommunications companies being subject to higher standards than other organizations in the private sector.

There is nonetheless reason to believe that the CRTC has demurred from assuming a strong regulatory role pertaining to privacy issues of relatively new technologies such as the Internet. In fact, the Chair of the Canadian Association of Internet Providers does not understand the CRTC as applying that portion of Act to Internet communications.[144] Apparently, the CRTC has indicated informally that it has no interest in applying that section of the *Telecommunications Act* to Internet communications. Notably, when the CRTC asserted its jurisdiction in the case described above, the question was under what conditions Bell Canada could provide law enforcement with local service provider identification associated with a particular telephone number.[145] The hands off approach of the CRTC towards the Internet is likely more pronounced for providers of derivative Internet services, largely because these services tend not to be understood as telecommunications. However, even the major telecommunications companies interviewed did not see the CRTC as filling the gaps of *PIPEDA* and there has not been significant change to the CRTC's provisions since the introduction of *PIPEDA*.[146] So it appears that the CRTC has not served to provide the answer to many of the questions left by *PIPEDA*.

b) The Agent of the State Test and the *Charter*

In addition to the statutory framework of *PIPEDA* and the *Telecommunications Act*, the *Charter of Rights and Freedoms* can bear on information sharing by Telecommunications Service Providers in certain circumstances. In *Buhay*, Decary J.A. explained that "the initial search of the appellant's locker by the security guards [could] only come under s. 8 scrutiny if the guards [could] be categorized either as 'part of government' or as performing a specific government function (*Eldridge v. British Columbia (Attorney General)*, [1997] 3 S.C.R. 624 (S.C.C.)), or if they can be considered state agents (*R. v.*

---

[143] *Response to the Government of Canada's "Lawful Access" Consultation: Submission of the Office of the Privacy Commissioner of Canada to the Minister of Justice and Attorney General of Canada* (5 May 2005) Privacy Commissioner of Canada, available online at: http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp (last accessed on January 31, 2008).

[144] Interview conducted by the author with Tom Copeland, Chair of the Canadian Association of Internet Providers on August 2, 2007. Hereinafter referred to as "Interview 1".

[145] "Provision of subscribers' telecommunications service provider identification to law enforcement agencies," *Telecom Decision CRTC 2002-21*, CRTC 2002-21 (12 August 2002) at para. 1, available online at: http://www.crtc.gc.ca/archive/ENG/Decisions/2002/dt2002-21.htm (last accessed on January 31, 2008).

[146] Interview 3, supra note 117.

Broyles, [1991] 3 S.C.R. 595 (S.C.C.); *M. (M.R.)*, *supra*)."[147] Whether the private enterprise can be seen as acting as an agent of the state is the most important consideration for determining whether information sharing between a telecommunications company and law enforcement or national security agency falls under the purview of the *Charter*. According to the *Broyles* Test, an informer is an agent of the state if the exchange between the informer and the accused would not have taken place in the same form and manner that it did without the state's intervention.[148]

A leading case found that an ISP, by forwarding messages containing child pornography in response to a request from law enforcement, had acted as an agent of the state.[149] In *Weir*, an ISP discovered files containing child pornography during repair of the defendant's account. After being voluntarily alerted of the files by the ISP, the police requested that the files be forwarded to them without a warrant. [150] The police also asked that the ISP re-enable Weir's account such that Weir would come in possession of the child pornography.[151] On the basis of the foregoing, the police obtained a warrant to seize Weir's computer. The court nonetheless found that the information obtained as a result of the warrant was admissible, as the police could have obtained a warrant based on the initial communication by the ISP alone.[152]

Weir was significant for several reasons. It provided an affirmative answer to the question of whether there is a reasonable expectation of privacy in e-mail.[153] The initial disclosure of information that the ISP discovered in the course of ordinary business operations did not engage the *Charter* making it permissible for the ISP to inform the police of the contraband.[154] Significantly, however, the *Charter* was engaged when the ISP responded to a request for information from law enforcement. While this finding does not entail that every response to a request by law enforcement will be a *Charter* violation, it casts doubt on the constitutionality of some of the provisions proposed in Bill C-416 and advocated for by law enforcement and national security. The ruling may also support the argument advanced by some civil liberties groups and the Privacy Commissioner of Canada that there is no evidence that the current laws are insufficient to meet the needs of law enforcement.[155] After all, Weir's conviction was upheld due to the fact that a warrant could have been obtained based on the ISP's initial disclosure; it was not necessary to engage the ISP as an agent of the state for investigatory purposes.

---

[147] *R. v. Buhay*, 2003 SCC 30, [2003] 1 S.C.R. 631 at para. 25.
[148] *R. v. Broyles*, [1991] 3 S.C.R. 595 at para. 30.
[149] *R. v. Weir*, 2001 ABCA 181, [2001] 11 W.W.R. 85 at para. 11.
[150] *Ibid.*, at para. 3.
[151] Notably, simply repairing the mailbox did not actually cause Weir to come in possession of the contraband. The ISP took the subsequent step of increasing Weir's storage limit. See *R. v. Weir*, (1998), 213 A.R. 285 (Alta. Q.B.) at paras. 17&19.
[152] *R. v. Weir*, 2001 ABCA 181, [2001] 11 W.W.R. 85 at para 12.
[153] *R. v. Weir*, (1998), 213 A.R. 285 (Alta. Q.B.) at para. 70.
[154] *R. v. Weir*, 2001 ABCA 181, [2001] 11 W.W.R. 85 at para 12.
[155] Response to the Government of Canada's "Lawful Access" Consultations (May 5, 2005) http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp Date Accessed: 27 July 2007. See also "Lawful Access: Police Surveillance" Canadian Internet Policy and Public Interest Clinic (2 June 2007), available online at: Canadian Internet Policy and Public Interest Clinic http://www.cippic.ca/en/projects-cases/lawful-access/ (last accessed on January 31, 2008).

D) Formal and Informal Information Sharing Practices

Weir reinforces that this activity for which there is a direct nexus between the private entity and law enforcement that has attracted the most attention and controversy. Information sharing most obviously implicates the privacy interests of individuals, is guided in part by a statutory provision that has been subject to different interpretations and is the most likely to engage the *Charter* in the information related activities of private telecommunications organizations. Weir also exemplifies informal information sharing between law enforcement and telecommunication providers. Considering that there is no statutory obligation for Internet Service Providers to disclose information to law enforcement in the absence of a warrant or court order, one could classify any such disclosure as informal to the extent that it depends on the discretion of the service provider and is not required by law. The following will consider 1) the instances in which telecommunications companies are likely to share information with law enforcement and national security agencies and 2) a standardized practice of information sharing that has emerged in cases of child pornography.

1) The Exercise of Discretionary Authority as Reflected in Terms of Services and Acceptable Use Policies

This subsection will attempt to describe the information sharing practices of telecommunications organizations with a focus on the manner in which they exercise the widely recognized though controversial discretionary authority to disclose information to law enforcement under s. 7(3)(c.1) of *PIPEDA*. Once again the ability of the TSP to legally disclose information will depend somewhat on the contractual arrangements between the TSP and the customer. This section will show that a) the terms of service may reflect the various ways in which TSPs choose to exercise the significant discretion that may be left to them by *PIPEDA* and the CRTC; b) all of the major telecommunications companies reserve the right to terminate or suspend service in response to breach of the Terms of Service including use of the service for illegal activities; and c) that the language contained in the terms of service may create varying expectations amongst customers as to when their TSPs will disclose information. The analysis will proceed through consideration of each major TSP in turn: COGECO, Shaw, Rogers, and Bell Canada.

In the absence of the customer's consent, COGECO's terms of service provides for disclosure that is "pursuant to a legal power." This language calls to mind the controversy of what constitutes lawful authority under s. 7(3)(c.1) of *PIPEDA* and renders the idea of disclosure "pursuant to a legal power" even more unclear than it otherwise would be.[156] COGECO, at least, seems to contemplate disclosure in the absence of a warrant on the basis of reasonable evidence. The COGECO High Speed Internet Service Acceptable Use Policy states that "COGECO may cooperate with law enforcement authorities in the investigation of suspected violations of any applicable laws, regulation, public AUP or order of a public authority having jurisdiction. Such cooperation may include COGECO providing the Customer's username, IP address, or

[156] *Re. S.C.*, 2006 ABQB 709.

other information based on reasonable evidence and/or receipt of a warrant… COGECO, in its sole discretion will determine what action will be taken in response to a violation on a case-by-case basis."[157]

Shaw reserves the right to disclose subject to its privacy policy. Shaw states that in its "efforts to promote good citizenship within the Internet community, [it] will respond appropriately if it becomes aware of inappropriate use of the Services." Shaw further reserves the right to take any responsive action, they deem appropriate." The policy goes on to state that customers "authorize Shaw to cooperate with law enforcement authorities in the investigation of suspected criminal violations."[158] Arguably Shaw's policy as set out may take disclosure to law enforcement outside of the s. 7(3) exception for disclosure without consent. A customer by agreeing to this policy may be seen as giving consent to disclosure to law enforcement.

Like Shaw, Rogers reserves the right to take "any responsive actions that they "deem appropriate" when the Acceptable Use Policy has been violated. In the cases where there is not "express consent or disclosure is *required* pursuant to a legal power." [emphasis added] Rogers states that it may disclose information regarding its customers to law enforcement when there is reasonable grounds to believe that a customer has been involved in unlawful activities.[159] The specification that, in the absence of consent, the legal power by which disclosure is to be made actually requires disclosure may distinguish Roger's policy from that of COGECO in relation to how Rogers may exercise any discretionary authority allowed it by s. 7(3)(c.1). Neither side of the controversy concerning the interpretation of this provision nor either of the major telecommunications companies interviewed saw this provision as requiring an ISP to disclose information to law enforcement in the absence of a warrant, court order, or other statutory basis.

Rogers stipulation that it may disclose when there is reasonable grounds to believe that a customer has been involved in unlawful activities does not significantly broaden the ability of Rogers to disclose confidential information to law enforcement under s. 7(3)(c.1). It, at least, seems unlikely that a mere request for information by law enforcement is sufficient to satisfy the standard of their being reasonable grounds to believe in the occurrence of unlawful activities.

Bell Canada reserves the right "to disclose any information *necessary* to satisfy any laws, regulations or other governmental request."[160] [emphasis added] The necessity of

---

[157] *COGECO High Speed Internet Service Acceptable Use Policy*, available online at: COGECO http://www.cogeco.ca/files/pdf/legal/HSI_PUA_on_en.pdf (last accessed on January 31, 2008).
[158] *Acceptable Use Policy – Internet*, available online at: Shaw http://www.shaw.ca/en-ca/AboutShaw/TermsofUse/AcceptableUsePolicyInternet.htm (last accessed on January 31, 2008).
[159] *Acceptable Use Policy*, para 29, available online at: Rogers https://www.shoprogers.com/about/legaldisclaimer/Unified_AUP_Eng.pdf (last accessed on January 31, 2008).
[160] "Sympatico™ High Speed, High Speed Ultra, Basic and Basic Lite Internet Service," para 17, available online at: Bell http://service.sympatico.ca/index.cfm?method=content.view&category_id=550&content_id=921 (last accessed on January 31, 2008).

disclosure deserves to be emphasized as Bell Canada goes beyond the requirements of *PIPEDA* by stating in its Privacy Code that "Unless required by law, the Bell Companies shall not use or disclose, for any new purpose, personal information that has been collected without first identifying and documenting the new purpose and obtaining the consent of the customer or employee."[161] [emphasis added] This language gives the impression that Bell Canada will not divulge information in response to requests by government under s. 7(3)(c.1). However, a subsequent statement tempers this impression where the Privacy Code states "The Bell Companies may also collect, use or disclose personal information without knowledge or consent if seeking the consent of the individual might defeat the purpose of collecting the information such as in the investigation of a breach of an agreement or a contravention of a federal or provincial law."

Counsel for a large ISP interviewed by the author indicated that that company will exercise s. 7(3)(c.1)(ii) discretion exclusively in response to requests involving child pornography.[162] There is some indication that child pornography is viewed as a special case by the ISP industry more broadly, as will be elaborated below.

2) An Emerging Practice in Cases of Child Pornography

In fact, there is an emerging practice among some members of the industry of providing law enforcement with customer name and address in response to a letter identifying the investigating officer as well as his or her supervising officer in cases of child exploitation ("Letter of Request").[163] This subsection a) briefly describes the practice, b) contemplates the implications of *Re: S.C.* for this practice and c) characterizes the practice as straddling the line between formal and informal information sharing practices.

The ISP industry, in conjunction with law enforcement, the Office of the Privacy Commissioner and Justice Canada is working toward making the Letter of Request a standard practice in child pornography investigations. If given an IP address in a Letter of Request , a participating ISP will provide law enforcement with a customer's name and address, considering the disclosure to fall under s. 7(3)(c.1)(ii).[164] One participating ISP interviewed cited the vulnerability of the victims, the gravity of the offence, and the importance of the information to the furtherance of the investigation as providing the rationale for distinguishing child exploitation from other crimes.[165] Some ISPs still require a warrant since neither the courts nor the OPC have issued any findings lending direct legitimacy to the Letter of Request. [166] In the course of the PIPEDA review, the government accepted the recommendation of the Standing Committee on Access to

---

[161] See *Bell Code of Fair Information Practices,* at clause 2.3, available online at: Bell http://www.bell.ca/web/common/en/all_regions/pdfs/bcfip.pdf (last accessed on January 31, 2008).
[162] Interview conducted by email by the author with Senior Counsel in charge of privacy at a large Canadian ISP. Written replies to questions received on September 7, 2007. Hereinafter referred to as "Interview 2".
[163] Interview 1, supra note 144.
[164] Interview 3, supra note 117.
[165] Interview 2, supra note 162.
[166] Interview 1, supra note 144.

Information, Privacy and Ethics that the definition of "lawful authority" in section 7(3)(c.1) needed to be clarified.[167] But at present, the practice of accepting a Letter of Request as grounds for disclosing customer name and address information is entirely a matter of the comfort level of each individual ISP, in the absence of more concrete official guidance.

The recent case *Re: S.C.* may give hesitant ISPs further reason to pause. This case, apparently the only case so far to interpret s. 7(3)(c.1)(ii), involved this emerging practice of ISPs. In response to a written request for subscriber information for the purpose of a child exploitation investigation, Bell Canada provided the police with subscriber name and address corresponding to an IP address.[168] The Justice of the Peace found that "Bell Canada did not have a basis upon which to disclose the information" and so denied the search warrant being requested on the grounds that the underlying evidence was not lawfully obtained.[169] Subject to the aforementioned reservations concerning the precedential value of this case mentioned in the general introduction to this report at page 16-17, *Re: S.C.* cast some doubt on the utility of this disclosure arrangement. The admissibility of evidence obtained via voluntary disclosure by private entities under current data protection law remains unclear.

This emerging practice of the telecommunications industry for child exploitation straddles the line between formal and informal information sharing. The practice is not surreptitious and has been adopted and acknowledged by at least two of the major telecommunications companies and the leading industry organization, CAIP, played a key role in the development of the practice. Furthermore, telecommunication companies perform this role pursuant to what is most likely the correct interpretation of a statutory provision. The practice has been tailored to such an extent that it limits the types of information to be disclosed to those to which a relatively low privacy interest likely inheres. However, it is informal in the sense that it is based on a broad consensus of private entities as opposed to the demonstrated will of the legislature or the judgement of an impartial judge.[170] Official guidance on this issue is therefore recommended.

E) Gaps and Controversies

There are several gaps and controversies pertaining to information sharing practices as between Telecommunications Service Providers and law enforcement and national security agencies. The primary piece of privacy legislation governing the handling of information by the private sector due to the phrasing of key provisions as well as the lack of judicial pronouncements frustrates a clear understanding of the law in this area. The

---

[167] Industry Canada, "Government Response to the Fourth Report of the Standing Committee on Access to Information Privacy and Ethics", available online at http://www.ic.gc.ca/epic/site/ic1.nsf/en/00317e.html (last accessed on March 12, 2008). See response to Recommendation 12.
[168] *Re: S.C.*, 2006 ABQB 709 at paras. 3-4.
[169] *Ibid*. at para. 10.
[170] Another significant aspect of the informal practices are informal relationships between the individuals at the ISP and law enforcement. Small ISPs have good working relationships with local law enforcement and tend to demand less formality from a local police force than they would from a provincial force or the RCMP. Interview 1, supra note 144.

dearth of authoritative judicial pronouncements on the issue of reasonable expectation of privacy for relatively new forms of communication as well as the highly contextual nature of such enquiry renders the constitutionality of various practices somewhat unclear. There is, furthermore, some question about where exactly Internet monitoring lies in the statutory framework governing police investigations. Largely due to the legal uncertainty, there is an information sharing context that is subject to criticism as well as a law reform agenda that is no less controversial. The following will consider 1) the foregoing sources of legal uncertainty and 2) the controversy attending proposed law reform.

1) Legal Uncertainty

There are particular areas of uncertainty within the legal regime. Among these are a) those that stem from the two statutory regimes regulating privacy for telecommunications organizations, b) the dearth of authoritative constitutional pronouncement on the reasonable expectation of privacy that particular telecommunications attract and c) the uncertainty regarding which legal regime covers computer monitoring.

The legal regime is complicated by the presence of a regulatory body that potentially has the ability to assume greater jurisdiction in the area of privacy but has largely refrained from doing so in the emerging and controversial area of Internet communications. Further uncertainty stems not only from the fact that *PIPEDA* is overseen by an ombudsman style commission, the decisions of which are not binding on the court but also from the fact that many of its provisions have yet to benefit from authoritative judicial treatment. Section 7(3)(c.1) is notable in this sense as it is one of the key provisions in terms of disclosure to law enforcement and national security agencies by private entities, assumes the peculiar form of saying that organizations "may" disclose under particular circumstances. As mentioned above, this provision has resulted in varying responses from members of the telecommunications industry. There has been neither a formal decision from the Office of the Privacy Commissioner nor an authoritative decision from the court in regards to its interpretation. The meaning of the terms "government institution" and "lawful authority" pose further interpretive challenges.[171]

The authority of the constitutional jurisprudence on the subject matter results in further uncertainty. Though *Weir* has rather more precedential value than *Re. S.C*, it cannot be seen as settling the contentious issues of under what circumstances an ISP will be acting as an agent of the state and an individual's reasonable expectation of privacy in their e-mail. *Weir* dealt with contraband as opposed to mere evidence.[172] It may or may not be significant that this particular contraband was child pornography. Further, *Weir* was a decision of the Alberta Court of Appeal and it is not apparent that its reasoning has been

---

[171] *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, available online at: http://cmte.parl.gc.ca/Content/HOC/committee/391/ethi/reports/rp2891060/ethirp04/05-rep-e.htm#part17 (last accessed on January 31, 2008).

[172] Stanley A. Cohen, *Privacy, Crime and Terror*, supra note 75 at 519.

adopted even in other Canadian jurisdictions. Significantly, the *Lawful Access – Consultation Document*, did not treat the question of whether e-mail could attract a reasonable expectation of privacy as settled.[173]

There are further unsettled questions of law pertaining to which of the existing legal regimes, if any, best covers computer monitoring. In addition to the conventional *Criminal Code* provisions for search and seizure, there is the possibility that the subject matter falls under the electronic surveillance regime of Part VI of the *Criminal Code*.[174] For the purpose of Part VI of the *Criminal Code*, which makes it an offence to intercept private communications, defines a private communication as "any oral communication or any telecommunication, that is made by an originator who is in Canada or is intended by the originator to be received by a person who is in Canada and that is made under circumstances in which it is reasonable for the originator to expect that it will not be intercepted."[175] In other words, a private communication for the purpose of the offence is any oral communication or telecommunication that attracts a reasonable expectation of privacy.[176] Interestingly, the *Lawful Access - Consultation Document* made much of the fact that e-mail is a written as opposed to an oral communication in questioning the applicability of Part VI without considering whether e-mail could be deemed a telecommunication.[177] Even if, e-mail and other Internet communications fall under the definition of a telecommunication, the inherent lack of security attending these sorts of communications continues to cast doubt on whether they attract the requisite reasonable expectation of privacy for them to be considered private communications.[178]

These chasms at law play a part in an information sharing landscape that some argue is not altogether appropriate. For instance, quite apart from the question of whether telecommunications companies have the discretionary authority to disclose information to law enforcement and national security agencies in response to requests is the question of whether it is appropriate for them to have this sort of gatekeeping function.[179] It is not self-evident that telecommunications companies are the appropriate bodies to adjudicate between the privacy interests of individuals and the state's legitimate interests in law enforcement and national security.

