Me Antoine Aylwin
National Privacy and Information Protection Group
Special thanks to Renee Darisse

K.C. Halm | Davis Wright Tremaine LLP

Transborder Data Flow: Should Canadians Fear the Patriot Act?

2007 Young Lawyers Division Spring Joint Conference
American Bar Association & Young Bar Association of Montreal
Montreal, May 4, 2007

FASKEN MARTINEAU

Canada → *Personal Information* → **U.S.A.**

Examples: Outsource employee information for treatment (payroll)
Transfer customer information to parent company

FASKEN MARTINEAU

INTRODUCTION

- Recent events have shown concerns that American laws respecting the collection, use and protection of personal information, notably the USA PATRIOT Act and the International Traffic in Arms Regulations (ITAR), may impact personal information of Canadians.
- While the federal and provincial governments endeavor to attenuate the implications of transborder data flow in relation to the privacy rights of Canadians, this concern is always kept in mind where personal information is transferred outside of Canada.
- Given the economic and political realities of a global economy, coupled with the constant evolution of information technology, serious questions are being constantly raised as to the protection of personal information.
- What is the legal framework for transborder data flow from Canada to United States in the private sector?

In the news…

Expro Tec

- Employees of Expro Tec, of Salaberry-de-Valleyfield, reached an agreement to avoid being subject to the application of the USA Patriot Act.
- Employees convinced their employer to take measures to prevent their personal information from being sent to the United States (parent company), which could then be subject to American laws respecting access to personal information.

In the news…

Bell Helicopter

- Bell Helicopter, for its part, was compelled to transmit personal information on its employees to the U.S. government, more specifically their nationality, under the U.S. International Traffic in Arms Regulation ("ITAR").
- One effect of ITAR would be to prevent businesses that agree to do business with the U.S. government from having employees with the nationality of any of the countries that the American government deems suspect.
- Consequently, several employees of Bell Helicopter in Canada were fired due to these requirements.
- Bell Helicopter must now deal with proceedings before the Québec Human Rights Commission, invoking illegal discrimination because of its decision.

In the news…

Royal Bank of Canada and U.S. dollar bank accounts

- In January 2007, it was reported in the media that since April 2006, RBC had been refusing to open U.S. dollar accounts for Canadians of dual nationality with Iran, Iraq, Cuba, Sudan, North Korea and Myanmar (formerly Burma). It was also reported that RBC had closed a small number of pre-existing accounts in order to comply with U.S. regulations. Later, RBC clarified that dual citizens could open U.S. dollar accounts if they meet the "Know Your Client" and "Anti-Money Laundering rules" that include proof of residency in Canada.
- Complaints were lodged with the Canadian Human Rights Commission alleging discrimination.
- The U.S. Department of Treasury instituted new anti-terrorism rules after the attacks of September 11, 2001 that attempt to combat money laundering and terrorism financing. Foreign banks that fails to comply with the regulations could be fined or banned from offering U.S. dollar accounts.

Legal framework of Privacy Legislation in Canada

- Canada is a federation composed of ten provinces and three territories.
- Under sections 91 and 92 of the *Constitution Act 1867*, the power to enact laws is distributed between the federal and provincial governments. In addition to its power to enact legislation within the classes of subjects over which it has exclusive jurisdiction, the federal government has residual power to "make laws for the peace, order, and good government of Canada," in relation to all matters not coming within those assigned exclusively to the legislatures of the provinces.
- Both the federal and provincial governments have legislated in the area of privacy in the private sector
- See *Air Canada v. Constant*, 2003 IIJCan 1018 (S.C.) (Pending in Appeal, 2003-10-02) for more details on the respective jurisdictions.

Legal framework of Privacy Legislation in Canada

- After the coming into force of the federal *Personal Information Protection and Electronic Documents Act* ["PIPEDA"] in January 2004, unless an organization is conducting business exclusively in one province and is exempted by an Order in Council under paragraph 26(2) of *PIPEDA*, both federal and provincial privacy laws are applicable to the organization.
- Alberta, Québec and British Columbia companies, other than federal works, undertakings or businesses, are exempt from the application of *PIPEDA* under specific orders in respect of the collection, use and disclosure of personal information that occurs within the province.
- Ontario "health information custodians", other than federal works, undertakings or businesses, are exempt from the application of *PIPEDA* under a specific order in respect of the collection, use and disclosure of personal information that occurs within the province regarding health information.