2) The Controversy of the Law Reform Agenda

There is clearly a sense among many governments that the existing legal mechanisms shaping the sharing of information between telecommunications companies and law enforcement are insufficient to serve the state's interest in monitoring Internet

---

[173] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 15, available online at: Department of Justice Canada < http://www.justice.gc.ca/en/cons/la_al/law_access.pdf > (last accessed on January 31, 2008).
[174] Stanley A. Cohen, *Privacy, Crime and Terror*, supra note 75 at 490.
[175] *Criminal Code, R.S.C. 1985, c. C-46*, s. 183.
[176] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 15.
[177] *Ibid.*
[178] Stanley A. Cohen, *Privacy, Crime and Terror*, supra note 75 at 491.
[179] *Ibid*, at 483.

communications. Such a perception is evidenced by resolutions, conventions and treaties from such organizations as the G8, The United Nations, and the Council of Europe.[180] Notable among these is the Council of Europe's *Convention on Cybercrime*. The Lawful Access Consultation reflects this concern at the national level. General as well as Specific Production orders, preservation orders, orders to obtain subscriber or service provider information are controversial proposed amendments to the *Criminal Code* that are discussed in the Consultation.[181] As the *Modernization of Investigative Techniques Act*, initially Bill C-74 - which attempted to give effect to some of the proposals pertaining to subscriber data and intercept capability- has been retabled as Bill C-416 in March 2007, the interest of law enforcement in law reform persists.[182]

However, many of the reforms for which law enforcement advocates are themselves controversial. The question of who will bear the additional costs of the proposed reforms is a source of concern from the industry's perspective.[183] Privacy advocates and the Office of the Privacy Commissioner are on record as endorsing the sufficiency of the current law for investigatory purposes.[184] One of the major telecommunications companies interviewed expressed the belief that the present regime provided adequate access to information while protecting the privacy of individuals.[185] Then there is the matter of the in roads that some of the proposed reforms would inevitably make into the protection of privacy and the resultant constitutional implications.

To the extent that the proposed law reforms would alter the interaction of telecommunications companies with their clientele, many of the changes contemplated in the Lawful Access Consultation threaten to enlist telecommunications companies as agents of the state meaning that they would be subject to *Charter* scrutiny. Considering that some of the reforms would entail disclosure of information in the absence of judicial authorization and that there may be a reasonable expectation of privacy attending some of the communications, there would seem to be a likelihood of some friction in a regime where warrantless searches are presumptively unreasonable and police would have the ability to compel personal information without a warrant.

---

[180] *Ibid*, at 488.
[181] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 5, available online at: http://www.justice.gc.ca/en/cons/la_al/law_access.pdf (last accessed on January 31, 2008).
[182] "Lawful Access: Police Surveillance" Canadian Internet Policy and Public Interest Clinic (2 June 2007), available online at: Canadian Internet Policy and Public Interest Clinic, http://www.cippic.ca/en/projects-cases/lawful-access/ (last accessed on January 31, 2008).
[183] Department of Justice, Industry Canada & Solicitor General Canada, *Lawful Access – Consultation Document*, (25 August 2002) at 7.
[184] *Response to the Government of Canada's "Lawful Access" Consultation: Submission of the Office of the Privacy Commissioner of Canada to the Minister of Justice and Attorney General of Canada* (5 May 2005) Privacy Commissioner of Canada http://www.privcom.gc.ca/information/pub/sub_la_050505_e.asp (last accessed on January 31, 2008). See also "Lawful Access: Police Surveillance", supra note 182.
[185] Interview 3, supra note 117.

F) Conclusions and Recommendations

1) Recommendations

Recommendation 1: Clarification should be given to the discretionary authority of private entities under s. 7(3) of *PIPEDA*.

The problems posed by s. 7(3)(c.1) of *PIPEDA* were principle among the gaps and controversies described above. Both the state and individuals have important interests at stake with respect to disclosure under this provision, and consideration should be given as to whether Telecommunications companies are the appropriate entities to balance these interests.[186] Telecommunications companies themselves have requested clarification of the provision in order to protect themselves against liability to customers which may result from disclosing information to law enforcement or national security agencies.

Recommendation 2: s. 7(3)(c.1) should remain discretionary, and not be amended to make disclosure to law enforcement mandatory.

The extent of the discretionary authority of private entities to disclose customer information to law enforcement and national security authorities should be clarified, and the Privacy Commissioner should issue guidelines for judging when that discretion should be exercised. Although amending s. 7(3) by replacing the word "may" with "shall" might clarify the course of action for telecommunications companies when faced with requests for information, the authors of this report are not prepared to take the position that s. 7(3)(c.1) should be amended to make s. 7(3)(c.1) mandatory.[187] Considering the uncertainty concerning the reasonable expectation of privacy in Internet communications, such an amendment would have unclear constitutional implications for information requested from the telecommunications industry. The distinction that the justice in *Re: S.C.* drew between the authority to disclose information and the authority to obtain it[188] is less problematic. If this distinction set out in *Re S.C.* holds, the existence of a mandatory provision obliging private entities to disclose information would raise constitutional implications requiring a determination of whether customers had a reasonable expectation of privacy in customer name and address data.

Amendment to make disclosure under this provision mandatory may be particularly

---

[186] Not everyone finds the discretion vested in the organization to be problematic. Interviewee 3 thought that the current privacy law appropriately balanced the interests of law enforcement and the individual. Interview 3, supra note 117. The Office of the Privacy Commissioner expressed a similar view, stating that the "the discretion whether or not to disclose should be left with the organization." See also "Letter to the Ministry of Industry regarding the 5 year statutory review of the Personal Information Protection and Electronic Documents Act (*PIPEDA*)," (13 July 2007), available online at: http://www.privcom.gc.ca/parl/2007/let_070713_e.asp (last accessed on January 31, 2008).

[187] That s. 7(3) should be made a mandatory provision is a recommendation of the Standing Committee on Access to Information, Privacy and Ethics. The President of CAIP (Canadian Association of Internet Providers) also favoured such a course of action. *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, supra note 171.

[188] *Re: S.C.*, 2006 ABQB 709 at para. 9.

problematic to privacy interests in light of s.7(1)(e)(i) of *PIPEDA* which allows the collection of information for the purposes of national security, the defence of Canada, and the conduct of International affairs.[189] Although the heightened state interests and the likelihood of exigent circumstances in these contexts may make the warrantless searches constitutionally permissible in some cases, it seems likely that the ability of private entities to collect information for the purposes of mandatory disclosure threaten to bring private entities into an agency relationship with the state more frequently.

Recommendation 3: Consideration should be given to allowing police to request information in the absence of a warrant pursuant to tailored legislative provisions, namely only if the crime being investigated is of a serious nature, the crime is of such a nature that inability of the state to access the information will foreclose the investigation and the information is of a sort for which the privacy interest of the individual is relatively low.

Considerations that may be relevant to determining the circumstances under which it may be appropriate for police to have the ability to compel information in the absence of a warrant are the nature of the privacy interest, the vulnerability of victims, and the extent to which non-disclosure impedes police in investigation of particular types of crime. The last consideration may be particularly relevant to some forms of cybercrime where it has been argued that non-disclosure by Internet Service Providers would foreclose investigations at their earliest stages.[190] However, judicial authorization for search and seizure is an important norm of criminal justice and any deviations from this instrument of privacy protection should be in the form of limited and highly tailored legislative provisions.

2) Conclusion

As the above recommendations suggest among the key factors complicating information sharing in this context are the implications of a less than clear law, notable among which is s. 7(3) of *PIPEDA*, and a dearth of statutory provisions that would afford law enforcement the authority to obtain information in cases where it is truly required and not destructive of *Charter* protected rights. In light of these complications, the telecommunications industry has played a role in mediating between the crucially important interests of law enforcement and national security, on one hand, and the individual's right to privacy, on the other. However, this demonstrated responsiveness by the industry does not relieve the government of the important task before it of clarifying the law in a way that stabilizes this balance of interests.

---

[189] *PIPEDA*, at s. 7(3)(c.1)(i). The Standing Committee on Access to Information, Privacy and Ethics took an alternative route to avoiding this sort of agency relationship, by recommending that s. 7(3)(c.1) be made mandatory, but also suggested that s. 7(1)(e)(i) be repealed. See *Fourth Report of the Standing Committee on Access to Information, Privacy and Ethics*, supra note 171. The government has decided not to accept this recommendation. Supra, note 183.

[190] Interview 2, supra note 162.

III. **Retail Industry**

Written by Tamir Israel

Introduction

Canadians enjoy comprehensive legislation safeguarding privacy rights of individuals as they interact with the retail sector. Canadian legislatures have ranked privacy as an important value that, while not being absolute, must nonetheless be guaranteed by law against private entities such as retailers. This guarantee takes the form of the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) and substantially similar Provincial Acts in British Columbia, Alberta and Quebec. Such Acts set out rights and obligations imposed on the relationship between customers and private organizations carrying out commercial activities and ensure that some level of privacy is respected in these interactions.

There are, however, gaps in such legislation that may well allow national security and law enforcement interests to overrun privacy rights given the heightened security concerns and rapidly developing technology that characterize our days. Advancing technology that will allow for greater capacity to collect and combine data as well as more incentives for retailers to do so may well tip this balance between individual and state by providing law enforcement and national security services with access to expansive and comprehensive collections of personal information on citizens with few direct restrictions on their use. Such potential uses would violate privacy in principle but not in law. In light of these anticipated changes in the landscape, current privacy protections will have to be enhanced to meet the challenge if the existing level of privacy is to be maintained.

In Canada, the data brokers that American law enforcement and intelligence services rely upon to provide them with a steady stream of individualized personal information on citizens are greatly limited in their ability to collect and resell personal information.[191] *PIPEDA* restricts private companies from using personal information for a purpose that has not been consented to and this prevents organizations of this sort from developing large aggregations of identifiable information specifically targeted to meet law enforcement and national security needs. There are, however, exemptions in *PIPEDA* that permit collection, use and disclosure of personal information by retailers without knowledge or consent of the individual in question if for purposes of law enforcement or national security. As such, *PIPEDA* effectively restricts the *creation* of large databases of personalized information for such interests to access, but does not block the actual access itself. This leaves a gap in the current legislative framework that can lead to a reduction in privacy protection that may be undesirable.

---

[191] Lawson, Philipa. *On the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations with Whom You Have No Relationship – A Report on the Canadian Data Brokerage Industry* (2006) at page 38, available online at: http://www.cippic.ca/en/news/documents/May1-06/DatabrokerReport.pdf (last accessed on January 31, 2008). The report finds that in Canada, there are few data brokers offering *individualized* personal information on Canadians.

There are a number of conditions under which this gap in the legislation may lead to an erosion of privacy rights. First, the impact of increasing security concerns may lead to legislation being passed similar to that enabling the Canadian Border Services Agency (CBSA) PAXIS airlines database. While the current framework allows individual organizations to decide if they would disclose personal customer information in aid of a public investigation, under a legislative regime similar to that governing the PAXIS database it would be required by law. In such circumstances, retailers would be conscripted to act in aid of law enforcement and national security interests. *PIPEDA* permits collaboration and some have viewed the current exemptions as a sign of support for collaboration between retailers and public organizations.[192] It is the permissive nature of the *PIPEDA* exemptions that creates this impression currently.[193]

Secondly, given technological developments, specifically with the increasing use of Radio Frequency Identification Devices (RFIDs) and greater sophistication in data aggregation and analysis, retailers will have greater incentive as well as capacity to aggregate personal information of consumers on a grander scale than before. This will provide public organizations with a potential source of information that is both legally accessible and, given the nature and scope of information available even to individual retailers, potentially extremely useful not only for investigations of suspected individuals but also in forward looking analyses aimed at uncovering future threats.[194] Information available to retailers from analysis of purchase histories of customers is especially useful in the latter type of data analysis, where predictions are made regarding the level of risk posed to the public by an individual in the future.

A final concern involves the quality of consent. Customers are not generally informed that the information they are disclosing to a retailer could ultimately become part of an investigation by public officials in a criminal or national security matter. A retail company's policies on this position – whether they are predisposed to disclose such information to public investigators or not, should be clearly stated in their privacy policies and this is not often the case. Though actual sharing occurs infrequently at this point, there should still be a legal requirement that customers be informed of this possible end point for their personal information.

The overall framework currently provided by *PIPEDA* is to create a regime that supports an expectation of privacy in an individual's purchase history. To collect, use or disclose such information for a legitimate secondary marketing purpose retailers must have the knowledge and informed, meaningful consent of the customer to whom that information

---

[192] Interviews were conducted by the author with the Privacy Officers of three major retail businesses operating in Canada (Hudson's Bay Company, HMV and UPS). The Interviews with Hudson's Bay Company ("Interview 1") and UPS ("Interview 2") were conducted in July 2007, and the interview with HMV ("Interview 3") was conducted in August 2007. All three put forward the fact that collaboration is legal under *PIPEDA* as justification for cooperating with law enforcement requests. A further interview was conducted by the author with a public liaison officer of the Vancouver Police Department in September, 2007.

[193] *PIPEDA* S.C. 2000, c. 5, Section 7.

[194] Scassa, Teresa, and Chiasson, Theodore, and Deturbide, Michael, and Uteck, Anne. *Consumer Privacy and Radio Frequency Identification Technology* (2005) 27 Ottawa L. Rev., 215 at para. 70.

is connected. In this way *PIPEDA* ensures that individuals maintain control over their own personal information when undergoing essential interactions in the retail world. However when dealing with law enforcement and national security organizations, there are no guarantees whatsoever. This gap in privacy legislation has little effect at this time, but this is mostly due to a lack of requests made by public investigators. This situation could easily change and privacy would then erode, not by any legislative decision, but by default.

Enquiry into the information sharing between retailers and law enforcement and national security agencies reveals A) the potential that *PIPEDA* (as the primary legislation in the area) is inadequate to respond to potentially emerging threats to the privacy interests of consumers; and B) the impact of *PIPEDA* in limiting information collection by Canadian retailers as compared with those in the United States; as well as the likelihood that technological advancement will, nonetheless, lead to increased information collection in the future notwithstanding the legislation. It furthermore establishes that C) investigation into fraudulent activity is currently the primary reason for police requests and that there is a risk that information sharing that is more intrusive of privacy will become increasingly prevalent; D) informal information sharing is the norm in the industry; and E) gaps in privacy protection and privacy-related controversies for retailers result from the potential use of personal information to identify future threats and the likely inability of the current legislative scheme to deal with such developments.

A) Overview of Industry and How it is Regulated

Analysis of how the retail industry is regulated shows that 1) *PIPEDA* is the primary legislation governing information sharing between retailers and law enforcement; 2) *PIPEDA* is permissive towards information sharing between retailers and law enforcement subject to the unclear implications of *Re: S.C.*; 3) there is a tendency amongst many retailers to comply with police requests; and 4) that potential issues that may arise through a) the use of databases and b) the development of technology.

The primary legislation governing retail industry information sharing with public investigators is *PIPEDA* with the exception of a few provinces which have their own substantially similar legislative frameworks regulating private industry.[195] With respect to the issue of information sharing between retailers and law enforcement or national security organizations, there is no essential difference between the provincial Acts and *PIPEDA* as noted above.[196] In addition, there are established guidelines of market self-regulation such as the Canadian Marketing Association Privacy Code and the principles set out by the Canadian Standards Association. Such regimes do not substantially extend the reach of the current legislation and focus more on compliance guidelines. Particularly

[195] See the introductory section of the document for an overview of the relevant provincial Acts.
[196] See ss. 14(d), 17(d) and 20(f) of the Alberta PIPA and ss. 15(c), 18(c) and 21(i), (j) of the BC PIPA. Also see exemptions under ss. 57, 59 and especially s. 65 of the Quebec Act. The effect of these statutes is substantially the same (available online at: http://www.privcom.gc.ca/fs-fi/02_05_d_26_e.asp, last accessed on January 31, 2008).

in the case of public security information sharing, these self-regulations depart little from the legislative mold.

PIPEDA is permissive with respect to information sharing between retailers and public organizations. Retailers may unilaterally collect information if knowledge and consent by the individual would reasonably compromise the availability or accuracy of that information and if collection is reasonable for purposes relating to an investigation of the contravention of a Canadian or provincial law.[197] Perhaps of greater significance, retailers are permitted to disclose information they have already collected to a public investigative body upon request or even on their own initiative if they believe on reasonable grounds that this information relates to the contravention of a law or if they suspect that it relates to national security purposes.[198] Such disclosure need not be with the knowledge or consent of the individual in question.

A recent lower court decision, *Re. S.C.*, appears to limit the options open to a retailer when confronted with a request for information from public investigators. It holds that in order to supply the "lawful authority" required by *PIPEDA* to justify disclosure by retailers without the knowledge and consent of the customer in question, more is needed than the mere fact that the requesting public investigators need the information for an ongoing investigation into the contravention of a law.[199] This case, which is discussed in greater length in the introductory section to this document, suggests that a retailer may only disclose information in response to a request from public investigators if such a request is accompanied by prior judicial authorization or some other form of explicit legal authorization such as a statutory provision or if the retailer decides based on reasonable grounds to disclose on their own initiative.[200] Despite the uncertainty cast on the legitimacy of such practices by *Re S.C.*, it would appear that the majority of retailers continue to respond to informal requests from public investigators. Effectively, it can be said that retailers possess discretion in deciding whether to respond to requests of this nature.

Some companies see it as their obligation as an ethical organization to assist the police in their investigations if requested to do so. Since such an approach is treated as neither prohibited nor required by the legislative framework, it is not possible for a customer to know as they are submitting personal information to a company whether the company is willing to disclose such information to a public investigatory body or not. The current legislation leaves consumers in the dark with respect to the possibility of having their personal information become part of a public investigation. In other contexts, *PIPEDA* nurtures an expectation that such knowledge would be provided to individuals so that they may maintain some level of control over their own personal information.

---

[197] *PIPEDA*, supra note 192, s. 7(1)(b).

[198] See Ibid s.7(3)(c.1) which extends permission to disclose beyond s.7(3)(c) (warrants and court orders) to cover requests from appropriate institutions as long as the purpose of the request is to enforce a Canadian, provincial or foreign law or investigate the contravention of such a law.

[199] *Re. S.C.* [2006] O.J. No. 3754.

[200] *PIPEDA* s.7(3)(d). In order to disclose under this section, a retailer must have reasonable grounds to believe a law has been contravened and the personal information in question is necessary to an investigation of that contravention.

While such practices may be reasonable with regards to a specific ongoing investigation into an individual, different issues are raised if public investigators take a more forward looking approach and collect personal information from private databases in an attempt to seek out potential future offenders. Such virtue testing based on, for example, past purchase preferences and other similar information may go beyond what s.5(3) of *PIPEDA* proscribes as appropriate under the circumstances, especially if conducted without knowledge or consent of the individual. This issue has yet to be officially tested, yet courts have in the past treated random fishing expeditions in the criminal context as being more invasive than concrete investigations into individuals suspected of specific crimes.[201]

Another key issue is how the regulatory and legislative framework will work with developing technology. Specifically, improved techniques in aggregating and storing information and Radio Frequency Identification Devices (RFIDs), which "have potential for widespread use in consumer products in Canada."[202] These will allow private retailers "to collect and compile data about individuals that is unprecedented in both volume and nature."[203] The effect of this increase in available information on consumers is difficult to predict and may affect a qualitative shift in the balance between privacy and security by making considerably greater amounts and types of information available.

While law enforcement requests from retailers are currently infrequent and case specific,[204] RFIDs have the ability to radically alter this landscape. While current retail databases contain minimal profiles in comparison to the detailed collections of information held by American data brokers, RFIDs will offer incentive to create more sophisticated and expansive profiles of customers by providing more uses for such profiles.

With RFIDs, a customer can potentially be identified from a distance as they enter a store through information read off of their loyalty card or credit card by portable readers spread throughout the store. This will instantly provide sales associates with a profile that is as detailed as the retailer can make it. Purchase preferences, income levels and whatever else can be gathered. Sales associates will have an added advantage with the ability to develop individualized sales strategies. They will have the capacity to conduct in person targeted marketing similar to what regularly occurs at online stores, where additional products are recommended to consumers based on purchase histories and other profile information. The value of such information will increase dramatically and so retailers will be more likely to collect larger more elaborate databases.

---

[201] *R. v. Mellenthin*, [1992] 3 S.C.R.615.

[202] Office of the Privacy Commissioner of Canada, *Annual Report to Parliament 2005-2006: Report on the Privacy Act.* (2006), at page 21, available online at: http://www.privcom.gc.ca/information/ar/200506/200506_pa_e.pdf (last accessed on January 31, 2008).