Legal framework of Privacy Legislation in Canada: Federal level

Personal Information Protection and Electronic Documents Act S.C. 2000, c. 5 [PIPEDA]

- *PIPEDA* applies to every organization in respect of personal information
  - a) **collected**, **used** or **disclosed** in the course of commercial activities and
  - b) about an employee of an organization collected, used or disclosed in connection with the operation of a federal work, undertaking or business (telecommunication, banking, postal service, etc…)
- Applicable to organizations located in provinces and territories where there is no exemption for similar legislation.
- Applicable to all personal information in all interprovincial and international data flow by all organizations in the course of their commercial activities.
- Section 5 of *PIPEDA* requires every organization to comply with the obligations set out in Schedule 1 of the Act, which lists 10 principles.

Legal framework of Privacy Legislation in Canada: Federal level

10 principles of Schedule 1 (National Standard of Canada):

Accountability

Identifying purposes

Consent (implicit or explicit)

Limiting collection

Limiting use, disclosure and retention

Accuracy

Safeguards

Openness

Individual access

Challenging compliance

Legal framework of Privacy Legislation in Canada: Federal level

- Section 7(3) of the Act provides exceptions to the general rules in Schedule 1 that a disclosure of information be done after a consent of the concerned individual and related to other purposes.
- Notable instances where an organization can disclose information without the knowledge or consent of the individual:
  - To comply with a subpoena or a warrant;
  - To a government institution where the information relates to Canada national security or the conduct of international affairs;
  - To a government institution where the disclosure is requested for the purpose of enforcing Canadian or foreign laws, an investigation under such laws or the gathering of intelligence for the purposes of enforcement;
- Outsourcing is considered to be a “use”, not a “disclosure”.

Legal framework of Privacy Legislation in Canada: Provincial level

- Québec: *An Act Respecting the Protection of Personal Information in the Private Sector* (1994)
- Alberta: *Personal Information Protection Act* (2003)
- British Columbia: *Personal Information Protection Act* (2003)
- Those three provinces account for less than half of the canadian population (StatCan, 2005);
- Ontario: *Personal Health Information Protection Act* (2004)
- *Similar principles that Pipeda, but some provisions worth mention regarding transborder data flow, because both acts may apply.*

Québec – *An Act Respecting the Protection of Personal Information in the Private Sector*

- The Québec legislator reacted to recent developments in the protection of personal information (including the USA PATRIOT ACT) in June 2006 with amendments to this Act (Bill 86).
- **Section 17 reads:**

> *17. Every person carrying on an enterprise in Québec who communicates personal information outside Québec or entrusts a person outside Québec with the task of holding, using or communicating such information on his behalf must first take all reasonable steps to ensure*
>
> *1) that the information will not be used for purposes not relevant to the object of the file or communicated to third persons without the consent of the persons concerned, except in cases similar to those described in sections 18 and 23;*

Québec – *An Act Respecting the Protection of Personal Information in the Private Sector*

2) in the case of nominative lists, that the persons concerned have a valid opportunity to refuse that personal information concerning them be used for purposes of commercial or philanthropic prospection and, if need be, to have such information deleted from the list.

If the person carrying on an enterprise considers that the information referred to in the first paragraph will not receive the protection afforded under subparagraphs 1 and 2, the person must refuse to communicate the information or refuse to entrust a person or a body outside Québec with the task of holding, using or communicating it on behalf of the person carrying on the enterprise.