[203] Scassa et al, supra note 199.

[204] The Hudson Bay Company receives such requests from law enforcement at a rate of less than one per year. Canadian Revenue Agency (CRA) requests relating to credit card fraud, while more frequent, still do not occur very often and also relate to specific identifiable individuals already suspected of wrongdoing. Interview 1. supra, note 191.

Once gathered, with consent and for a legitimate if secondary marketing purpose from which consumers generally do not withhold consent, it is open to law enforcement to request this information. Expanded databases of this type lend themselves to more than ad hoc case by case investigations and could be compiled to create more elaborate predictive initiatives such as the FBI's System To Assess Risk (STAR) program where database information is used to assess the potential risk that an individual is involved with terrorist activities.[205] Such inferential systems involve high risks of error but can nonetheless lead to serious consequences for individuals.

The current legislative and regulatory framework does little to prevent this type of information sharing. It will also be left to individual retailers to decide whether to provide such information to law enforcement officials on an ongoing basis or not if such requests are made in the future. Information that public investigators would otherwise have great difficulty collecting will be supplied to them by unsuspecting private citizens at the discretion of retailers collecting information for their own professed legitimate marketing purposes.

All this will be exacerbated by increased capacities for aggregating and analyzing data. The overall impact could well tip the equilibrium between law enforcement and individual interests that currently holds sway as privacy interests are eroded by these new more elaborate collections of personal information. The current legislation and regulations strike that balance at a certain point, however they do little to guard against such changes. It is possible that if they come to pass, the purpose of the legislation may be frustrated.

B) Information Collected by the Industry

Analysis of the nature of information collection by Canadian retailers reveals information collection practices that are significantly different from those in the United State. It appears that 1) *PIPEDA* has impacted information collection by retailers in Canada particularly with respect to the use of data brokers and 2) there is a possibility that technological advancements will increase information collection by retailers which may, in turn, further excite the interest of investigators in the information held by retail businesses.

Given the range of information dealt with by retailers as an industry – sensitive information touching closely on many aspects of private life, the limited degree of data collection that occurs in Canada may be surprising especially when compared with practices south of the border. Part of this restricted activity is an effect of the limited availability of individualized personal information from data broker sources due to requirements under *PIPEDA* that restrict uses of personal information to those purposes which are explicitly consented to by the consumer to whom that information relates. See the discussion in the introductory section to the document for more details.

---

[205] Jordan, Lara Jakes. *Data on Americans Mined for Terror Risk.* Associated Press (July 10, 2007).

The Federal Court and the Privacy Commissioner of Canada have both held that supplying personal information to data brokers properly requires consent and knowledge of the individual consumer.[206] A customer's purchase history and many of the other details bought and re-sold by American data brokers fall under this category. Retailers would find it difficult to share such information without alienating some customers by requiring them to agree to the selling of their personal information for purposes beyond the company's own marketing. It would remain the responsibility of retailers to secure consent for all uses a data broker would make of a customer's personal information.[207] It would be difficult for a retailer to incorporate such information into their privacy policies and, moreover, while many customers may find information sharing for a company's own marketing purposes reasonable, this may not extend to the outright selling of a customer's personal information for pure profit. While outright selling of personal information to data brokers may occur at times, especially with less sensitive material such as name, address and telephone number, the need for informed consent ensures such cases remain rare.

Canadian marketing firms that aggregate data do not generally purchase personal information. Instead, a retailer gives them access to personal information under strict contractual terms protecting the privacy of the individuals in question and this information is then analyzed and aggregated with demographical statistics, with publicly available information, with other information packaged in anonymous form and with personal information of other consumers of the same retailer.[208] This can include, for example, average neighbourhood income levels or purchase preferences of those who have bought similar products from the same retailer. In this way, comprehensive customer profiles are developed that allow retailers to utilize the personal information they have gathered without breaching the requirements of *PIPEDA* and without alienating customers.[209]

Conversations with representatives of major retail chains in Canada have shown that they do collect personal identifying information such as name, address, age, and so on. They additionally collect a record of the purchase history of identifiable individual customers. These purchase histories may contain, depending on the nature of the retailer, extremely sensitive information such as travel arrangements, reading preferences or personal habits such as drinking and smoking.[210] A bank administering a credit card, for example, collects a record of all purchases conducted with that card as well as where and when

---

[206] *Lawson v. Accusearch*, [2007] F.C. 125 at para. 2. The practices of the defendant American Data Broker amounted to collection, use and disclosure of Canadian personal information that was "for inappropriate purposes and without the knowledge and consent of the individuals in question." Accusearch bought personal information from Canadian companies and sold it back to other Canadians in a packaged format. The Federal Court found that this contravened *PIPEDA*, as did the Privacy Commissioner of Canada, who refused to hear the case on other grounds (at para. 10).

[207] *PIPEDA* Case "Statistics Canada census taker not responsible for disclosing personal information to banks" 2002, http://www.privcom.gc.ca/cf-dc/pa/2002-03/pa_200203_07_e.asp (last accessed on January 31, 2008).

[208] Lawson supra note 190, at page 39.

[209] Ibid at page 38.

[210] For a comprehensive list of factors found to be included in such customer profiles, see the list in Lawson supra note 190 at page 27, reproduced in appendix 1 below.

such purchases took place.[211] Consent is obtained by the retailer to use this personal information for their own secondary marketing purposes.[212] The information is then submitted to a data broker under strict contractual privacy protections. The data broker analyzes the information, combines it with publicly available and general demographic information which is not considered 'personal' under *PIPEDA*,[213] and creates a more detailed aggregate profile that can be used for direct marketing campaigns.

This detailed profile is rarely, however, sold on the open market as is done in the United States, nor is it combined with sensitive personal information gained from other retailers. Canadian data brokers do not often sell individualized consumer information – most offer non-personal information alone, which is aggregated with the personal information provided by a specific retailer.[214] Then, each profile is provided for use by the contracting retailer and their corporate family alone. In this way, aggregate profiles are created but control over personal information is maintained to a substantial extent by the original retailer and its subsidiaries. These profiles are not at this point as detailed as those prepared by American data brokers who have access to large databases of individualized personal information from many retailers which they may add to demographic and publicly available information.

While the type of personal identifiable information collected by various retailers covers a broad range of information, individual retailers do not possess extensive customer profiles. To match the resources made available to American law enforcement and national security interests by data brokers such as ChoicePoint, public investigators would need to query a number of individual retailers and other sources and combine the results of such queries themselves. ChoicePoint offers diverse informational databases comprised of individualized personal information from many private organizations as well as publicly available information. ChoicePoint has built in powerful search tools to manage this information and public investigators can access detailed profiles on people by entering limited information such as a partial address or phone number.[215] Thus Canadian sources are far less rich and require more effort to get comparable levels of information, but the demand for such aggregated information is clear.

As technology advances and individual retailer databases become more sophisticated with more complex profiles there will be greater cause for law enforcement and national security interests to request personal information from retailers. In this way, through a

---

[211] *PIPEDA* Case Summary #296 (March 2005).

[212] Lawson, supra note 190 at page 41. This consent is usually collected through a statement of purpose in a retailer's privacy policy. See for example the online privacy policy statement of Indigo, available online at: http://www.chapters.indigo.ca/Privacy-Policy/priv-art.html (last accessed on January 31, 2008)

> The [personal] information [collected by Indigo] also enables Indigo to customize products or services to better meet your preferences and to offer you products and services from Indigo and other sources that may be of interest to you.

[213] Lawson, supra note 190 at page 39.

[214] Ibid at page 41.

[215] Hoofnagle, Chris Jay. *Big Brother's Little Helpers: How ChoicePoint and Other Commercial Data Brokers Collect and Package Your Data for Law Enforcement*. [2004] 29 N.C.J. Int'l L. & Com. Reg., 595 at page 602.

mere increase in the availability of information, the balance between privacy and security that is currently maintained may become unbalanced.

We have seen that RFID technology may lead to larger and more elaborate databases of personal information collected by retailers. In addition to this, the technological developments will likely lead to a greater variety of information being collected by retailers. This is because of the increased value and capacity to gather such information. Retailers will be able to collect information on consumers even before the point of sale, as they browse through the store itself, for example. Parallel developments in data aggregation technology will allow greater inferences to be drawn from the same amount of data that was previously collected. This will leave retailers with considerably more evolved databases of customer profiles that will contain a much more diverse amount of information. While many retailers currently make use of data brokers to aggregate the personal information they collect with non-personal information that is publicly available to all, such practices are limited and not pursued to the extent possible. Once such information becomes more useful to retailers, they can be expected to pursue such sources more rigorously and improved aggregation techniques will allow for more elaborate profiles to be produced even as retailers seek them out.

These more complete profiles will offer greater advantages to public investigators by providing increased breadth of information, making it more likely for them to find access to information of this sort a useful investigatory tool. The information is also likely to be more accessible and organized for faster retrieval. Given the more immediate uses retailers will be making of customer profiles – uses that require quick access at the store as the customer walks in - it is likely that the profiles will be organized in user friendly ways that enhance speed of access. Searchable databases would make police queries far simpler and this searchable quality has been named one of the key advantages that American data brokers offer public investigators.[216]

The bottom line is that not only will more information be available encouraging public investigators to make requests. There will also be greater variety of information available and this will be more conducive to broader investigations – ones not relating to verification of specific details regarding a particular suspect, but to general background information on suspected potential threats. The easy availability on a large scale of this type of information seems likely to encourage, as it does in the U.S., practices of virtue testing and fishing expeditions to assess through inferences how great of a potential threat an individual suspect may turn out to be. This latter kind of investigation is one that is problematic and invasive of privacy concerns.

C) Personal Information of Interest to Law Enforcement and Legal Mechanisms Shaping Information Sharing

Retailers handle on a daily basis a wealth of information that is of potential use to public officials carrying out law enforcement or national security investigations. One need only look to the degree to which data broker services available to American public

[216] Ibid.

investigators are used to see how useful such a resource can be.[217] This section considers 1) the varying roles that information held by retailers may play in investigations, 2) the emergence of investigation into fraudulent activity as the dominant reason for police requests for personal information, and 3) the risk of use of information by law enforcement in a manner that is more intrusive of privacy interests than the current norm.

There are different levels of use that public investigators may make of personal information. Retailers and service providers such as credit card companies or travel agencies can supply personal information aimed at specific findings as part of a narrow investigation into a particular individual. The need for such information will arise only infrequently as the course of an investigation intersects directly with retailer activity. This type of information request will often relate directly with investigations into fraudulent activity suffered by the retailer, who is often the initiator of the investigation.

Another level of use potentially made by public investigators will be more general and closer to virtue testing where investigators have no concrete reason to suspect an individual but rely on inferences and statistics to show that an individual is likely to be involved in an offence or in terrorist activity in the future. Information collected from retailers would be especially useful for this latter level of use. Reading preferences can be matched with suspicious travel itineraries acquired through credit card purchase histories to mark an individual as 'suspect'. A designation of this sort would lead to closer investigation and perhaps to more serious consequences.

In Canada, it is mostly the first of these different levels of information use that is utilized by public investigators. Interviewed retailers report that the predominant number of information requests they receive from public investigators relate to fraudulent activity by a customer or an employee and it is often the retailer or service provider itself that is the victim of the crime. Assuming that the information is submitted to a court of law and is not merely used in the preliminary stages of an investigation, the issue with this level of information use becomes whether a warrant is required for public investigators to gather the personal information in the first place. The *PIPEDA* exemption that allows retailers and service providers to disclose information to public investigators, s. 7(3)(c.1), extends this exemption beyond s. 7(3)(c), which covers compliance with warrants and court orders, to include mere "request[s] for information".[218] It seems that it is envisioned that there is room for information sharing without a warrant.

However, in light of Conacher, J.P.'s judgment in *Re. S.C.*, there may be less discretion left for cooperation with informal requests given that a public investigation is held to be insufficient to meet the requirement for "lawful authority" under s. 7(3)(c.1) in that case. For a more detailed discussion of the matter see the introduction to the document. American courts have held that information, once disclosed to a private organization such

[217] Ibid, at page 600. For example, the United States Marshal Services (USMS) accessed databases held by data brokers to conduct electronic searches an average of 20,000 times per month in the late 1990s and the frequency of queries has only increased since.

[218] *PIPEDA*, supra note 192. See s. 7(3)(d) as well, which allows private organizations to disclose personal information on their own initiative under certain circumstances.

as a retailer, no longer holds a reasonable expectation of privacy and so such information is not covered by the Fourth Amendment.[219] The Canadian position appears to be different and to uphold such expectations when dealing with personal information, even if disclosed to retailers. For more details see the discussion of s. 8 principles in the introductory section. Additionally, retailers responding to a request for information may be labeled agents of the state in which case a court will apply the *Charter* to their actions in assessing whether their evidence is admissible or not.[220]

With the type of personal information processed by retailers, there is the risk that public investigators will undertake another level of use with what they acquire. As mentioned above, this level of use would involve virtue testing of individuals where no concrete grounds exist to suspect any wrongdoing. Instead, this form of analysis is used to focus investigatory techniques on a number of individuals that are more likely to turn out to be terrorists or criminals. Such uses of personal information impact more heavily on privacy concerns and should be adopted in Canada only with careful consideration.

In the U.S., retail information from data brokers is used in this way to facilitate virtue testing techniques of this type.[221] The STAR program is an example of one such use. Those implicated by this program are not labeled as terrorists, but they are assessed as higher risk individuals who will be watched more closely.[222] It is likely that Canadian public investigators would find this level of usage of personal information attained from retailers equally as useful if they developed a similar framework for exploiting such a resource. This would involve collection of a broader range of information from retailers than is currently made use of by most Canadian public investigators. Reading preferences, for example, will be less relevant to most fraud investigations but can be of use in deciding the probability that a given individual may become a terrorist.

As mentioned above, American case law has held that acquiring the type of information necessary for this form of analysis from retailers does not infringe a reasonable expectation of privacy and so is not offensive to the Fourth Amendment.[223] It has also been noted that in the U.S. there is no legislative privacy regime which governs disclosures by private companies such as retailers to public investigators.[224] In Canada, the handling of customer personal information by private industry is regulated and we have seen that one effect of this regulation is to limit the development of large aggregations of individualized personal information under the control of data brokers. While this may limit the capacity of public investigators to develop programs such as the

---

[219] Hoofnagle, supra note 214 at page 620: information provided to others doesn't raise a reasonable expectation of privacy: *United States v. Miller*, (1976) 425 U.S.435, 442.
[220] See the discussion of *R. v. Weir* in the Telecommunications section of this document for more details on the effect of the agency of a private organization.
[221] Jordan, supra note 204.
[222] Ibid.
[223] Hoofnagle, supra note 214 at page 621.
[224] The American *Privacy Act* only relates to government activity. See Dempsy, James and Flint, Lara. *Privacy's Gap: The Largely Non-Existent Legal Framework for Government Mining of Commercial Data* (2003) Ctr. for Deomocracy & Tech., available online at: http://www.cdt.org/security/usapatriot/030528cdt.pdf, at page 4 (last accessed on February 7, 2008).

FBI's STAR, it does not rule it out altogether especially if personal information becomes more available as larger information aggregates are created by individual retailers and service providers. While the *Charter* may protect against this form of usage, it is likely that the type of personal information collected from retailers for programs of this sort will come early in the investigative process and may never be used in a court hearing, and so not be subjected to *Charter* scrutiny.

Such purchase history information is considered to be personal and sensitive in other contexts and is only exempted from legislative protection by the law enforcement or national security purposes which it serves. Information gathering of this sort may also avoid judicial scrutiny under the *Charter* and under rules of evidence because it occurs at so early a stage in the investigation. This means there may be little direct scrutiny of the issues involved and an erosion of privacy may take place without the analysis one would hope to see accompanying such an important value. The type of sensitive information possessed by retailers is potentially of great interest to public investigators. It is possible that while currently there is little information sharing, the near future will show an increase in requests for information of this form by public investigators.

D) Formal and Informal Information Sharing Practices

Informal information sharing appears to be the norm in this industry. A pronounced perception among many retailers of an ethical obligation to share information with law enforcement appears to compensate for the lack of sector-specific formal information sharing procedures for the retail industry. This section will describe 1) the nature of informal information sharing and 2) the potential form that sector-specific formal procedures could take by reference to those that have been implemented by the airline industry.

The interviews conducted for this report reveal that most information sharing that occurs between retailers and enforcement agencies is generally on an informal, ad hoc basis. Individual investigators come upon information they need and make a request from the retailer in question. In general, the request would go either to a regional manager or to the privacy officer for a case-by-case assessment as to whether the request should be filled. Though it is at the discretion of each individual company whether to make such a disclosure or not, companies surveyed seem to consider it their ethical obligation to assist in an investigation to the extent they are legally permitted to do so. As we have seen, this legal standard allows for full disclosure under the law enforcement and national security exemptions.

Some companies, such as HMV and Hudson's Bay Company, have protocols for dealing with such requests as they occur. The request is made to a local manager, but it is their national privacy officer that assesses it and processes the response. This allows for case by case adjustments to be made to the general policy of cooperation as needed to ensure that customer's privacy rights are maintained if they are engaged more intensely in a particular situation. Other companies such as UPS have an overall policy of cooperation but leave case by case decisions to local managers. This latter approach is sufficient for

dealing with infrequent requests as they currently occur, but were requests to become more regular, it would become difficult to ensure that privacy concerns were upheld in all cases and the former approach would be preferable.

There are no formal information sharing procedures in place between law enforcement or national security concerns and private retailers at this time. However, if such practices were to develop they would likely take the form of the CBSA PAXIS airlines database, where private members of the airline industry are involved in collecting and providing information according to a set of criteria that are combined in a database used by the CBSA for certain immigration related concerns. The RCMP and CSIS have access to this database and use it in the course of their investigations to uncover information on travel arrangements of suspects. Similar information can be gained from credit card companies, travel agents, or other service providers and in the U.S. such travel information is often included among other purchase history preferences contained in databases of data brokers such as ChoicePoint and others.[225]

Legislation similar to s. 148(1)(d) of the *Immigration and Refugee Protection Act* (which establishes the PAXIS database requirements) could be passed in the context of the retail industry. Even without such a strong legislative mandate, if requests from public investigators become more frequent or if a database is developed by law enforcement officials similar to the Airlines Database – one that relies on retailers and service providers for some of its content - there will be nothing to stop individual companies from lawfully submitting personal information on a formal basis to such a database. While individual companies such as the Hudson's Bay Company take much care to protect the privacy of their customers, that such practices are permitted by *PIPEDA* suggests that information sharing with law enforcement or national security is not contrary to a privacy-focused approach. In this way, *PIPEDA* encourages organizations to share information with public investigators and many companies see it to be their responsibility to help such agencies carry out their duties as far as it is legally permitted.

E) Gaps and Controversies

The omnipresence of technological advancement and comparison with the United States reveals several controversial issues which arise from gaps in the current privacy matrix. The possibility of developments that threaten encroachment on the privacy interests of Canadians include 1) the potential use of personal information to identify future threats and 2) the likely inability of the current legislative scheme to deal with technological developments. Whether or not the resulting increased access that these factors are likely to afford police is desirable is a question ripe for policy debate. Another subset of gaps arises from there being no requirement that retailers to inform consumers that information collected may be used for investigatory purposes even though it is not always clear that lack of knowledge or consent by consumers is necessary to achieve investigatory objectives.

[225] *Ibid* at page 3.

The scope of information that retailers and service providers such as credit card companies and travel agents have under their control is broad and touches many aspects of our personal lives that are generally considered private and beyond the reach of the state. Much of this information is of potential use to law enforcement or national security agencies in their investigations not only of past crimes but also of future threats. Travel itineraries can be analyzed together with reading preferences and other available information, for example, to draw inferences about the potential risk an individual poses to national security. A result of this sort would not be certain enough for a court of law, but it would provide investigators with a basis for separating some higher risk Canadians from others. Similar to the FBI's STAR system, programs can be developed that take advantage of such information and technology. Advances of this type are beneficial to law enforcement and national security organizations, but would inevitably come at the cost of privacy.

Under the current legislative regime, such changes in the privacy landscape can occur without any analysis of the issues at hand. *PIPEDA* and the equivalent provincial legislation is permissive with regards to information sharing of this sort. This is not problematic at this point given that there is little direct interaction between retailers and public investigators unless there is a direct investigation of fraud or theft relating to the actual retailer or with a past employee. The problem lies in the fact that were law enforcement or national security interests to expand their use of databases and to rely on retailers to supply practices of this type, there is nothing to impede their doing so.