Québec – *An Act Respecting the Protection of Personal Information in the Private Sector*

- **Section 18 reads:**

  A person carrying on an enterprise may, without the consent of the person concerned, communicate personal information contained in a file he holds on that person

  (4) to a person to whom it is necessary to communicate the information under an Act applicable in Québec or under a collective agreement;

  6) to a person or body having the power to compel communication of the information if he or it requires it in the exercise of his or its duties or functions;

Québec – *An Act Respecting the Protection of Personal Information in the Private Sector*

- **Section 20 reads:**

  In the carrying on of an enterprise, authorize employees, mandataries or agents or any party to a contract for work or services may have access to personal information without the consent of the person concerned only if the information is needed for the performance of their duties or the carrying out of their mandates or contracts.

- **Outsourcing is considered to be a "disclosure".**

Québec – *An Act Respecting the Protection of Personal Information in the Private Sector*

- *22. A person carrying on an enterprise may, without the consent of the persons concerned, communicate a nominative list or any information used to establish such a list to a third person, if*
  - *1) the communication is made pursuant to a contract that includes a stipulation prohibiting the third person from using or communicating the list or the information for purposes other than commercial or philanthropic prospection;*
  - *2) prior to the communication, in cases where the list is a nominative list of the person's clients, members or employees, the persons concerned are given a valid opportunity to refuse that the information be used by a third person for purposes of commercial or philanthropic prospection; and*
  - *3) the communication does not infringe upon the privacy of the persons concerned.*
- *A nominative list is a list of names, telephone numbers, geographical addresses of natural persons or technological addresses where a natural person may receive communication of technological documents or information.*

Alberta – *Personal Information Protection Act*

- Under section 19, an organization, as defined in the Act, may disclose personal information only for purposes that are reasonable, and only to the extent that is reasonable for meeting the purposes behind disclosing the information.
- The Act also provides a list of exceptions (section 20) to the general rule that disclosure of personal information requires the consent of the individual concerned. These include for example:
  - Compliance with a subpoena, warrant or order;
  - Disclosure in accordance with a treaty that authorizes or requires disclosure;
  - Disclosure to a public body or a law enforcement agency in Canada to assist in an investigation;
- Outsourcing is considered to be a “use”, not a “disclosure”.

Alberta – *Personal Information Protection Act*

- There is a special provision on the disclosure of employee information by an organization at section 21. Disclosure of employee information without their consent is permitted if
  - The individual is or was an employee of the organization, or
  - The disclosure of the information is for the purpose of recruiting a potential employee, and
  - The disclosure is reasonable for the purposes for which the information is being disclosed, is employment-related and the organization has provided the individual with reasonable notification of the disclosure to an actual employee and its purposes prior to actually disclosing the information.
- Section 22 permits disclosure of personal information in a context of the acquisition of a business.

British Columbia – *Personal Information Protection Act*

- Under section 6, consent of the individual is always required prior to the collection, use or disclosure of personal information unless otherwise authorized by the Act, or unless the Act deems the collection, use or disclosure to be consented to by the individual concerned.
- The Act also provides a list of exceptions (section 18) to the general rule that disclosure of personal information requires the consent of the individual concerned. These include for example:
  - In the context of an investigation or proceedings where the knowledge of the individual could compromised it;
  - Disclosure in accordance with a treaty that authorizes or requires disclosure;
  - Compliance with a subpoena, warrant or order;
  - Disclosure to a public body or a law enforcement agency in Canada to assist in an investigation;

British Columbia – *Personal Information Protection Act*

- Section 18 (2) recognizes the outsourcing of personal information:
  - (2) An organization may disclose personal information to another organization without consent of the individual to whom the information relates, if
    - (a) the individual consented to the collection of the personal information by the organization, and
    - (b) the personal information is disclosed to the other organization solely
      - (i) for the purposes for which the information was previously collected, and
      - (ii) to assist the other organization to carry out work on behalf of the first organization.
- Outsourcing is considered to be a "disclosure".
- Section 19 permits to otherwise disclose employee personal information without consent, but with a prior notification.
- Section 20 permits disclosure of personal information in a context of the sale of an organization or business assets.