It may be that such a development is desirable from a policy perspective and that the accompanying diminishment of privacy rights would be worth the increased security and investigative effectiveness. This is, however, a debate that will be bypassed under the current privacy regime in that all investigative agencies need do to bring about this new world order is to ask. As matters stand, the retailers interviewed see it as their obligation to assist law enforcement and, moreover, the *PIPEDA* scheme appears to encourage such an attitude by allowing for an exemption in the area of law enforcement. There are no formal bars to this type of increased security activity. Any steps taken in this direction should at the least be more formalized and involve legislative activity (as with the CBSA PAXIS database) so their extent can be carefully delineated and not left to public investigators to decide for themselves. If, on the other hand, the current level of privacy is to be maintained in spite of increased technological advances, then the privacy legislation should be updated in anticipation of upcoming changes to the privacy landscape.

Whether there should be concern about not too distant developments in the realm of privacy or not, there is a legislative gap that should be addressed. Changes are certainly coming and though some may think such changes are welcome, they should be guided by legislatures and not developed ad hoc under the impetus of law enforcement and national security organizations. Privacy is an important Canadian value that ought to be safeguarded against undue infringement. The current regime allows for privacy to be diminished without the careful analysis and care that such an important right demands.

Another gap in the legislation involves the lack of any requirement to inform consumers that the personal information they are providing to a retailer may end up as part of a public investigation. Section 7(3) of *PIPEDA* allows disclosure of personal information to public investigators without the knowledge or the consent of the individual in question. The purpose of this section is to allow public investigators to access information they need without compromising their investigations.

It is possible, however, to make knowledge or even consent pre-requisites for information sharing of this sort without impacting on any ongoing investigation. If retailers were required to state their policy on such practices in their privacy policies, then consumers will be able to exert some measure of control over their personal information at least by foregoing the transaction with that particular company if they object to this practice. This will not include knowledge and consent over specific disclosures to public investigators, but will inform consumers in advance as to the general practices of a particular company.

Given that *PIPEDA* leaves it to the discretion of individual companies whether they will share information with public investigators, this is the only way in which consumers can become informed. Otherwise individuals are left to guess which retailers will or will not disclose their personal information if asked as part of a public investigation.

F) Conclusions and Recommendations

There are a number of privacy concerns raised by the practices of the retail industry that should be addressed. There should be general debate on a policy level to decide whether the potential erosion of privacy rights is acceptable. If security matters are found to justify an erosion of this sort, the matter should nonetheless be more carefully guided by legislation than it currently is. The legislation now merely leaves it to public investigators and individual retailers to decide where to strike the balance between security and privacy.

Recommendation 1: Customers should be informed that information they are disclosing to their local retailer may under certain circumstances be disclosed to public investigators.

At a minimum, customers should be informed that information they are disclosing to their local retailer may under certain circumstances be disclosed to public investigators. It is clear that in many cases it would be impossible to notify individual customers as their information is being disclosed because this could compromise an ongoing investigation. However, if customers were informed of a retail organization's policy on the matter ahead of time by the inclusion of this detail in the retailer's privacy policy, then the customer can make an informed purchasing decision.

Recommendation 2: The extent of permissible voluntary collaboration between retailers and public investigators should be clarified.

Stronger steps can be taken in the protection of privacy rights if the current level of individual privacy is to be maintained in spite of prospective changes that are likely to lead to an increase in information sharing between public investigators and retailers. There should be clarification of the extent to which collaboration between retailers and public investigators is permissible and desirable and under what circumstances this practice should take place. A balance can be struck that allows for a high level of information sharing and still maintains a level of privacy protection. Certain types of personal information such as reading preferences or hobbies can be placed out of bounds of the law enforcement and national security exemption. This will not effect investigations into individual cases of fraud or theft but may limit the capacity of public investigators to conduct fishing expeditions with no concrete evidential basis.

Recommendation 3: Mandatory collection and disclosure requirements should be avoided.

Legislation compelling retailers to contribute personal information of consumers to a database similar to the CBSA PAXIS database should be avoided. Currently, there is an equilibrium between security and safety on the one hand and privacy rights on the other but it is one that has developed by chance. There is no guarantee it will be maintained in the future, especially given the likelihood of future technological developments in the area.

IV. **BANKING INDUSTRY**

Written by Ali Mian

Introduction

The Canadian banking industry[226] is one of the most highly regulated industries in Canada. Analysis of this industry in the context of information sharing with law enforcement and national security agencies will begin with A) an overview describing the manner in which generally applicable statutes as well as those that are more specific to the focus of this report regulate the banking industry. It will proceed by showing in section B) that information collection by banks extends beyond that which is required by law and that there are both similarities and differences in the types of information that the various banks collect. Analysis of legal mechanisms governing the collection of information will consider privacy principles under *PIPEDA* in the banking context and identify issues that remain to be resolved. Section C) looks to FINTRAC as demonstrative of the types of information of interest to law enforcement and suggests that there are three main legal mechanisms shaping information sharing: s. 8 Charter jurisprudence, *PIPEDA*, and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA).* Section D) draws a distinction between formal and informal information sharing and discusses the process when met with a formal request for information as opposed to informal requests. Finally, E) the analysis considers gaps in privacy protection and privacy related controversies before F) making conclusions and recommendations.

A) Overview of Industry and How it is Regulated

The overview section briefly considers the network of statutes that regulate banks in the privacy and law enforcement contexts and explains the general applicability of (1) the *Bank Act* as well as the applicability of (2) the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)*[227] and (3) *PIPEDA*, the latter two of which are more specific to privacy concerns. Mention is also made of the regulatory agencies empowered by these statutes.

The banking industry falls under federal jurisdiction, so most of the laws and regulations which pertain to it are enacted at the federal level. At its core, the industry must adhere to the requirements in the *Bank Act*[228] and its regulations. The *Act* outlines the primary regulatory regime for banks in Canada. It highlights two specific regulatory agencies for the banking sector. The first agency highlighted is the Office of the Superintendent of Financial Institutions (OSFI). The OSFI supervises the banks to ensure they are solvent and it also assists banks in interpreting the *Bank Act* and its regulations. The second agency highlighted is the Financial Consumer Agency of Canada (FCAC). Both of these

---

[226] Throughout this paper, unless stated otherwise, the banking industry will refer to financial institutions that have as their core functions deposit-taking and money-lending. The focus will be on the activities of Canada's largest domestic chartered banks which are outlined in Schedule I of the *Bank Act.*

[227] *PCMLTFA* (2000, c. 17).

[228] *Bank Act* (S.C. 1991, c.46).

agencies deal with a bank's personal information on clients in a restricted way. Only if an agency is investigating a bank's compliance with the *Bank Act* or other applicable federal legislation will it come across a bank client's personal information. In the *Bank Act*, there are specific provisions to ensure that this information once acquired is kept confidential.[229] The information obtained under such an investigation can likely be handed over to law enforcement as it is in other types of investigations such as taxation. However, as discussed in Section 3 of this Part, clear rules have been established as to when and how such information can be transferred to law enforcement.

The banking sector is also regulated by the *PCMLTFA* and its regulations. The *Act* came into effect on June 12, 2002. It deals with how a bank must monitor financial transactions to ensure that the bank does not deal with proceeds of crime or assist with terrorist financing. Section 2 will outline the record keeping and client identification requirements that the *Act* and its regulations impose on banks. Finally, a bank's collection, use and disclosure of clients' personal information are regulated by *PIPEDA.* All "big five" banks, the five largest domestic banks,[230] have privacy policies or codes that resemble *PIPEDA*'s ten principles.

B) Information Collected by the Industry

1) Nature of Information Collected

The banking industry collects substantial and varied information from its clients. In the course of listing the various types of information that the banking industry collects, consideration will be given to a) information collection that is required by law; b) information collection that exceeds minimum legal requirements; and c) similarities and differences between the banks as to the types of information that each bank collects about its clients.

a) Required Collection

The banking industry is required by law to collect certain pieces of personal information on the clients it serves. As mentioned above, the *PCMLTFA* imposes specific requirements on what banks must collect. The collection requirements vary by type of banking activity and type of records. For the opening of a new bank account, a bank must record the name, address and occupation of all individuals who open the account, including signing officers on business accounts. The bank must also take reasonable steps to determine if the account will be used by or on behalf of someone who is not opening the account. When processing a transaction, the transfer or remittance of funds, over $3000 for one who does not have an account with the bank, the bank must record the name, address, date of birth, and the type of identification that was presented. For

[229] *Ibid.* at s.636 and s.658.
[230] The five largest domestic banks measured in total assets are Royal Bank of Canada (RBC), Toronto-Dominion (TD) Bank, Bank of Nova Scotia (BNS), Bank of Montreal (BMO), and Canadian Imperial Bank of Commerce (CIBC).

signature cards, transaction tickets, large cash transaction records and account operating agreements, the type of identification provided for these services must be recorded.

The types of identification banks may accept for identification purposes include a Canadian driver's licence, a valid Canadian passport, a Canadian birth certificate, a Social Insurance Number (SIN) card, a Certificate of Indian Status, a provincial health insurance card (except in Ontario, P.E.I. or Manitoba), a Certificate of Canadian Citizenship or Certification of Naturalization, a Permanent Resident card or a Citizenship and Immigration Canada form IMM 1000 or IMM 1442, an employee I.D. card with a photo from a known employer, a debit card or bank card with client's name and signature, a Canadian credit card with client's name and signature, a Canadian National Institute for the Blind (CNIB) client card with photo and signature, and a valid foreign passport.[231] The *Access to Basic Banking Services Regulations* under the *Bank Act* indicates that these forms of identification are permissible for the purpose of opening a personal bank account.

On June 23, 2008, the *PCMLTFA* regulations will introduce more record keeping requirements.[232] Since the *PCMLTFA* requires the reporting to government of such things as large transactions, suspicious activities and terrorist property, a bank must keep a record of the party names, date, time, amount, currency, and method of all transactions.[233] Another piece of legislation that requires the collection of personal information is the *Income Tax Act*.[234] Section 237 of the *Act* requires banks to obtain the SIN of clients who seek taxable products such as interest bearing bank accounts. Other legislation such as consumer reporting and securities legislation also impose requirements to record various forms of personal information. For example, the OSFI requires banks to record client's incomes when they apply for credit services.[235]

b) Collection Beyond Statutory Requirements

Banks can and do exceed these minimum record keeping requirements of their clients' personal information. If one looks at the publicly available privacy policies of the five largest domestic banks in Canada, one gets a better picture of the type of information which these banks collect. Banks offer numerous services and require varying forms of personal information depending on the service requested. Banking services include the following activities: opening a personal or business bank account, opening an online brokerage account, providing loans and mortgages, providing insurance, providing trust services, offering discount brokerage service or full-service brokerage, offering investment advice for products such as Registered Retirement Savings Plan (RRSPs) and Registered Education Savings Plan (RESPs), issuing a debit or credit card, and selling

---

[231] Available online at http://www.fcac-acfc.gc.ca/eng/consumers/rights/Accounts/RightsAccounts_1_e.asp (last accessed on February 7, 2008).
[232] For a summary of changes to the regulations affecting financial institutions see http://www.fintrac.gc.ca/re-ed/sc/fe-ef-eng.asp (last accessed on March 3, 2008).
[233] Proceeds of Crime (Money Laundering) and Terrorist Financing Regulations (*SOR*/2002-184).
[234] *Income Tax Act* 1985, c. 1 (5th Supp.).
[235] *PIPEDA* Case Summary #169, April 24, 2003.

investments like term deposits, Guaranteed Investment Certificates (GICs), and mutual funds.

Some banks will store a client's personal information into two separate types of databases: a general database and a service-specific database. Some information in the service-specific database, which stores personal information received during the provision of a particular banking service, will not be included in the general database, which can be accessed by any employee at the bank. [236] A general database contains more limited information on a client such as a list of all of his account numbers, balances in the accounts and the transaction history for the accounts.[237]

Banks also retain a history of credit card purchases for valid purposes such as the detection and prevention of crime and for monitoring credit use.[238] A greater discussion of the records banks keep on retail purchases is found in the part of this report on law enforcement activities in the retail industry. A review of the personal information collected by each of the five major banks, as outlined in their privacy policies, follows below.

c) Written Personal Information Collection Policies of the Major Banks

i) Similarities

The major banks collect a core of similar personal information on clients. In their written privacy policies, banks explicitly or impliedly indicate that they collect and maintain the following personal information on clients in the provision of products and services: the client's name, address, e-mail address, telephone number, SIN, birth date, employment, annual income, credit history, transaction history, health information, and identification.[239] Different pieces of personal information are collected for different products and services. As discussed above, for investment products, a client's SIN is required. For insurance products, the banks will collect health information. For loans and mortgages, the banks will seek a client's credit history from credit bureaus and reporting agencies and will include such information as employment history, current and past debts, bankruptcy history and any judgments and/or history of third-party collections. For all products and services, the banks reserve the right to collect personal information on clients that is publicly available. Most banks also reserve the right to record and retain the content of all client telephone discussions with its representatives. Similarly, most banks reserve the right to collect and retain information relating to the use of its online services,

---

[236] *PIPEDA* Case Summary #105, December 19, 2002.
[237] *PIPEDA* Case Summary #212, August 6, 2003.
[238] *PIPEDA* Case Summary #296, March 14, 2005.
[239] RBC Privacy Policy, available online at: http://www.rbcroyalbank.com/privacy/info_we_col.html (last accessed on February 7, 2008); TD Privacy Agreement, available on line at: http://www.td.com/privacy/agreement.jsp (last accesses on February 7, 2008); Scotiabank Privacy Agreement, available online at: http://www.scotiabank.com/cda/content/0,1608,CID8309_LIDen,00.html (last accessed on February 7, 2008); CIBC Privacy Policy, available online at: http://www.cibc.com/ca/legal/privacy-policy.html (last accessed on February 7, 2008); BMO Privacy Code, available online at: http://www4.bmo.com/popup/0,4442,35490_49258,00.html (last accessed on February 7, 2008).

namely the Internet Protocol (IP) address used by the client and the web pages he or she visits within the bank's website.

ii) Differences

There are some notable differences among the written privacy policies of the major banks. Some differences are genuine while others appear to exist only because a particular bank's policy is not as thorough as those of the other banks. The following discussion outlines unique features in each bank's written policy.

The Royal Bank of Canada (RBC) policy does not mention anything about reserving the right to record telephone conversations with clients. The policy mentions that the bank collects mailing addresses as opposed to simply 'address' or 'current address.' Also, the policy mentions that the bank collects information about the place of employment. RBC will also request and maintain any 'additional detail' it needs to better serve clients. However, the RBC policy does not specify what additional details it requests other than to say that it "will need to ask for more detailed financial and personal (or business) information" in certain situations. RBC indicates that it collects and retains any information that assists it in knowing more about one's family, assets held, financial goals, retirement plans, tax situation, trusts, will and estate plans. For opening a bank account or purchasing investments, RBC requires a client to provide his or her permission to review credit history.[240]

The Toronto Dominion Bank (TD Bank) policy states that the bank will collect its clients' employer's name. Although the *PCMLTFA* requires information on a client's occupation, it does not require that the employer's name and address be provided. However, TD Bank has interpreted the *PCMLTFA* as requiring this information, likely for verification purposes. TD Bank also retains clients' e-mail messages and a record of web pages a client visits prior to access of its online services. Moreover, TD Bank reserves the right to collect transactional information on a client from other service providers who are associated with a client's bank account. For example, it can obtain such information from a service provider that receives bill payments from a client's account.[241]

The Scotiabank privacy policy states that the bank collects personal information when receiving a guarantee in respect of a product or service from a client. It will also collect documents such as a recent utility bill to verify a client's name and address. For certain types of investments and credit products, Scotiabank will collect information on a client's annual income, assets, liabilities, risk tolerance and investment knowledge. For these services, the bank will consult sources such as private investigative bodies and "any other person as may be permitted or required by law." Scotiabank states that it uses hospitals, government health insurance plans, and private investigators as sources of getting personal information. Scotiabank does not currently record personal information on

[240] *Supra*, note 238, RBC Privacy Policy.
[241] *Supra*, note 238, TD Privacy Agreement.

clients' browsing activities on its websites which are unrelated to use of its online services. [242]

The CIBC privacy policy does not view name and address as personal information. It indicates that CIBC collects client's marital and education status. It defines financial information as including tax returns, net worth statements, and employment income.[243]

The Bank of Montreal's privacy policy does not explicitly indicate what pieces of personal information it collects other than SINs and telephone conversations. Although it states it collects financial information, it does not provide examples.[244]

2) Legal Regime Governing Information Collection

Analysis of legal mechanisms governing the collection of information by the banking industry will consider a) the application of general privacy principles under *PIPEDA* in the banking context; b) the interaction between these and other principles and provisions of *PIPEDA*; and c) issues that remain to be resolved. The general principles under *PIPEDA* include i) the requirement that banks clearly identify the purpose of information collection; ii) the requirement that there be informed consent for collection; iii) the principle that the provision of services can only be contingent on consent to collection and legitimate purposes for collection; iv) the limitation on the requirement of informed consent where obtaining consent would undermine law enforcement activities such as fraud detection; and v) the limitation of information collection to that which is required for stated purposes. Issues that remain to be resolved include A) limitations on information collection when banks provide investment and insurance services; B) whether banks may share illegally collected information with law enforcement and national security agencies; and C) similar issues pertaining to the retention of information.

Canadian domestic banks are repositories of significant amounts of personal information. The privacy regime that governs the collection of personal information is *PIPEDA*. *PIPEDA*'s Principle 4.2 requires banks to identify the purpose of collecting personal information at or before the time the information is collected. This requirement applies regardless of whether certain pieces of personal information are required to be collected under law. A bank can collect a SIN only after relaying to a client the purpose behind its required collection.[245] Similarly, a bank teller can ask a client from where his or her money is coming provided that the teller first informs the client that such a question is being asked in order to comply with the *PCMLTFA*.[246] A recent Privacy Commissioner finding relating to collection pursuant to the *PCMLTFA* is notable for it may further narrow the scope of s.7 of *PIPEDA,* which this report has repeatedly identified as needing clarification. For example, the finding undermines s.7(1)(e) which allows for collection

[242] *Supra*, note 238, Scotiabank Privacy Agreement.
[243] *Supra*, note238, CIBC Privacy Policy.
[244] *Supra*, note 238, BMO Privacy Code.
[245] *PIPEDA* Case Summary #209, August 5, 2003.
[246] *PIPEDA* Case Summary #369, January 12, 2007.

of personal information without knowledge or consent where collection is made for the purpose of making a disclosure that is required by law. Moreover, a bank cannot misrepresent the purpose of collecting personal information nor can it rely on proposed legislative purposes of collecting personal information for its current collection.[247]

PIPEDA's Principle 4.3 requires that in almost every instance, banks obtain clients' informed consent before they can collect their personal information. This means that, for instance, a bank cannot rely on a client's consent which was received eight years earlier by a different bank for a different product.[248] Similarly, a bank cannot collect a client's personal information on the basis of consent given for its collection two years earlier to the bank's subsidiary, which operates as a separate and distinct legal entity, and for an account that had closed.[249] The client must reasonably be able to know that he or she is presently consenting to the collection of personal information. The Privacy Commissioner has affirmed this position in cases of taped telephone calls. Despite a bank's written notifications that it reserves the right to tape telephone calls, it must bring this policy to the attention of callers at the time they call; otherwise, any personal information gathered from the taped call will be illegally collected.[250] The purposes of taping the call must be brought to the attention of a client so that he or she is given the ability to object to the taping if it is not necessary to the provision of the service, or otherwise required by law.[251] A bank cannot rely on call display to identify a client and so record a call with him or her based on prior consent.[252] While a bank could tape calls while relying on the express consent of a client which was received while opening a bank account, it appears that the bank would still have to inform the client about being taped at the time of taping.[253]

The Privacy Commissioner of Canada also indicates that meaningful consent in the context of personal information collection means that a bank must be specific about the legal authority under which it is requesting such information so that a client can reasonably understand how the information will be used or disclosed. If a bank does not clearly specify the legal purposes for collecting personal information and collects it anyway, there will be a violation of *PIPEDA*. Banks have violated this principle on numerous occasions through outlining in personal bank account and credit card application forms vague or incomprehensible reasons for collecting and/or using personal information.[254]

---

[247] *PIPEDA* Case Summary #45, April 11, 2002; *PIPEDA* Case Summary #46, April 26, 2002.
[248] *PIPEDA* Case Summary #266, April 16, 2004.
[249] *PIPEDA* Case Summary #246, December 4, 2003.
[250] *PIPEDA* Case Summary #215, August 26, 2003; *PIPEDA* Case Summary #176, June 3, 2003; *PIPEDA* Case Summary #86, October 22, 2002.
[251] *Ibid. # 215.*
[252] *PIPEDA* Case Summary #155, August 15, 2003
[253] *PIPEDA* Case Summary #51, May 16, 2002.
[254] *PIPEDA* Case Summary #350, June 9, 2006; *Supra*, note 235; *PIPEDA* Case Summary #256, October 1, 2003; *PIPEDA* Case Summary #203, August 5, 2003, *PIPEDA* Case Summary #192, July 23, 2003; *PIPEDA* Case Summary # 184, July 10, 2003; *PIPEDA* Case Summary # 97, September 30, 2002.