Recent trends in transborder data flow

- *Groupe Jean Coutu v. Deschênes*
- Federal Privacy Commissioner ruling #313
- Federal Privacy Commissioner ruling #333
- Federal Privacy Commissioner ruling #365
- RBC and U.S. dollar bank accounts

Recent trends

*Groupe Jean Coutu v. Deschênes** (Québec)

- This decision interprets section 20 of the *Act Respecting the Protection of Personal Information in the Private Sector*. Mandataries (agents) may access personal information without the consent of the individual concerned where the following additional conditions are present:
  - The contract between the enterprise and the mandatary is in writing;
  - The contract specifies:
    - The scope of the mandate;
    - The purposes for which the mandatary (agent) would use the information;
    - The category of individuals who would have access to the information; and
    - The obligation to keep the information confidential.

* [2001] C.A.I. 210

Recent trends

Privacy Commissioner ruling #313, October 2005

- A Canadian bank (CIBC) sent a notification to its VISA customers that amended its credit cardholder agreement to provide for the use of a service provider located in the U.S. and the possibility that U.S. law enforcement or regulatory agencies might be able to obtain access to cardholders' personal information under U.S. law.
- The CIBC did not allow customers to opt-out where CIBC used an outside company to process personal information.
- The complaints made to the Privacy Commissioner were based on an objection to the possible scrutiny of personal information by the U.S. authorities under the guise of intelligence gathering.
- The issue to be decided was whether CIBC had complied with *PIPEDA*.

Recent trends

Privacy Commissioner ruling #313 (cont'd)

- The Assistant Privacy Commissioner ruled as follows:
  - PIPEDA does not prohibit the use of U.S. based third party service providers but does oblige Canadian-based organizations to ensure comparable levels of protection when these service providers are used;
  - The contract between CIBC and its service providers contained stipulations guaranteeing confidentiality and the security of personal information, in conformity with principle 4.1.3 of *PIPEDA*. It also provided for the oversight, monitoring and an audit of the services being offered. CIBC clearly maintained control of the information;

Recent trends (cont'd)

Privacy Commissioner ruling #313 (cont'd)

- While in the hands of a U.S. third party service provider, the information is subject to all laws of that country despite any contractual disposition to the contrary. The contract could not prevent the lawful access to the information by U.S. authorities;
- Given current Canadian anti-terrorism legislation, there was a comparable legal risk even within Canada that this information held by any organization and its service provider could be obtained by government agencies pursuant to either Canadian or U.S. law.
- Outsourcing is treated as an use permitted when consent is given to an agreed purpose, but the Commissioner insists on transparency and encourages to inform the concerned individuals;

Is the situation different in Canada?

Several Federal laws address issues of national security and the collection, use and disclosure of information, including:

- *Canadian Security Intelligence Service Act;*
- *Charities Registration (Security Information);*
- *Customs Act* (s. 107 and 107.1)
  - *"if the information is required to comply with a subpoena or warrant issued or an order made by a court of record outside of Canada, solely for the purposes of criminal proceedings";*
- *Department of Public Safety and Emergency Preparedness Act;*
- *Proceeds of Crime (Money Laundering) and Terrorist Financing Act.*

Is the situation different in Canada?

- *Treaty between the Government of Canada and the Government of the United States of America on Mutual Legal assistance in Criminal Matters* (1985, EIF: 1990)
  - *1. The Parties shall provide, in accordance with the provisions of this Treaty, mutual legal assistance in all matters relating to the investigation, prosecution and suppression of offences.*
  - *2. Assistance shall include:*
    - *a) examining objects and sites;*
    - *b) exchanging information and objects;*
    - *c) locating or identifying persons;*
    - *d) serving documents;*
    - *e) taking the evidence of persons;*
    - *f) providing documents and records;*
    - *g) transferring persons in custody;*
    - *h) executing requests for searches and seizures.*

Recent trends

Privacy Commissioner ruling #333, July 2006

Canadian-based company shares customer personal information with U.S. parent

- A security system company advised its Canadian customers that it intended to share customer contact information with is U.S. parent under limited urgent circumstances, namely the rerouting of alarm signals in case of an overload of the Canadian system.
- The company allowed Canadian customers to opt out of this practice and choose a reduced level of service by requesting that their accounts be managed exclusively by the Canadian customer monitoring centres.
- Complaints were made to the Privacy Commissioner regarding the security system provider. There was concern that U.S. law enforcement officials might access the information pursuant to the USA PATRIOT ACT.