Consent cannot be overly broad; a client cannot accept a bank's practice of collecting excessive amounts of personal information as condition of obtaining a banking service. Principle 4.3.3 mandates that a bank shall not, as a condition of the supply of a product or service, require a client to consent to the collection, use, or disclosure of information beyond that required to fulfill explicitly specified and legitimate purposes. A bank cannot request all different types of identification from a client solely for the purpose of having a more comprehensive file on the client.[255] A client should not have to consent to providing his or her SIN if he or she is not seeking investment products such as interest-bearing accounts.[256] Also, a client should not have to consent to disclose his or her credit history as a condition of opening a personal bank account if there is no evidence that a client is a financial risk.[257] However, a bank can collect information such as a client's vehicle's model year, the number of kilometres on it, its current value, and property and school taxes when it is offering a loan or other credit service.[258] The ability to repay debt is a legitimate purpose for which such information can be required. Moreover, a bank can collect personal financial information from the sole proprietor of a business when he or she is requesting business products such as loans.[259]

One of the only exceptions to the requirement of seeking a client's informed consent for the collection of personal information is the case where seeking a client's informed consent would undermine the detection and prevention of fraud or other law enforcement activities. The Privacy Commissioner of Canada has rarely discussed this exception. This is likely because in most instances law enforcement and national security services use non-consensual means of obtaining information, namely search warrants, subpoenas and court orders to attain a client's information. In the rare instances where the Commissioner has explored this exception, the Commissioner has discussed it from the perspective of a bank's internal security branch and not from the perspective of external law enforcement or national security services. In one case, the Commissioner found that a bank reasonably disclosed the personal information of a manager to its internal security branch without his knowledge and consent. The manager's knowledge and consent to the disclosure could have compromised the availability or accuracy of the information which was needed to support the case for his dismissal.[260] In a similar case, the Commissioner found that a bank's regional security manager has investigative authority under s.7(1)(b) of *PIPEDA* to collect a client's information without his knowledge or consent in circumstances of a fraud investigation.[261]

Principle 4.4 is another *PIPEDA* principle that governs personal information collection. It stipulates that organizations limit the collection of personal information to that which is necessary for its stated purposes. If purposes for collection are unstated, violating principles 4.2 and 4.3, there will also be a violation of principle 4.4.[262] If purposes are

[255] *PIPEDA* Case Summary #132, March 6, 2003.
[256] *PIPEDA* Case Summary #166, April 23, 2003.
[257] *PIPEDA* Case Summary #40, March 12, 2002.
[258] *PIPEDA* Case Summary #223, January 16, 2003.
[259] *PIPEDA* Case Summary #117, February 11, 2003.
[260] *PIPEDA* Case Summary #84, October 10, 2002.
[261] *PIPEDA* Case Summary #68, August 30, 2002.
[262] *Supra*, note 253, Case Summary #203.

stated, they must not result in indiscriminate collection of personal information. In a credit card application, a bank cannot require a client to consent to the bank's ability to seek out "other information" on a client from "any other source" without specifying what "other" means.[263] The Privacy Commissioner was satisfied the bank in question modified "other" to mean only "other financial-related information" from "references you have provided to us in support of your application." Although the finding was made in relation to seeking personal information for a credit card, it likely applies to the seeking of all banking services. When seeking credit, such as a loan, a client does not need to provide a Notice of Assessment that indicates non-refundable tax credits.[264] When opening a personal bank account, a client does not need to provide a health insurance card or credit history.[265] If there is a violation of Principle 4.4, there will likely be a violation of Principle 5.3 because a bank that collects more personal information than necessary will likely not be collecting such information only for purposes that a reasonable person would consider appropriate in the circumstances. According to Principle 4.1.3, a bank must always ensure that sub-contractors of its services abide by *PIPEDA*. A bank that collects clients' personal information which its marketing agents solicit on its behalf will be deemed to collect it illegally if the bank does not contractually bind its agents to *PIPEDA*.[266]

As one can see, there are many Privacy Commissioner findings on the legality of banks' personal information collection practices. However, several issues remain to be resolved. First, the extent to which *PIPEDA* limits the collection of financial information is unclear when banks are giving clients investment advice or the extent to which *PIPEDA* limits the collection of health information when banks are providing insurance products. Although the Privacy Commissioner has noted that banks should provide specific examples of the types of personal information it collects for its services,[267] the major banks have not sufficiently indicated the contours of personal information collection for investment and insurance services. More importantly, even if the collection of extensive personal information for investment and insurance services is legal, there is uncertainty about whether banks should be providing such information to law enforcement who may not even know of its retention in client files.

Second, the Commissioner has yet to grapple with the question of whether banks can share illegally collected information with law enforcement and national security officials. The Commissioner has not been asked to answer this question because there are seldom, if any, complaints involving such issues. This may be due to the fact that clients are unaware of when banks illegally collect their personal information or of when banks disclose such information to law enforcement and national security services. If the Commissioner were ever to decide a case on the ability of law enforcement and national security services to use a bank's illegally collected information as evidence, there is some grounds on which the Commissioner could find in favour of law enforcement and

---

[263] *PIPEDA* Case Summary #76, October 10, 2002.
[264] *Supra*, note 232.
[265] *PIPEDA* Case Summary #259, January 27, 2004; *Supra*, note 30, Case Summary #256.
[266] *PIPEDA* Case Summary #35, January 10, 2002.
[267] *Supra*, note 235.

national security services. In one of its findings the Commissioner noted that information provided by a bank to credit agencies would be taken by the credit agencies to conform to *PIPEDA* personal information collection requirements, a presumption that becomes stronger with evidence of a contract between the bank and the credit agencies requiring the bank to attest to conformity with *PIPEDA* as a condition for the latter's services.[268]

It is worth noting that similar unresolved issues raised in relation to personal information collection in the banking industry also arise with respect to personal information retention in that industry. Illegal retention can occur when a client explicitly revokes his or her consent to a bank's retention of his or her personal information[269] or when a bank retains personal information on a prospective client who is denied its services.[270] While a bank can provide retained information to law enforcement and national security without the subject's knowledge and consent under s.7(2) of *PIPEDA* if it becomes aware that it has information which it has reasonable grounds to believe could be useful in an investigation of criminal activity or a terrorist threat, can that bank provide this information to them if it was retained years earlier, at a time when the bank had no suspicion of a client's involvement in such activities or threats, and when that client expressly requested that information be destroyed? If this disclosure were permissible, how could one ever exercise one's Principle 4.3 right to have a bank remove his or her personal information? If disclosure were permitted in the hypothetical circumstances outlined above, it would likely undermine the thrust of Privacy Commissioner findings on this issue.[271]

C) Personal Information of Interest to Law Enforcement and Legal Mechanisms Shaping Information Sharing

This section 1) looks to FINTRAC as providing examples of types of information that may be of interest to law enforcement before considering 2) the legal mechanisms that shape the ability of law enforcement to obtain this information. This latter analysis will show that there are three main legal mechanisms shaping information sharing: a) s. 8 Charter jurisprudence, b) *PIPEDA*, and c) PCMLTFA.

1) Interest of Law Enforcement

Law enforcement and national security services are likely to be interested in any information a bank retains that can further an investigation into a crime or terrorist threat. So, any of the information outlined in section 2 is available to police if they know of its existence and can find legal means of attaining it. The most sought after information from a bank is obviously financial information. Financial information is that of an identifiable client and includes bank account balances, bank account activity, payment history and credit history. The Financial Transactions and Reports Analysis Centre (FINTRAC), an independent federal agency that collects, analyzes and discloses banking information to

---

[268] *PIPEDA* Case Summary #181, July 10, 2003.
[269] *PIPEDA* Case Summary #189, July 22, 2003.
[270] *PIPEDA* Case Summary #6, July 23, 2001.
[271] *Supra*, note 267; *Ibid.*

police to help detect, prevent and deter money laundering, terrorist financing or threats to the security of nations, provides examples of the types of financial information police access.[272]

FINTRAC requires banks to provide it with suspicious transaction reports, which document financial transactions which a bank has reasonable grounds to suspect are related to the commission of a money laundering or terrorist activity financing offence.[273] Additionally, FINTRAC requires banks to provide it with large cash transactions reports, which document financial transactions of $10,000 or more, as well as electronic funds transfers reports, which document funds of $10,000 or more sent into or out of Canada. While banks must report to FINTRAC all property in their possession or control that they 'know' is owned or controlled by or on behalf of a terrorist group listed in the *United Nations Suppression of Terrorism Regulations*, they must report directly to RCMP and CSIS all property in their possession or control which they 'believe' is owned or controlled by such a group. This last requirement highlights an important point; FINTRAC has not co-opted the role played by police. Banks can, and sometimes must, disclose certain information that they believe is evidence of crimes or terrorist threats directly to police.

2) Legal Mechanisms Shaping the Sharing of Information

There are three main legal mechanisms that shape the sharing of personal information between banks and police. These three legal mechanisms are s.8 *Charter* jurisprudence, *PIPEDA*, and *PCMLTFA* and its regulations. Discussion of s. 8 reveals i) longstanding recognition of a reasonable expectation of privacy in banking records; ii) limitations on this reasonable expectation of privacy in some circumstances notable among which are bank records held abroad; and iii) the constitutional implications of police obtaining banking info to which a reasonable expectation of privacy applies. Subsequently, the focus will be on the scope for warrantless disclosure to law enforcement and national security agencies pursuant to *PIPEDA* and PCMLTFA through consideration of i) subpoena and court orders, ii) other lawful authority, iii) national or international security threats, iv) voluntary bank disclosure, and v) FINTRAC.

a) S. 8 Charter Jurisprudence

Section 8 *Charter* jurisprudence is the primary way law shapes the sharing of personal information between banks and police. As discussed in the introduction of this report, section 8 governs when there is a reasonable expectation of privacy in items seized. The courts have long held that clients have a reasonable expectation of privacy in their bank records. Mr. Justice Iacobucci stated in *Plant* that "bank records are a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the State." [274] Courts recognize that a balance must be struck between a client's right to confidentiality of banking information and the

[272] See FINTRAC, March 24, 2003, *Guideline 1: Backgrounder* available at http://www.fintrac-canafe.gc.ca/publications/guide/Guide1/1-eng.asp (last accessed on March 3, 2008).
[273] *Ibid.* at 20.
[274] *Supra*, note 232 at 12 (introduction).

public's right to effective law enforcement. As such, not all information held by banks will constitute bank records for purposes of *Charter* protection. In *R. v. Eddy*, Puddester J. described the type of banking information which will be protected by the *Charter* as "the records of an individual's personal financial position, and the pattern of the individual's operating on his or her bank account."[275] Consequently, brokerage records are also protected.[276] However, many pieces of information are not protected. 'Tombstone information' in the form of the name(s) of an account holder and its signatory authority is not protected.[277] A client's signature is not protected.[278] The existence of banking activity, such as a cheque deposit into a particular account, is not protected.[279] Banks can, but do not have to, provide such information to police in the absence of a legal basis requiring their provision. Where banks provide such information to police there will not be a search as no reasonable expectation of privacy exists in the information.

Similarly, in *R. v. Schreiber*, the Supreme Court of Canada held that there is no reasonable expectation of privacy in bank records held in another country.[280] This means that Canadian police are more restricted when collecting personal information stored in Canada than abroad. Although information stored abroad will not be subject to section 8, it may be subject to s.7 of the *Charter*. If foreign authorities collect banking information in a manner that renders a subsequent Canadian criminal trial unfair, it will be excluded under s.7. In *R.v.Hape*, the Supreme Court of Canada indicated that one way in which foreign authorities could render a subsequent Canadian criminal trial unfair is if the procedural requirements for lawful search and seizure under their law fail to meet standards commonly accepted by free and democratic societies.[281]

When police ask for and are given banking information that comprises a biographical core of personal information it will always be a search regardless of whether the information is received by telephone or in person.[282] Personal information which banks voluntarily provide to police can also constitute a search under s.8 of the *Charter*.[283] There will be a search where a bank provides police with details of an identifiable client's bank records, such as his or her transactional record of deposits and withdrawals.[284]

Police search of Canadian bank records will only violate the *Charter* if the search is conducted unreasonably. The reasonableness of a search always depends on contextual factors. A warrantless search of Canadian bank records is *prima facie* unreasonable. Even where warrants are used, there have been instances where courts have quashed them on the basis that the Informations to Obtain them have been fraught with serious errors such

---

[275] *R. v. Eddy*, [1994] N.J. No. 142 (Nfld. S.C.) at para. 175.
[276] *R. v. Zuk*, [2004] O.J. No. 4379 (Ont. C.J.).
[277] *R. v. Quinn*, [2006] B.C.J. No. 1170 (B.C.C.A).
[278] *R. v. Pheasant*, [2000] O.J. No. 4237 (Ont. C.J.) at para. 41.
[279] *R. v. Lillico*, (1994), 92 C.C.C. (3d) 90 (Ont. Gen. Div.), upheld on appeal at [1999] O.J. No. 95 (C.A.).
[280] *R. v. Schreiber*, [1998] 1 S.C.R. 841.
[281] *R. v. Hape*, [2007] S.C.J. No. 26.
[282] *Supra*, note 273 at para.183.
[283] *R. v. Evanishen*, [1998] S.J. No. 752.
[284] *Supra*, note 273.

as deliberately misleading evidence[285] or mere speculation that bank records will afford evidence of criminal activity.[286] A court will not grant a search warrant for bank records based only on observations of large cash deposits being made into a bank account.[287] Where search warrants are used, they can only be used in a manner that accords with its stipulations. There will be an unreasonable search where banks provide police with bank records from a location not specified in the warrant.[288] For criminal investigations, banks can only voluntarily release information if they have reasonable grounds to believe that a crime has occurred, is occurring or is about to occur.[289]

b) Laws Governing Warrantless Disclosures of Bank Records pursuant to *PIPEDA* and *PCMLTFA*

A warrantless search is permitted when it is carried out reasonably in accordance with a reasonable law. Since its *Jarvis* and *Ling* decisions, the Supreme Court of Canada has made it clear that warrantless searches in the form of requirements issued on banks pursuant to the *Income Tax Act* will not be permitted to investigate penal liability.[290] As discussed in the introduction, *PIPEDA* allows for exceptions to disclosure of personal information to police in a variety of circumstances aside from the use of search warrants. According to *PIPEDA*, banks can disclose personal information to police pursuant to a subpoena, court order, national or international security threat, or other 'lawful authority.' *PIPEDA* also approves disclosures to FINTRAC, which in turn can disclose personal information to police pursuant to the *PCMLTFA* and its regulations.

i) Subpoena and Court Orders

Under 7(3)(c) of *PIPEDA*, banks can disclose personal information in the form of an identifiable client's bank records to police when banks receive subpoenas and court orders from them. Section 30(5) of the *Canada Evidence Act* allows for a court to compel bank records without a search warrant. If banks choose not to disclose the records to police when faced with a subpoena or court order, they will not violate *PIPEDA* but may be found in contempt of court. A court-issued subpoena to banks will typically involve use of s.698 and s.700 of the *Criminal Code* requiring bank officials to appear in court with requested bank records. Once it receives the records, the court will seal them until it is prepared to rule on their admissibility in court proceedings.[291] The court will apply the *O'Connor* test to determine whether records should be admitted; it will firstly ask whether the bank records are likely relevant to an issue before the court and secondly ask whether the salutary effects of admitting the bank records outweigh the deleterious consequences of their admission. The court retains much discretion in this process; it is a process of ad hoc judicial balancing of various factors such as the extent to which bank records are necessary to fulfill the public interest in effective and fully informed law enforcement as well as the reasonable expectation of privacy held in such records. In *Cheung*, although the court conceded that the accused retained a reasonable expectation

---

[285] *R. v. Triffin*, [2005] O.J. No. 3484.
[286] *R. v. Nguyen* [2004] B.C.J. No. 250 (B.C.S.C.).
[287] *Ibid*.
[288] *R. v. Donaldson*, (1990), 58 C.C.C. (3d) 294 (B.C.C.A.).
[289] *PIPEDA*, s.7(3)(d)(i).
[290] *Supra*, note 241 (introduction); *R.v.Ling*, [2002] 3 S.C.R. 814.
[291] *R. v. Cheung*, [2001] O.J. No. 3289 (Ont. S.C.J.).

of privacy in bank records being sought, the state interest in using the records to oppose her co-accused's application for their seized proceeds of crime outweighed the privacy interest.[292]

The use of other types of court orders is another means for police to legally obtain bank records. Courts have ordered banks to release information to police pursuant to a s.18 "evidence gathering order" of the *Mutual Legal Assistance in Criminal Matters Act (MLACMA)* where a treaty partner, like the United States or Czech Republic, is seeking bank records held in Canada for criminal investigations it is conducting in its own jurisdiction.[293] Similarly, courts have ordered FINTRAC to release bank records pursuant to s.60 "production orders" of the *PCMLTFA* when police have demonstrated reasonable and probable grounds that an offence has been, is being, or will be, committed.[294] Another common type of court order is the *Norwich order*. This order is used to compel banks to provide victims of crime with bank records when the banks have an equitable duty to assist them. A bank has an equitable duty to assist victims in cases where they have been defrauded and only banks can reasonably identify the wrongdoers, find and preserve evidence that may discover, support or substantiate a legal action against wrongdoers, or trace and preserve their assets.[295] Unless stated otherwise in the order, victims of crime can share bank records obtained pursuant to it with police.

ii) Lawful Authority

Police can obtain personal information from banks if they request this information and indicate their lawful authority. There is very little case law on what 'lawful authority' entails for the purposes of s.7(3)(c.1)(ii) of *PIPEDA*. As discussed in the introduction, *Re (S.C.)* indicates that the mere fact that police are conducting a criminal investigation is not a basis upon which banks can disclose personal information. Lawful authority is likely authority outside of a warrant, subpoena, or court order. 'Lawful authority' may include warrantless searches in exigent circumstances short of national or international security threats. This area of the law needs to be clarified. As one lawyer who deals with privacy issues noted, major banks are uncertain about the application of this provision to requests of information made by police pursuant to common law investigatory power as opposed to other governmental regulators who base their 'lawful authority' in statute.[296]

iii) National or International Security Threat

Unlike in criminal investigations where bank records are not sought from *FINTRAC*, police can use their suspicion, rather than credibly based probability, of national and international security threats to reasonably search and seize bank records. Police can request bank records if they "suspect that the information relates to national security, the

---

[292] *Ibid.*
[293] *Canada (Attorney General) v. Pacific Network Services*, [2003] B.C.J. No. 3004 (BCCA); *Krhanek (Re)*, [2006] B.C.J. No. 1513 (BCSC).
[294] FINTRAC, 2006, *Annual Report*, available online at http://www.fintrac.gc.ca/publications/ar/2006/menu-eng.asp (last accessed March 3, 2008).
[295] *Alberta (Treasury Branches)* v. *Leahy*, [2000] A.J. No. 993 (Q.B.); aff'd (2002), 51 Alta. L.R. (4th) 94 (C.A.); application for leave to appeal dismissed, [2002] S.C.C.A. No. 235; *Isofoton S.A. v. Toronto Dominion Bank (c.o.b. TD Canada Trust)* [2007] O.J. No. 1701 (Ont. S.C.J.).
[296] Interview conducted by author, subject requested name be withheld, August 21, 2007.

defence of Canada or the conduct of international affairs."[297] Likewise, banks can proactively and voluntarily provide bank records to police if they suspect that such records relate to the same concerns.[298] It is unclear how often police request bank records, and how often banks proactively and voluntarily disclose such records to police, using these grounds. There is no external oversight in the use of this power.

iv) Voluntary Bank Disclosures

Section 7(3)(d)(i) of *PIPEDA* allows banks to voluntarily disclose bank records to police if banks have reasonable grounds to believe that the records relate to a crime that has been, is being, or is about to be committed.

v) FINTRAC

As indicated above, FINTRAC is not a police agency. Section 7(3)(c.2) of *PIPEDA* allows banks to provide certain types of bank records to FINTRAC for purposes of financial intelligence gathering and analysis. FINTRAC will assess bank records and pass them on to Canadian police if there are "reasonable grounds to suspect" that such information would be relevant to investigating or prosecuting a money laundering offence, a terrorist activity financing offence, or threats to the security of Canada. It is unclear whether this suspicion standard is constitutionally permissible in relation to crimes as opposed to security threats. When other government agents, such as income tax auditors or social assistance case workers, provide criminal investigators with bank records they must establish reasonable and probable grounds that the records are evidence of criminal activity.[299] A lower standard appears to apply to FINTRAC.

Other privacy safeguards that are aimed at ensuring that FINTRAC only discloses bank records to the extent minimally required by law include regulations which mandate only "designated information" to be disclosed and which provide criminal penalties of up to five years in jail or a $500,000 fine, or both, for unauthorized disclosure.

D) Formal and Informal Information Sharing Practices

It is possible to draw the distinction between formal and informal information sharing according to whether disclosure is pursuant to a court issued order. For the former police will present banks with a court issued document; for the latter they will not. The following will discuss 1) the procedures banks follow when met with a formal request for information and 2) informal information sharing a) that is pursuant to some other legal authority following a police arrest as opposed to b) that which is initiated by the bank.

1) Formal Personal Information Sharing

The formal means of information sharing between banks and police occurs through a police request in the form of a search warrant, subpoena or court order. Police will have to meet all the requirements to obtain such court-issued documents. Police will deliver these court-issued documents to bank branches or bank headquarters. Some banks will

---

[297] *PIPEDA*, s.7(3)(c.1)(i).
[298] *PIPEDA*, s.7(3)(d)(ii).
[299] *R. v. Hannah*, [1996] O.J. No. 3489 (Ont. Ct. Gen. Div.); *Supra*, note 287.

accept these formal requests at the branch level where information is being kept while other banks will require formal requests be made at the central corporate security level. Banks like TD-Canada Trust, BMO, RBC, and CIBC have accepted requests both at the branch and at the headquarters level.[300] Even where a request is made at the branch level, branch managers at various major banks have stated that they will consult with their regional supervisor before the bank releases any information to police.[301] Banks will record all requests for bank records received in the form of court-issued documents. If a bank refuses to disclose bank records after a search warrant, subpoena or court order has been served on them, the police may be able to obtain a general warrant under s.487.01 of the *Criminal Code* and an accompanying assistance order to coercively rather than cooperatively seize bank records.[302]

2) Informal Personal Information Sharing

Informal information sharing occurs when police receive bank records without the use of a search warrant, subpoena or court order. This may occur in two primary ways. First, police can request and receive bank records from banks and FINTRAC pursuant to some other legal authority. Secondly, banks and FINTRAC can proactively provide police with bank records without a police request.

a) Requests for bank records pursuant to some 'other' legal authority

Police often make requests for personal information using some legal authority, other than a search warrant, court order or subpoena. As indicated above, "lawful authority" in *PIPEDA* remains undefined. "Lawful authority" may refer to the statutory legal authorities police currently use in seeking bank records. Police request bank records pursuant to many statutes.

For instance, police request bank records pursuant to the *Bankruptcy and Insolvency Act (BIA)*. The Superintendent of Bankruptcy can order police to investigate crimes related to bankruptcy claims. In one case, a police officer had a card issued by the Superintendent of Bankruptcy that identified him as a member of the Royal Canadian Mounted Police authorized "to make inquiries and investigations pursuant to Sections 10(1), 5(3)(e) and 6(2) of the *Bankruptcy Act* and to make or cause to be made one or more copies of any book, record, paper or other document pursuant to Section 10(7) of the said Act."[303] In that case, the court held that the officer was entitled to request and retain bank records without having reasonable and probable grounds to believe that a crime had been, was, or was about to be, committed. The court made clear that banks which refused to provide bank records after receiving such a request would be subject to statutory penalties identified in the *BIA*.

---

[300] *United States of America v. Orphanou*, [2004] O.J. No. 622; *R.v.Lear*, [1998] M.J. No. 351 (Q.B.); *Supra*, note 276; *Supra*, note 289.

[301] Interviews conducted by the author, Ali Mian, August 2007, with various bank managers who asked to have their names withheld.

[302] *Canada (Department of National Revenue) (Re)* [1998] O.J. No. 3517 (Ont. C.J. Prov. Div.).

[303] *R. v. Ezzeddine*, [1996] A.J. No. 338 (Q.B.) at para. 14.

Police can also request information from FINTRAC. This is typically done through production orders. However, these orders are rarely used; only nine such orders have been issued to date.[304] In fact, police rarely request bank records from FINTRAC because they find that FINTRAC is almost never helfpul, in that there is usually no response or, when there is a response, it provides limited information that cannot assist police with commencing new investigations.[305] Limited information comes in the form of ”tombstone” data”: a transaction's date and place, its value, and the associated account numbers and names of the parties involved. This continues to be the case even after the Auditor General noted this deficiency in her 2004 report. FINTRAC still does not provide reasons for disclosing suspicious transactions to police. The Auditor General noted that it is precisely these reasons which police are seeking but lack.[306]

The other commonly used form of legal authority is common law investigative powers. Cases have shed some light on the types of requests police can make without infringing *Charter* rights. Police can request that a bank provide it with the name of an account holder only if police do not already have a complete transactional record which they can link to that name,[307] with a confirmation or denial of a certain banking activity such as a deposit being made in a particular account,[308] and with information about whether a bank carries a suspect’s bank records and where it is held.[309]

Although the major banks receive thousands of police requests for bank records, it is difficult to gauge how many of these requests are informal because some of these banks do not keep records of informal requests.[310] Consequently, it is difficult to assess the extent and nature of these informal requests.

b) Proactive Release of Bank Records

As indicated above, s.7(3)(d)(i) of *PIPEDA* allows banks to release bank records to police when banks have reasonable and probable grounds to believe that a crime has occurred. Courts have allowed this to occur in cases of suspicious transactions indicative of dealings in proceeds of crime. [311] It is unclear how often banks disclose information directly to police rather than to FINTRAC. It is unlikely that banks are disclosing more information to police now than they used to in pre-FINTRAC years. In 2000, each of the five major banks disclosed between fourteen and 169 cases of suspicious transactions to police.[312] It is more likely that banks are disclosing more suspicious transaction reports to FINTRAC rather than to police. In 2006, reporting entities, which include the major banks, disclosed 29,367 suspicious transaction reports to police.

---

[304] *Supra*, note 292.
[305] Auditor General Report, 2004, Office of the Auditor General, at para 2.39.
[306] *Ibid.* at para 2.40-2.41.
[307] *Supra*, note 273; *Supra*, note 275, *Supra*, note 277.
[308] *Ibid.* note 55.
[309] *Supra*, note 275.
[310] Canadian Bankers’ Association, interview conducted by the author, Ali Mian, August 2007.
[311] *Supra*, note 275; *R.v.Gordon*, [1999] O.J. No. 541 (Ont. C.J. Gen. Div).
[312] Beare, Margaret, 2000, “Suspicious Transaction Study: Referrals by Financial Institutions” cited in Beare, Margaret and Stephen Schneider, 2007, *Money Laundering in Canada: Chasing dirty and dangerous dollars*. Toronto: University of Toronto Press at 213.

The reports collected by FINTRAC will be analyzed for unusual patterns of transactions that resemble money laundering or terrorist financing activity. FINTRAC will match these preliminary analyses with information from law enforcement and other databases. As indicated above, FINTRAC releases information to police on the "reasonable grounds to suspect" standard, a standard that FINTRAC admits is informed not by Canadian but by international guidelines.[313] Surprisingly, while FINTRAC collects millions of reports each year from banks, it discloses less than 1% of these reports to police. For example, in 2006, FINTRAC received 14,920,758 large cash transactions, electronic funds transfer and suspicious transaction reports from reporting entities, it only made 168 disclosures to police.[314] Of the 168 disclosures, 134 were for suspected money laundering, 33 were for suspected terrorist financing and other threats to the security of Canada, and 1 was for a combination of these activities. 77% of these disclosures were based on electronic funds transfer reports, 71% were based on large cash transaction reports, and 64% were based on suspicious transaction reports. Police do not give much weight to these unsolicited FINTRAC reports for the same reasons that they do not request much information from FINTRAC: namely, to make this information useful, police would need to know why FINTRAC finds this transaction to be suspicious.[315]

E) Gaps and Controversies

There are a number of gaps in privacy protection and privacy-related controversies surrounding the sharing of personal information between banks and police. This section will discuss the following gaps and controversies: 1) the dearth of law regarding retention of information on banking clients; 2) the fact that there is no present requirement that banks document informal police requests; 3) the lack of transparency pertaining to circumstances in which banks proactively disclose information; 4) questions surrounding the constitutionality of the "reasonable grounds to suspect" standard for disclosure by FINTRAC; and 5) the dearth of law regulating the use of foreignly obtained banking records by Canadian police.

First, there are few laws that limit the amount of information a bank can retain on its clients. Although Principle 4.4 of *PIPEDA* limits collection of information to that which is necessary for identified purposes such as the provision of banking services, there is no guidance on how much of a client's financial information can be retained.

Second, laws presently do not require banks to document informal police requests for bank records. This makes it difficult to assess the nature and extent of informal requests at banks that do not keep records of them. For example, it is unclear how successful police are at using "lawful authority" or "national or international security threat" justifications from *PIPEDA* for disclosure of bank records. Also, without a record of informal requests, it is impossible to document how often and under what circumstances banks disclose bank records pursuant to such requests. Of the major banks that do keep

[313] *Supra*, note 303 at para 2.35.
[314] *Supra*, note 292.
[315] *Supra*, note 303 at para. 2.25.

these records of informal requests, there is presently no independent publicly accountable authority responsible for assessing the legality of these requests. Thus, there is presently no independent public accountability in the current process.

Third, there is a lack of transparency in the types of circumstances in which banks proactively disclose information to police. Although banks have said that they disclose information to police after reviewing cases "on their merits,"[316] this does not elucidate the types of cases where the "reasonable grounds to believe" standard required by s.7(3)(d)(i) has been met.

Fourth, the "reasonable ground to *suspect*" standard that FINTRAC uses to disclose personal information to the police for those suspected of criminal activity may be unconstitutional. As indicated above, *PIPEDA* requires banks to meet a standard of "reasonable grounds to *believe*" for disclosing bank records in cases of suspected crimes; it may be unconstitutional for a lower standard to apply elsewhere. Presumably, one retains the same level of reasonable expectation to privacy in bank records regardless of who has them.

Fifth, and again on the issue of the appropriate standard to be applied to disclosure of bank records to police, there are no laws which regulate Canadian police when they obtain Canadian bank records from foreign authorities. For example, could Canadian police receive and use Canadian bank records, obtained by U.S. police, which were seized using subpoenas under the authority of the President and Congress such as those of the Office of Foreign Assets Control (OFAC) of the United States Treasury Department? This is a logical extension of the facts in the *SWIFT* case where the Privacy Commissioner held that these U.S. authorities could use these non-judicially sanctioned subpoenas.[317]

F) Conclusions and Recommendations

Recommendation 1: Banks should provide clear guidelines to clients on what types of personal information can and must be collected for services such as investment advice.

The major banks are repositories of significant amounts of personal information. With ever expanding services, there is increasing tendency by the banks to retain more personal information. However, the banks have not effectively indicated to clients the extent of personal information needed for many of their services. Clients should be able to know what personal information the banks are retaining, and are permitted to retain, for services such as investment advice.

[316] *Supra*, note 308.
[317] *PIPEDA* Case Summary #365, April 2, 2007.

Recommendation 2: all banks should keep track of the nature and extent of informal police requests for bank records, especially the authority under which these records are being sought, as well as the circumstances in which the records are disclosed.

The major banks receive many informal requests from police to disclose bank records. Some major banks do not keep records of these informal requests because there are no laws requiring them to do so. Without a proper trail of informal requests, it is difficult to gauge how police are trying to access bank records without judicial authorization and, consequently, in what circumstances banks are choosing to disclose them without judicial authorization.

Recommendation 3: an independent and publicly accountable authority, such as the Office of the Privacy Commissioner of Canada, should be tasked with assessing the legality of informal police requests for bank records which banks document

Even where banks keep a record of the nature and extent of informal police requests, their legality is often not assessed by an independent and publicly accountable authority.

Recommendation 4: Parliament should clarify PIPEDA terms such as "lawful authority" and "national security threat" by providing examples of when personal information such as bank records can be disclosed without judicial authorization.

There remains uncertainty under what circumstances bank records can be released without judicial authorization but in conformity with *PIPEDA*. Exceptions to non-disclosure of personal information found in *PIPEDA* such as "lawful authority" and "national security threat" must be clarified by Parliament, the Office of the Privacy Commissioner of Canada, or by the courts.

Recommendation 5: The Government of Canada or the Privacy Commissioner should bring a reference to the Supreme Court of Canada to inquire whether the standard of 'reasonable suspicion' can ever be justified to disclose personal information, such as bank records, to police in a criminal context.

A final issue that must be resolved is the constitutionality of the "reasonable suspicion" standard used by FINTRAC in its disclosures of bank records to police.

V. **Airlines Industry**

Written by Michelle Yau

Introduction

In the post-9/11 world, one of the most important questions facing many states is how to balance the nation's security interests with individual privacy interests. The object of this report is to examine the current balancing of these interests in the context of personal information sharing between airlines and investigative authorities such as the RCMP and CSIS, and to make recommendations as to ways in which privacy rights can be better protected.

Following A) an overview of the industry and how it is regulated, the section considers B) the collection of personal information by airlines and the statutory regime that governs it and C) the types of personal information that may be disclosed by the airlines to the authorities and the statutory regimes that govern disclosure. Then, D) formal and informal information sharing practices of the airlines will be discussed, and E) any gaps in privacy protection in practice or in the legislative/regulatory regimes will be identified. Finally, F) recommendations for enhancing individual privacy will be suggested.

As will be demonstrated later, the limited research that it was possible to conduct for this report does not reveal that substantial breaches of privacy are in fact occurring on a regular basis; however, based on the current state of the legislative and regulatory regimes concerning personal information sharing between airlines and the authorities, as well as certain practices of airlines and investigative agencies, the risk of undue violation of privacy of airline passengers is nonetheless high. The recommendations at the end of this report are made in consideration of these possibilities.

A) Overview of Industry and How it is Regulated

The Canadian airline industry is a federally regulated industry that is governed by a number of statutes. However, there are two that are particularly pertinent to the collection, retention and sharing of information – the *Aeronautics Act* and the *Personal Information Protection and Electronic Documents Act* (*PIPEDA*.) The *Aeronautics Act* is specific to the airline industry, while *PIPEDA* applies to federally regulated industries (such as aviation) and provincially regulated businesses. The former regulates information sharing between airlines and the RCMP, CSIS, and Department of Transport, specifying when airlines may be obligated to disclose information to the authorities, what types of information they are obligated to disclose, how the information is to be handled by authorities after disclosure, etc. The latter regulates how federal industries collect, use and disclose personal information in a commercial context. The relevant provisions of the *Aeronautics Act* will be discussed in detail in the following sections, and *PIPEDA* will be referred to where relevant while keeping in mind the detailed discussion of it in the general introduction to this report. As well, various other statutes governing disclosure of information by airlines and subsequent handling of information by government entities will be discussed in the section on disclosure of information.

B) Information Collected by the Industry

Information collection by the airline industry reveals itself to be quite extensive. This section will consider not only 1) the nature of information collection by the airline industry but also 2) the legal mechanisms governing collection. In subsection 1) analysis of the nature of information collection shows that among the types of information collected by the airline industry are a) the sort of customer and payment information that is collected by many other industries; b) information specific to some of the services airline provide, such as meals and c) sector specific information such as Advance Passenger Information (API) and Passenger Name Records (PNRs). Interviews with officers of airlines further illuminated the information handling practices of airlines. Subsection 2) reveals that mechanisms governing collection include *PIPEDA*, in conjunction with the guidance provided by non-binding Privacy Commissioners findings.

1) Nature of Information Collection

Information collection by airlines is governed by *PIPEDA* (particularly s.5(3), s.7(1), and clauses 4.2, 4.3, 4.3.2, 4.3.3, and 4.4 in Schedule 1,) which finds expression in the privacy policies of various airlines such as Air Canada and Westjet. In order to get a sense of the typical airline privacy policy and the kinds of information airlines collect, the online privacy policies of Air Canada and Westjet were reviewed.

Air Canada collects passengers' names, addresses, telephone numbers, credit card numbers/expiry dates and gender in order to process purchases, estimate the weight of aircraft and build profiles of passengers' interests for promotional purposes. If special services are requested, such as special meals, discount offers for children/seniors and special assistance, additional information such as meal preferences, date of birth and medical information is collected.[318] Westjet collects substantially the same information as Air Canada; to process purchases and refunds it collects passengers' names, addresses, e-mail addresses, phone numbers, credit card information and gender. Special services such as the ones mentioned previously require additional information similar to that required by Air Canada.[319]

Westjet's privacy policy also mentions that U.S. and/or Canadian government authorities may require it to collect passengers' full name, date of birth, citizenship, gender, passport number and country of issuance, means of payment for the flight, details about how it was booked, and any other unspecified information required by the authorities.[320] Though Air Canada's privacy policy does not directly state the types of information that may be required by governmental authorities, it does state that it is subject to requirements to collect "advance passenger information."[321] Advance passenger

[318] Air Canada Privacy Policy. Available online at: http://www.aircanada.com/en/about/legal/privacy/policy.html (last accessed on February 7, 2008).
[319] Westjet Privacy Policy. Available online at: http://c1dsp.westjet.com/guest/showAgreement.shtml?AgreementType=Privacy+Policy#personalinfo (last accessed on February 7, 2008).
[320] *Ibid.*
[321] *Supra* note 317.

information (API), which is collected every time an individual purchases a plane ticket, includes individual's name, date of birth, sex, type/number/country of issue of his/her travel document, citizenship and/or nationality, and Passenger Name Record Number.[322]

In addition to API information, Passenger Name Record (PNR) information is also collected every time a passenger purchases a ticket. PNR information includes information contained in airline travel reservation systems, such as passenger name, travel itinerary, booking personnel (if a travel agency is used), phone number, ticket number, and special services information. It can also include checkpoint information, such as seat number, pieces of baggage checked, and frequent flyer information.[323] A PNR can reveal where someone went, when, with whom, for how long, and at whose expense; also, depending on whether an individual requests certain opt-in services or offers, a PNR can reveal whether someone asked for one bed or two in a hotel room when traveling with others; through meeting codes used for discounts, it can reveal affiliations with organizations; through special service codes, it can reveal physical and medical conditions (such as being in a wheelchair or being in need of oxygen on board;) and through meal requests, it can reveal religious practices (e.g. on an Air Canada flight, passengers can order special kosher meals, Hindu non-vegetarian meals, and Muslim vegetarian meals.) When a travel agency is used, PNRs may even contain notes intended for the use of the travel agency on tastes, preferences and even personality traits (e.g. "customer is difficult, always changes his mind.")[324]

To further clarify the information handling practices of airlines, phone interviews were conducted with officers of two airlines who were responsible for handling requests for information from investigative authorities. One of the interviews was held with Jeff Plimmer, the Manager of Corporate Security at Westjet, in July 2007. Mr. Plimmer indicated that Westjet does not collect any information from travelers that is not mentioned in its online privacy policy. However, Westjet's privacy policy states that it may be required to collect and/or provide "any other personal information… as required by [a] government authority." This vague statement (perhaps inevitable considering the broadness of various statutory provisions requiring airlines to provide government authorities with information) technically covers any and all types of personal information, and does not tell the traveler much about what can actually be collected or disclosed to authorities. Furthermore, the traveler is not told at the time of collection of information (e.g. at check-in or booking) that the information may be disclosed for national security or law enforcement purposes. Mr. Plimmer also indicated that Westjet stores all personal information in one place (the reservation system,) and that no traveler information is stored in systems or databases that are accessible to other air transport organizations. Westjet also does not collect passenger information from other airlines or government agencies (beyond noting certain individuals as subjects of investigation upon being informed by the authorities.) Lastly, Mr. Plimmer states that Westjet considers

---

[322] Stanley Cohen, *Privacy, Crime and Terror*, p.461.
[323] Colin J. Bennett, "What Happens When You Book an Airline Ticket? The Collection and Processing of Passenger Data Post-9/11," in Elia Zureik and Mark B. Salter, eds. *Global Surveillance and Policing: Borders, Security, Identity* (Portland: Willan Publishing), p.117.
[324] *Ibid.* at p.118.

correspondence to and from a passenger, as well as Westjet's internal correspondence about a passenger, to be personal information about that passenger.

The second interview was conducted with the Director of the Privacy Office at a smaller Canadian airline, who wished himself and his airline to remain anonymous, in August 2007. The Director indicated that his airline only collects information necessary for processing the traveler's purchase, but also that passengers are not told at the time of collection that their information may be disclosed for national security or law enforcement purposes (though, as with Westjet, this possibility is mentioned in the privacy policy.) The airline stores information in its reservation system, and no passenger information is stored in systems or databases that are accessible to other air transport organizations. However, on rare occasions the airline does request personal information about passengers from other airlines on a case-by-case basis. The Director also stated that his airline interprets the meaning of "personal information" as broadly as possible, and considers anything that identifies the passenger to be personal information – including the passenger's image and voice.

2) Legal Regime Governing Information Collection

In addition to being governed by *PIPEDA*, the collection of information by airlines is guided by the findings of the federal Privacy Commissioner in cases brought under *PIPEDA*. In one such case, a traveler complained that in order to claim missing baggage, she had to fill out a form asking for her SIN number and occupation, neither of which were marked optional. The Privacy Commissioner found that the collection of SIN and occupational information was inappropriate for the purpose of processing and verifying a baggage claim (i.e. in contravention of Principle 4.3.3 of *PIPEDA*.) The airline agreed to take the SIN requirement off the form, but refused to remove the occupational information requirement (the Federal Privacy Commissioner's findings are not legally "decisions" and are not binding on the parties.)[325] Thus, there exists at least one airline that may collect occupational information if a baggage claim is made.

C) Personal Information of Interest to Law Enforcement and Legal Mechanisms Shaping Information Sharing

The disclosure of personal information by airlines to various government authorities, and its collection/use by these authorities, is regulated by a number of statutes. In addition to specifying procedures and conditions of information sharing, these statutes also give a sense of what kinds of information the authorities request by specifying what kinds of information airlines are obligated to disclose to the authorities. This section will consider information sharing by reference to 1) the *Aeronautics Act*, 2) the *Canadian Security Intelligence Service Act*, 3) the *Immigration and Refugee Protection Act* (*IRPA*) and its regulations, 4) the *Customs Act* and 5) *PIPEDA*. Further sources that bear revelations pertaining to the context of information sharing and the impact of the privacy interests of Canadians include: the *USA Patriot Act,* The Report of the Events Relating to Maher

[325] Privacy Commissioner's Findings *PIPEDA* case #148.

Arar, Federal Privacy Commissioners Findings under *PIPEDA* and the interviews with airline representatives.

The *Aeronautics Act* governs disclosure of personal information by airlines to the RCMP, CSIS, and Department of Transport, and the use of the information by these authorities. Sections 4.81 and 4.82 of the *Aeronautics Act* require airlines to potentially disclose 34 items of information, on request, to the Minister of Transport, an officer of the Department of Transport, the Commissioner of the RCMP, a person designated by the Commissioner of the RCMP, the Director of CSIS, or a person designated by the Director of CSIS. The aforementioned authorities may require an airline to disclose any of the following information if in the airline's possession:

- full name
- date of birth
- citizenship/nationality/country of issuance of travel documents
- gender
- passport number/visa number/residency document number
- date of creation of PNR
- a notation that the person arrived at the departure gate with a ticket but without a reservation for the flight (if applicable)
- names of travel agent/agency that booked the flight
- date of issue of ticket
- a notation that the person exchanged their ticket for the flight (if applicable)
- travel itinerary
- the name of the operator of the aircraft
- destination
- seat assignment
- number of pieces of baggage
- tag numbers on baggage
- stated seat requests
- PNR number
- phone number
- address
- method of payment
- a notation that the ticket was paid for by another person (if applicable)
- a notation that there are gaps in the person's itinerary that necessitate travel by an undetermined method, etc.[326]

Although the wording of the Act suggests that the authorities may request this information as it concerns a particular specified person or as it concerns all the passengers on a specified flight, the federal Privacy Commissioner, the RCMP, CSIS, and other government officials all claim that the intention of s.4.82(4) and (5) was that the

[326] A complete list of data elements can be found in the Schedule of the *Aeronautics Act.*

authorities should receive a continuous data feed from the airlines regarding all passengers for all flights.[327]

The Minister of Transport, officers of the Department of Transport, and the Commissioner/officers of the RCMP may request this information for the purposes of transportation security, and the Director/officers of CSIS may request this information for the purposes of transportation security and investigation of "threats to the security of Canada" as defined in the *Canadian Security Intelligence Service Act*. Furthermore, s.4.82(2) and (3) allow the RCMP and CSIS to match the information collected with any other information in their control, and s.4.82(6) allows all of the aforementioned authorities in the RCMP and CSIS to share with each other all information collected under s.4.82 as well as all information obtained as a result of matching the collected information with other information. Subsections 4.82(7), (8), (9), and (10) allow RCMP and CSIS authorities to disclose collected information and information obtained as a result of matching to various entities, including the Canadian Air Transport Security Authority, peace officers, any employee of CSIS, air carriers and aircraft protective officers, for various purposes such as transportation security and immediate threats to the "life, health, or safety of a person."

Subsections 4.81(6) and (7) require the Minister of Transport/Department of Transport officers to destroy information obtained under s.4.81 within 7 days, while s.4.82(14) requires RCMP and CSIS authorities to destroy information obtained or shared with each other under s.4.82 within 7 days, *unless* it is reasonably required for transportation security or investigations of "threats to the security of Canada." If information is kept for these purposes, a record must be kept setting out the reasons for retention. Lastly, s.4.83(1) allows airlines operating aircraft that are to land in a foreign state to disclose to authorities in the foreign state any information in its possession relating to persons on board that is required by the laws of the foreign state, despite sections 5 and 7(3) of *PIPEDA*.

Another statute relevant to the sharing of information between airlines and government is the *Immigration and Refugee Protection Act (IRPA)*. Subsection 148(1)(d) requires airlines to provide, according to the regulations, prescribed information (to Citizenship and Immigration Canada.) Section 149 provides that information obtained under s.148(1)(d) can be used to identify a person for whom a warrant of arrest has been issued, and that the person to whom the information relates must be given notice. Subsection 150.1(1)(b) states that the regulations may provide for any matter relating to the disclosure of information for the purposes of national security, the defense of Canada or the conduct of international affairs.

---

[327] Legislative History of Bill C-7 (The Public Safety Act, 2002), available online at: http://www.parl.gc.ca/common/bills_ls.asp?Parl=37&Ses=3&ls=c7 (last accessed on February 7, 2008); the extent to which this is actually practiced is unclear. Whatever the present state of its implementation, if the intention of the section is continuous streaming of data, such continuous streaming of data may come to be regular practice by all airlines.

Under the *Immigration and Refugee Protection* (IRP) *Regulations* s.264, a transporter must provide, within 72 hours after the presentation for examination of a person carried by the transporter to Canada, any of the following documents as requested by an officer designated by the Minister of Citizenship and Immigration: a copy of the ticket issued to the person, the person's itinerary, number/type/country of issue of the travel document carried by the person, and name of the person to whom the travel document was issued. Subsection 269(1) states that transporters must provide, at the request of an officer designated by the Minister of Citizenship and Immigration, and on the departure of their vehicle from the last point of embarkation before arrival in Canada, the following information in writing on each person carried: full name, date of birth, citizenship/nationality/country of issue of travel document, gender, travel document number, and reservation record locator or file number. Subsection 269(2) provides that at any time after a transporter undertakes to carry a passenger to Canada, the transporter must provide an officer access to its reservation system or provide in writing all reservation information held by the transporter on passengers to be carried to Canada.

The *Protection of Passenger Information Regulations* were also created under the *IRPA*, specifically s.150.1. These regulations govern the Canada Border Services Agency's (CBSA) ability to access, retain and disclose API/PNR information. Section 3 provides that API/PNR information can be retained by the CBSA for the purpose of identifying persons who are/may be involved with/connected to terrorism or other serious transnational crimes. Section 4 provides that API/PNR information must be stored in the PAXIS system separately from each other. Section 5(1) states that API information may be retained for a maximum period of three years and six months after it is received, and access to it may be provided during that period to intelligence officials for the purposes in s.3 or for conducting trend analysis or developing future risk indicators in relation to the purpose in s.3, or to officials of the CBSA responsible for selecting persons for enhanced questioning with a view to identifying persons described in s.3. Section 5(2) restricts intelligence officials from using API information to gain access to PNR information about the same person during the first two years, unless such access is necessary for an investigation for the purpose in s.3, and during the latter one year and six months, unless such access is approved by the president of the CBSA. Section 6 provides that PNR information (which is more sensitive) may be retained for three years and six months, but access to it must be restricted in accordance with s.7. Section 7 provides that access to PNR information may be provided within the first 72 hours to intelligence officials and officials of the CBSA for the respective purposes aforementioned; from 72 hours to two years access to the name attached to the (now anonymized) PNR information may be given to intelligence officials if they require it for an investigation referred to in s.3, and access to the PNR information may be given to an intelligence official for conducting trend analysis or developing future risk indicators in relation to the purpose in s.3; from two years to three years and six months access to identifying data elements in the PNR may be provided to an intelligence official on approval of the president of the CBSA, and access to non-identifying data elements may be provided to intelligence officials for conducting trend analysis or developing future risk indicators in relation to the purpose in s.3.

Section 9 provides that the CBSA may disclose API/PNR information to any Canadian government department if a CBSA official has determined that the information relates to terrorism/crimes in s.3, is required to comply with a subpoena/warrant/order made by a court, or is required for judicial proceedings in Canada. Section 9 also requires the receiving department to provide the same protection for the information as the CBSA, and not to further disclose it without the CBSA's permission unless required to by law. Finally, s.10(2) allows the CBSA to disclose API/PNR information to a foreign state for purposes referred to in s.3, if the foreign state is an E.U. state or has received an adequacy finding under Article 25(6) of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and the free movement of such data, and if the CBSA only discloses the minimum data elements required for that purpose.

Another statute with privacy implications is the *Customs Act*. Subsection 107.1(1) allows the Minister of Public Safety and Emergency Preparedness, in prescribed circumstances, to require any prescribed person or class of persons to disclose prescribed information about any person on board a conveyance in advance of the arrival of the conveyance in Canada. Subsection 107.1(2) provides that information shall be disclosed under subsection (1) despite any restrictions in the *Aeronautics Act* on the disclosure of such information. Subsection 107(4) states that an official[328] may provide access to customs information if it will be used solely to prepare for criminal proceedings under any Act of Parliament, if it may reasonably be regarded as necessary for a purpose relating to the life, health or safety of an individual or to the environment in Canada or any other state, and if it is reasonably regarded by the official as relating to national security. Subsection 107(5)(o) provides that an official may provide access to customs information to "prescribed persons or classes of persons, in prescribed circumstances for prescribed purposes, solely for those purposes," among a list from a) to o) of other persons to which information may be given.

Lastly, *PIPEDA* s.5(3), s.7, and clauses 4.3, 4.3.3, 4.5, and 4.9 of Schedule 1 apply to information sharing by airlines, and s.8 of the Charter as well as the relevant case law apply to the collection of personal information by government authorities.

A review of the privacy policies of Air Canada and Westjet show that none of the above statutes and regulations are mentioned explicitly. The full extent of the privacy policies' reference to them is confined to general statements that the particular airline will not collect, use or disclose information without consent unless "required by law." There is no mention of the specific government entities that information will be disclosed to, how long those entities may retain passenger information, or the ways that information may be shared by the receiving authority with other government authorities.

---

[328] Section 107(1) of the *Customs Act* sets out that "official" has the broad meaning of any person who: (*a*) is or was employed in the service of Her Majesty in right of Canada or of a province; (*b*) occupies or occupied a position of responsibility in the service of Her Majesty in right of Canada or of a province; or (*c*) is or was engaged by or on behalf of Her Majesty in right of Canada or of a province.

In addition to Canadian law, U.S. law can also affect the privacy of Canadian travelers. In particular, s.215 of the *USA PATRIOT Act* allows the FBI to request a court order "requiring the production of any tangible things (documents, papers, records, books, etc.) relevant to an investigation of terrorism."[329] Technically this applies only to corporations that have an operation in the U.S.; however, airlines by their nature have operations spanning many countries and information on Canadian passengers collected by the Canadian side of an airline may end up in the airline's American operations, and from there in the hands of the FBI and other American authorities. Putting aside the effects of the *USA PATRIOT Act*, information on Canadian travelers can still end up in the U.S., even for trips entirely within Canada. This is a result of information-sharing agreements between the U.S. and Canada, such as the US/Canada Smart Border Initiative, which provides for an automated Canada-US API/PNR data-sharing program (in place since Spring 2003.)[330]

The *Report of the Events Relating to Maher Arar*, prepared by the Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar, provides further insight into the dynamics of airline disclosure/government collection of personal information. It outlines the broad approaches that the RCMP takes to collection and handling of personal information. The RCMP's approach to inclusion of personal information into its national security database (the Secure Criminal Information System or SCIS) is one of broad inclusion; the reasons for this being to ensure that investigative files are complete (including exculpating as well as inculpating evidence), to prevent reinvestigation of individuals who resurface numerous times in an investigation, and to avoid neglecting important information on which the nation's security rests.[331] The decision to include information in SCIS is made by the person entering it, and the criteria for inclusion are relevance and importance to an investigation.[332]

Because the approach to inclusion is so broad and inclusion depends on each person's subjective judgment (as opposed to a more objective set of rules), personal information with questionable relevance and import may end up in SCIS. Furthermore, the broad inclusion approach and its justifications may cause RCMP officers to probe deeper and wider when requesting personal information from airlines. For example, in the interests of completeness, officers may probe deeper into an individual's associations than is appropriate, and may even probe into the backgrounds of people who travel with or are otherwise connected to the person under investigation. Indeed, Maher Arar is an example of how innocent people connected with a person under investigation may fall victim to the investigative process.[333]

---

[329] *Supra* note 322 at p.125.
[330] *Ibid.*
[331] Dennis R. O'Connor, Commission of Inquiry in the Actions of Canadian Officials in Relation to Maher Arar, *Report of the Events Relating to Maher Arar, A New Review Mechanism for the RCMP's National Security Activities*, p.109, available online at www.ararcommission.ca/eng/EnglishReportDec122006.pdf (last accessed March 3, 2008).
[332] *Ibid.*
[333] Arar became a subject of investigation after he was spotted meeting Abdullah Almalki, a man targeted for investigation, at a café; a series of subsequent errors in investigative reports led to the flagging of Arar

The Federal Privacy Commissioner's Findings under *PIPEDA* also influence the way information is shared between airlines and government authorities. In case #62, a federal government department investigating its employee's use of sick leave requested that an airline confirm travel itinerary information about the employee. The government department made its request under s.7(3)(c.1)(iii) of *PIPEDA*, indicating that it was conducting a lawful investigation pursuant to a cited directive under the authority of a specific act, and that the request was for purposes of administering federal public servants' employment legislation, regulations, and policies. The airline disclosed the information, and the government employee brought a complaint. It was later discovered that the cited directive was incorrect; however the department demonstrated that it nevertheless had lawful authority to collect under other legislation. The Privacy Commissioner was satisfied that, ultimately, the government department did have lawful authority to collect its employee's travel information, but was concerned that the department had cited an incorrect authority and that the airline had failed to verify the authority's correctness. The Privacy Commissioner thus found that when faced with a request for personal information from government authorities, private organizations must not take the authority's submissions at face value; they must always independently confirm that the authority relied on is correct and authorizes collection of the information requested.

The two airline representatives interviewed were also asked about the kinds of information requests they receive from government authorities such as the RCMP and CSIS. Mr. Plimmer indicated that Westjet usually receives inquiries about whether a particular individual has flown on a certain flight on a certain date, whether there are reservation records on a particular individual, and whether Westjet can notify the government agency if a particular individual makes a booking in the future. He also indicated that Westjet receives a number of inquiries relating to fraud investigations, such as whether a person used a third party credit card to purchase a ticket (information which may also be relevant to a national security investigation.) The Director of Privacy (at the airline requesting anonymity) indicated that his airline receives few information requests (perhaps since this airline is smaller than Westjet), but that sometimes it gets requests from the authorities about whether a particular individual was aboard a certain flight. Like Westjet, this airline also receives inquiries relating to fraud, such as whether an individual was on vacation, and for how long (which would be relevant to, for instance, welfare fraud).

D) Formal and Informal Information Sharing Practices

In order to uncover the formal and informal information sharing practices of airlines, interviews were attempted with CSIS as well as privacy lawyers with knowledge of national security. Unfortunately, it is CSIS' policy not to talk in detail about its information collecting practices, and the privacy lawyers contacted were not able to give interviews. Therefore, all information on sharing practices was gleaned from the interviews with airline representatives.

---

as a terrorist and his eventual deportation; *Report of the Events Relating to Maher Arar, Factual Background, Volume 1*, p.52-53. *Supra*, note 332.

1) Formal Information Sharing

a) Westjet

With respect to formal information sharing, a conversation with a Westjet representative illuminated i) the procedure for processing information requests, ii) a policy of making verbal responses to requests unless there is a legal requirement for a written response, iii) circumstances under which Westjet may refuse requests iv) that the preponderence of requests for information are unaccompanied by warrants, and v) circumstances in which Westjet would share information at its own initiative.

According to Mr. Plimmer, the formal procedure for processing information requests from government authorities at Westjet is to refer the officer making the request to Westjet's Corporate Security Department, where it is verified that the officer is actually an officer, that the information is requested pursuant to an active investigation, and that the investigation is a matter of national security or administration of the law. Once this is done, the information requested is given to the officer by the department. Westjet also has a policy of only providing information verbally unless a legal requirement, such as a statutory provision or a warrant obtained by the authorities, requires it to provide information in writing.[334] The Corporate Security Department only refuses information requests if it cannot verify that the person requesting information is really an officer, if it cannot confirm an active investigation, or if the investigation is not a matter of national security or administration of law. Mr. Plimmer also indicated that Westjet receives requests for information that are unaccompanied by a warrant daily, and that they make up about 90% of all the information requests received by Westjet. He also said that Westjet would volunteer personal information to the authorities on its own initiative if it felt that there were aviation security issues that would be a threat to the airline, or if there was a potential violation of the law (such as if they received information that someone was smuggling drugs.)

b) A Smaller Anonymous Airline

The interview with the Director of the Privacy Office at the anonymous airline also provided insights into his airline's information sharing practices. The interview revealed i) a continuous data stream of API to government authorities, ii) requirements and procedures for requests iii) the limited circumstances under which this airline would disclose without judicial authorization or legislative mandate, and iv) a rarity of request that are unaccompanied by warrants, quite unlike the stream of requests received by Westjet.

---

[334] It is questionable how much of a difference this policy makes in reality, as there are a number of statutory provisions that expressly require airlines to provide information in writing. For example, s.269 of the *Immigration and Refugee Protection Regulations* explicitly requires commercial transporters to provide certain information in writing on each passenger on request of an officer, and the *Aeronautics Act* requires air carriers to provide the Department of Transport, the RCMP and CSIS with information in any manner specified by officials of these agencies. The broadness of these provisions means that airlines can only use discretion not to provide written information when the government official has not requested it.

The Director indicated that his airline currently provides a continuous data stream of API information on all passengers to government authorities and is in the process of setting up a continuous data stream of PNR information. Besides the data streams, all *ad hoc* requests for information must be in writing, and must be sent to the Director for consideration. The Director then verifies the identity of the officer, and confirms any court order, warrant, or legislative provision that authorizes the collection of the information. If all of the above is confirmed, the information will be given to the officer. If there is no authorizing court order, warrant, or legislative provision, or if it is obvious that the officer is engaging in a fishing expedition, the request for information will be declined; the only situation in which information will be given to the authorities without an authorizing court order, warrant, or legislative provision is when the Director is convinced that there is an imminent emergency.

However, according to the Director his airline receives very few *ad hoc* requests. He estimates that the airline has received two requests for information without a warrant in the last two years. Again, this may be because this airline is smaller than Westjet, or it may be because this airline already provides a continuous data stream to the authorities, lessening the need for *ad hoc* requests. Furthermore, the Director asserted that his airline would under no circumstances volunteer personal information to the authorities of its own accord.[335]

2) Informal Information Sharing

Neither of those interviewed were able to provide insight into informal information sharing that does not pass through the companies usual means of handling formal and informal requests from government authorities (formal being written and pursuant to a court order or other legal authority; informal being verbal requests). Most informal disclosures in response to informal law enforcement requests would presumably occur on the front lines with lower level airline employees. Anecdotal evidence provided to the author by a former customs agent at Vancouver International Airport suggest that staff often give out information to authorities on whether an individual is on a particular flight, due to the development over time of informal networks of personal contacts.[336] It is not known how often such informal sharing of this type may be occurring.

E) Gaps and Controversies

There have been many debates and controversies surrounding privacy issues in Canada and abroad, especially concerning the myriad of legislative measures and policies adopted by governments in response to 9/11. Among such controversies are 1) the PAXIS database, 2) the Passenger Protect Program commonly known as no-fly lists and 3) the deportation of Maher Arar by the US government.

---

[335] Presumably the Director is referring to *ad hoc* volunteering of a particular individual's personal information, separate from the continuous data streams that his airline provides to the authorities regularly.
[336] *Supra* note 322 at p.121.

1) The PAXIS Database

Notable was the controversy surrounding the proposed Canada Customs and Revenue Agency (CCRA) database, now the PAXIS database controlled by the newly created CBSA.[337] At the time the database was still under the mandate of the (now defunct) CCRA, there was a debate involving an opinion written by retired Justice La Forest for the Privacy Commissioner of Canada on the constitutionality of the proposed database. In his opinion Justice La Forest concluded that the database's digital form threatens privacy by allowing officials to use API/PNR data, either alone or in conjunction with information from other databases, to infer personal information such as race, ethnicity, religion, and national affiliation of passengers. This information would allow officials, consciously or unconsciously, to engage in racial profiling.[338] Also, since the API/PNR information of *all* passengers entering Canada would be entered into the database, Justice La Forest concluded that it would violate s.8 of the *Charter* as it violates a reasonable expectation of privacy in the movements of individuals without prior authorization or any individualized suspicion.[339] A further problem with the new scheme is how it interacts with the *Customs Act*. Under the broad wording of s.107, customs officials can disclose API/PNR information in the database to wide classes of persons,[340] for a variety of vaguely specified purposes. Combined with the broadness of collection criteria (all passengers entering Canada), the *Customs Act* can result in mass breaches of personal privacy. Other criticisms leveled at the new database include the inadequacy of the anonymization of the information after the first 72 hours. According to privacy lawyer Michael Power, the anonymization process consists of taking names off records, mapping them to numbers and then storing them in a separate database. Mr. Power points out that it is only one more step to go through, and does not provide adequate protection.[341]

2) Passenger Protect Program

Another significant debate is the one concerning the Passenger Protect Program, or the Canadian "no-fly" list. This program has its legislative basis in the *Aeronautics Act* s.4.81, which allows the Minister of Transport to specify persons who are a threat to aviation security and to require airlines to provide information on those persons.

The *Aeronautics Act* s.4.71 and s.4.9 also gave rise to the *Aeronautics Act Identity Screening Regulations*, which require airlines to inform the Minister when a possible match to a listed person is identified.[342] Section 3 of the Regulations require air carriers to screen persons age 12 or older by comparing his/her name to the names on the

---

[337] See *Protection of Passenger Information Regulations* above for details on the regulation of information in the PAXIS database.
[338] *Supra* note 321 at p.462.
[339] *Supra* note 321 at p.469.
[340] E.g. s.107(5)(b): "a person that is… legally entitled to the information by reason of an Act of Parliament, solely for the purposes for which that person is entitled to the information."
[341] Michael Power, "Security and freedom: are the government's efforts to deal with terrorism violative of our freedoms?" Canada-United States Law Journal, (2003) 29 Can.-U.S. L.J. 331-337
[342] Transport Canada Passenger Protect Program Page, available online at: http://www.tc.gc.ca/vigilance/sep/passenger_protect/menu.htm (last accessed on February 7, 2008).

specified persons list before issuing a boarding pass. If the person's name matches, the air carrier is required to compare the person's date of birth and gender (as shown on the person's government-issued identification) to the date of birth and gender shown for the listed person. If there is a match, the airline must immediately contact the Minister for confirmation of identity and a decision whether to board or not to board the individual.

When the Minister of Transport receives notice of a match from an airline, s.4.76 and s.4.77 of the *Aeronautics Act* authorizes him or an officer designated by him to issue Emergency Directions prohibiting boarding of the specified persons if he is of the opinion that there is an immediate threat to aviation security. When an Emergency Direction is issued, Transport Canada notifies the RCMP and police having local jurisdiction are informed and take action as required.[343] Furthermore, the *Aeronautics Act* s.4.81(3) authorizes Transport Canada to share information received from airlines with the Minister of Citizenship and Immigration, the Minister of Public Safety and Emergency Preparedness, the Chief Executive Officer of the Canadian Air Transport Security Authority, persons designated by the Commissioner of the RCMP, and persons designated by the Director of CSIS for the purposes of transportation security.

Any person denied boarding is given access to a reconsideration process through Transport Canada's Office of Reconsideration.[344] In addition, Transport Canada has adopted guidelines for the listing of persons, guidelines which are used to inform an Advisory Group created to make recommendations to the Minister for listing of persons.

Under the guidelines, a person will be recommended for listing if:

> - he/she is or has been involved in a terrorist group, and can be reasonably suspected to endanger aircraft, aerodromes or the safety of passengers, crew or public;
>
> - he/she has been convicted of serious and life-threatening crimes against aviation security;
>
> - he/she has been convicted of serious and life-threatening offences and may attack or harm an air carrier, passengers or crew members.

Despite the guidelines, there is no automatic inclusion or exclusion of an individual based on any single factor or combination of factors. Each case is decided on its own merits, and the Minister of Transport will make the ultimate decision to include a person in or remove him from the list.

The decision of the Ministry of Transport is based on information received from Canadian security and intelligence agencies, which may include information originating from foreign and/or multilateral intelligence and law enforcement agencies (such as INTERPOL), including information concerning individuals that are on the U.S.

---

[343] *Ibid.*
[344] *Ibid.*

Transportation Security Administration "No Fly List."[345] To address the possibility of false matches, Transport Canada has taken steps to reduce the risk by including date of birth and gender on the list, which makes matching more accurate; by reviewing and refreshing the list every 30 days; by limiting the scope of the list to aviation security; by requiring the final decision regarding boarding to be made by the Minister, not the airline; and by providing a reconsideration process. As well, risk mitigation measures suggested by stakeholders and the Office of the Privacy Commissioner await consideration and possible incorporation into the Passenger Protect Program.[346]

The Passenger Protect Program has come under criticism because Canadian law does not provide criteria or procedures for putting people on the list (even though Transport Canada has guidelines for listing), and does not define and circumscribe how the list works. The law also fails to give persons listed an enforceable right to appeal the listing or a right to seek redress (although they can attempt an appeal at the transport department's reconsideration office, or petition Federal Court for a review). There is no right of persons to know why they have been listed, and there is no assurance that the list will not be shared with foreign governments.[347] The no-fly list is also open to abuse, as it is to be widely distributed to airlines and there is no guarantee that state-owned airlines will not give the list to its government.[348] One can also foresee potential problems with the Passenger Protect Program by looking at the problems encountered by the U.S. concerning its no-fly list. One such problem is that when two individuals have the same name, the government will need more information about those individuals to differentiate them and to accurately match them to the list; it is difficult to define how deeply the government should be able to dig, and there is a chance of a slippery-slope situation occurring. As well, the growing size of the list has resulted in a growing number of false positives.[349] Despite the Passenger Protect Program's safeguards against false positives (the efficacy of which is limited if not questionable,) it is not unlikely that the same problem can occur in Canada.

A third major debate about privacy and the consequences of its violation surrounds the deportation of Maher Arar by the U.S. government. The incident was caused by the RCMP sharing erroneous information about Arar with U.S. authorities – the result of failure to follow RCMP policies requiring screening of information for relevance, reliability and irrelevant personal information, and attachment of written caveats to shared information.[350] After being spotted with a man who was under investigation for terrorism, Arar was labeled a "person of interest" by investigators; subsequently,

---

[345] *Ibid.*
[346] *Ibid.*
[347] "Fixing Canada's Flawed No-Fly List", available online at: http://www.thestar.com/comment/article/231102 (last accessed on February 7, 2008).
[348] Richard Brennan,**"**No-fly list open to abuse, Air India inquiry warned", available online at: http://www.thestar.com/article/222052 (last accessed on February 7, 2008).
[349] "Air-Travel Prescreening Is Laden With Baggage" Congressional quarterly weekly report [0010-5910] au:Yoest yr:2006 vol:64 iss:42 pg:2907, available online at: (http://www.airportbusiness.com/web/online/Airline-and-Airport-Security-News/Air-Travel-Prescreening-Is-Laden-with-Baggage/5$8978) (last accessed on February 7, 2008).
[350] *Supra* note 330 at p.39.

numerous errors in the investigators' reports eventually resulted in the labeling of Arar as "target," "suspect," "principal subject," etc., and ultimately "Islamic extremist." This failure to distinguish labels resulted in misinformation being shared with U.S. authorities, leading to Arar's deportation.[351]

The Deputy Commissioner of the RCMP testified before the Arar Commission that if an individual is seen with a person under investigation, a field officer can enter that individual into the security intelligence system without receiving specific authority to do so; thereafter the information can be freely shared with other agencies, including foreign agencies, and the individual would have no awareness of his/her status in the intelligence gathering process – making him/her powerless to remove his/her information from the databases.[352] The case of Maher Arar illustrates the many junctures at which errors can be made in a government investigation. This makes the Passenger Protect Program all the more worrisome, as potential for mistakes during investigations and intelligence-gathering translates into potential for mistakes on the no-fly list. Furthermore, the fact that the no-fly list may be shared with foreign governments, whether by the Canadian government or by state-owned airlines that have access to the list, compounds the potential for violation of an innocent individual's privacy, or worse – even though the Canadian Passenger Protect Program purports to limit the use of the list to aviation security purposes, there is no guarantee that foreign governments will limit their use of the list in the same way.

F) Conclusions and Recommendations

The problem of balancing individual privacy interests with the public national security interest is a difficult one, as both are vital interests worthy of protection in a free and just society. In order to protect national security, some compromise of privacy rights is inevitable. However, the balance of these two interests in current law and practice create the potential for infringement of privacy rights beyond that which can be justified in the name of national security. To correct this, changes must be made both in the legislation and in the daily practices of airlines. The following recommendations are an attempt at maintaining an appropriate level of privacy protection while keeping in mind the necessity of not unduly hampering the government's investigative efforts.

Recommendation 1: Legislated mandatory collection and disclosure requirements should be amended to clarify and specify conditions that must be met before an officer can compel an airline to disclose personal information.

One problem with the legislation regulating information sharing between airlines and government is that even if an airline earnestly wanted to protect its customers' privacy, it will be hard pressed to do so when faced with the requirements of various legislative provisions. For example, the *Aeronautics Act* s.4.81 and s.4.82 requires airlines to provide information to Transport Canada, CSIS or the RCMP at the request of an officer,

[351] W.R. Stephen, "The Arar Affair", *HS Today*, April 1, 2007, available online at http://hstoday.us/index.php?option=com_content&task=view&id=654 (last accessed March 3, 2008).
[352] Parliamentary review of the ATA, 38th Parliament, 1st Session, Sept. 21, 2005.

with no mention of the necessity of a warrant or court order. Similarly, under the *Customs Act* s.107.1(1) the Minister of Public Safety and Emergency Preparedness may require airlines to provide information about any passenger, again without any mention of prior authorization or any specified conditions for collection of information. Since these provisions make disclosure of information mandatory, airlines have little choice but to comply, even absent any proof that the collection is justified. To correct this problem, these provisions should be amended to specify conditions that must be met before an officer can compel an airline to disclose personal information. Only then can one begin to focus on the information sharing practices of individual airlines and their adequacy in terms of privacy protection.

Recommendation 2: The legislative provisions relating to disclosure to the PAXIS database should be clarified to specify the conditions for disclosure.

A second threat to privacy is the PAXIS database. Subsections 107(4) and 107(5) of the *Customs Act*, which allow officials to provide customs information to a variety of individuals and for a variety of purposes, should be clarified as follows. Subsections 107(4)(e) (which allows an official to provide customs information if he/she regards it as necessary for a purpose relating to the life, health or safety of an individual or to the environment in Canada or any other country) and 107(4)(h) (which allows an official to provide customs information if he/she regards it to be information relating to the national security or defence of Canada) should be made more specific, i.e. for ss.107(4)(e) "necessary" should be defined and specific purposes should be identified, while for ss.107(4(h) specific examples of "information relating to the national security or defence of Canada" should be included. Making these provisions less vague reduces the chance that information in PAXIS can be shared for any arbitrary purpose. As well, s.107(5)(o) (which allows an official to provide customs information to "prescribed persons or classes of persons, in prescribed circumstances for prescribed purposes, solely for those purposes") should be clarified to specify which persons and circumstances are prescribed.

Recommendation 3: Continuous data streaming should not be the norm.

A third recommendation is to stop all continuous data streaming from airlines to government authorities. The streaming of API and PNR information on all passengers entering Canada presumably facilitates fishing expeditions by the authorities even more than if they were merely allowed to "pull" information from the airlines on an *ad hoc* basis. In fact, streaming would eliminate the need to fish (at the airlines), as the authorities may already have all or most of the information they could want from the API and PNR. Furthermore, when information about all passengers is streamed regularly there is no way to know which individuals the authorities are scrutinizing and how they are doing it, while individual information requests at minimum reveal the government's targets of investigation and perhaps leave some trail of accountability. Lastly, continuous streaming of API and PNR information does not accord with the plain meaning of the words of the *Aeronautics Act* s.4.82. It is somewhat of a mystery how the section could have been interpreted as intending continuous data streaming; however, if it is correct that the intention of the section is as such, then the section should be amended to include

express language indicating that it is providing for *ad hoc* information requests. In addition, all PNR information disclosed (whether as part of a stream or pursuant to an *ad hoc* request) should first be purged of all special meal and health information, if that is not being done currently. This may help reduce racial/religious profiling on the part of investigators, and make the PAXIS database slightly less intrusive on privacy.

Recommendation 4: Safeguards should be put in place to ensure the accuracy and minimize imprecision of the Passenger Protect Program.

In regard to the Passenger Protect Program, it may not be warranted to abolish the program completely, as it is arguable that the danger of letting even one potential terrorist onto a plane is too great. However, a number of safeguards should be put in place to protect individual privacy and to reduce the probability of false listing and false matches. First and most importantly, clear, objective criteria (to the extent possible) for inclusion on the no-fly list should be created through the cooperation of investigative authorities and privacy advocates, and updates of the list should be conducted regularly. Second, official limits should be created on the kinds of information that Transport Canada may use to distinguish two people with the same name for the purposes of matching. As well, additional items of information such as address and phone number should be required to confirm a match with a listed person, as name, date of birth and gender may still lead to false matches in some cases. Fourth, listed persons should be given an enforceable legal right to know why they have been listed, to appeal the listing, and to seek redress for being falsely listed, and they should be able to exercise these rights within a reasonable time after being listed. Lastly, the Canadian government should attempt to keep the list out of the hands of governments that do not share the same respect for human rights and due process. It should refrain from sharing the list with those governments, and attempt to prevent state-owned airlines of those countries from sharing the list with their governments on pain of sanction under Canadian law or by some other method. These recommendations do not solve all the problems of the Passenger Protect Program, but they may go some way in reducing the risk of violation of individual rights to an acceptable level.

Recommendation 5: Airlines should adopt policies to discourage informal information sharing between airline staff and government.

Finally, there are some practices that airlines may adopt to enhance passenger privacy. To reduce the likelihood of informal information sharing between airline staff and government, airlines should attempt to minimize contact between government officers and front line staff; less contact means less opportunity for informal relationships and networks to form. The “no verbal requests” policy of the anonymous airline, whose Director of Privacy was interviewed for this report, may be a viable method of achieving this goal. Requiring all information requests to be in writing and to be sent directly to the department that handles privacy issues bypasses front line workers who may otherwise interact with the same officers repeatedly. It also may reduce the risk of relationships developing between government officers and airline staff in the privacy department, since requests in writing have less of a personal dimension than verbal, in-person requests.

Secondly, airlines should refrain from giving any information, verbal or written, to authorities upon request absent a warrant, court order or mandatory legislative requirement.[353] Airlines should also only volunteer personal information to the authorities if it feels, based upon some tangible evidence, that there is a real and imminent danger to public safety. Finally, all airlines should have an online privacy policy explaining the potential disclosures that may be made of passenger information, or some other easily accessible form of its privacy policy. Privacy policies should attempt to explain in more detail what is actually "required by law," i.e. they should indicate the specific agencies that information may be disclosed to, and lay out in plain language some of the most relevant legislative provisions concerning information sharing (such as the *Aeronautics Act* s.4.81 and s.4.82.)

Although from the limited evidence gathered for this report there is little direct indication that any substantial violation of privacy rights is occurring on a regular basis, the recommendations above are designed to address the problems which may or may not exist on a wide scale but which we, for the most part, cannot see. Whatever the reality may be behind government investigations, it is hoped that making the changes recommended above will give individual privacy rights as well as the public national security interest greater protection, by ensuring that the authorities and airlines follow practices which promote the investigation of true terrorists rather than innocent bystanders.

[353] Again, this recommendation rings hollow unless certain legislative provisions requiring unconditional disclosure of information upon request are amended or repealed.

Appendix I: Information Typically Collected in the Retail Sector[354]

- Household health information (e.g. households where at least one member has experienced ADHD, arthritis, bedwetting, depression, diabetes, heart or kidney disease, high blood pressure or cholesterol, lactose intolerance, macular degeneration, migraines, neck pain, nut allergies, urinary tract and yeast infections)
- Marital status
- Credit card holders / users
- High net worth individuals with discretionary funds
- Gender
- Age
- Household income—both annual and monthly
- Race and ethnicity
- Geography
- Household occupants (whether the person has children)
- Telephone number
- Occupation
- Level of education
- Whether the person is likely to respond to "money-making opportunities"
- Homeownership
- Product ownership
- Diet
- Hobbies (whether and what the person collects)
- Religion (affiliation and denomination)
- Length of time spent residing at current residence, and type (e.g. house, apartment, condominium, trailer)
- Type of automobile owned
- Holders of loans for high-end automobiles
- Frequent air travelers (including destination and class of ticket purchased)
- Habits (smoking, drinking)
- Contributions to political, religious, and charitable groups
- Shopping preferences
- Pet ownership and type
- Interests (including gambling, arts, antiques, astrology, technology)
- Book, magazine and music preferences
- Membership in book, video, tape, and compact disc clubs
- Whether the person responds to direct mail solicitations
- Online and mail order purchases and type

[354] List reproduced from Lawson, Philipa. *On the Data Trail: How Detailed Information About You Gets Into the Hands of Organizations with Whom You Have No Relationship – A Report on the Canadian Data Brokerage Industry* (2006) at page 27, available online at: http://www.cippic.ca/en/news/documents/May1-06/DatabrokerReport.pdf (last accessed on January 31, 2008).

Appendix II: Author Biographies

- **Tamir Israel:** Third year JD student at the University of Toronto, Faculty of Law. Tamir worked for the Law Courts Education Society of British Columbia on a research project regarding Aboriginals and criminal justice system in summer of 2006. He will be articling with the Canadian Internet Policy and Public Interest Clinic in 2008-2009.

- **Ali Mian**: Second year student in the JD program at the University of Toronto, Faculty of Law. Ali has done research as a political science student on information sharing between government departments.

- **Aba Stevens:** Second year JD student at the University of Toronto, Faculty of Law. Aba plans to pursue criminal law as a focus, and has an undergraduate degree in International Relations. In addition to authoring the Telecommunications Industry section of this report, Aba also served as the report's editor, weaving together the various reports, drafting the Introduction from the various contributions of the other three student researchers, and drafting the Executive Summary.

- **Michelle Yau:** Third year JD student at the University of Toronto, Faculty of Law. Michelle led the Anti-Human Trafficking Working Group of the International Human Rights Program in 2006-2007, and has focused her course work this year on privacy issues.

Supervisor:

- **Dr. Andrea Slane:** Executive Director of the Centre for Innovation Law and Policy, University of Toronto, Faculty of Law. Andrea received her J.D. (honours) from the University of Toronto in 2003 and practiced intellectual property, privacy and technology law before returning to the Faculty in 2006. She has a PhD in Comparative Literature, and has written on privacy related topics such as unsolicited bulk email and the privacy interests of the subjects of photographs and other visual representations. She has chaired two international symposia on Online Child Exploitation on behalf of the CILP, in 2005 and 2007.