Recent trends

Privacy Commissioner ruling #333 (cont'd)

- The Assistant Privacy Commissioner determined:
  - The company was not required to obtain the consent of its customers in this instance because the customers had already consented to the provision of personal information to the Canadian company for its services;
  - The information being sent to the U.S. parent was being used for the same purposes as those already consented to by the customers;
  - The company had met its obligations under Principle 4.8 by adequately informing its customers about its personal information practices;
  - The evidence showed that the parent company adhered to the same level of data protection as the Canadian company;

Recent trends

Privacy Commissioner ruling #333 (cont'd)

- Because this was a parent-affiliate situation, a separate contract between the two entities was unnecessary;
- Echoing comments from her ruling # 313, she noted that while customer personal information is in the control of a U.S. third-party service provider, it is subject to U.S. law and no private contract can override that legislation;
- *"An organization with a presence in Canada that shares customer personal information with its U.S. parent cannot protect its customers' personal information from being lawfully accessed by U.S. authorities."*
- *PIPEDA* cannot be used to prevent a Canadian company from sharing this type of information with a foreign-based parent. What *PIPEDA* does require is **transparency** with respect to their data handling practices and to protect personal information to the extent possible through contractual means.

Recent trends

Privacy Commissioner ruling #365, April 2007

- Disclosures by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) of personal information to US authorities;
- SWIFT describes itself as “the financial industry-owned co-operative supplying secure, standardized messaging services and interface software to 7,900 financial institutions in more than 200 countries.” SWIFT has identical operating centres that simultaneously collect, send, and store all SWIFT messages;
- SWIFT’s information, including the one provided by 6 Canadian banks member, was accessed by the United States Department of the Treasury.

Recent trends

Privacy Commissioner ruling #365 (cont'd)

- The complaint was ruled not well-founded:
  - Principle 4.1.3 requires to ensure a comparable level of protection when information is used by a third party;
  - The contract in place between SWIFT and the banks, as well as the other means available to the banks to ensure that SWIFT is providing a comparable level of protection;
  - When an organization contracts with a firm that operates both within and outside of Canada, it cannot prevent that firm from responding to lawfully issued subpoenas;

Recent trends

Privacy Commissioner ruling #365 (cont'd)

- "*48. Multi-national organizations must comply with the laws of those jurisdictions in which they operate. Thus, while they operate in Canada, they obviously must comply with Canadian law. However, to ask the organization to ignore the legitimate laws of other jurisdictions in which they operate is unrealistic and unworkable. Moreover, it has the potential of being interpreted as an infringement by Canada on that nation's sovereignty. It is for this reason that, in my opinion, the Act acknowledges that an organization that is subject to the Act and that has legitimately moved personal information outside the country for business reasons may be required at times to disclose it to the legitimate authorities of that country. In this case, I am of the view that paragraph 7(3)(c) operates to allow SWIFT to respond to a valid subpoena issued in the United States.*"

The "USA Patriot Act"
An Overview and Summary

- Legal framework in U.S. governing collection, use, and disclosure of data is broad and varied (and separate from USA Patriot Act);
- Different statutes govern collection, use, and disclosure of data;
- Laws governing data collection, use, and permissible disclosure often applied to specific industries:
  - Financial data privacy – Gramm-Leach-Bliley Act (GLB)
  - Health data privacy – Health Insurance Portability and Accountability Act (HIPAA)
  - Telephone and VoIP data privacy – Communications Act of 1934 (CPNI statute)
  - Online communications data privacy – Children's Online Privacy Protection Act of 1998 (COPPA)
- Other laws govern duties and liabilities for data ***breach*** or ***impermissible disclosure*** of such data more generally applicable.

The "USA Patriot Act"
An Overview and Summary

- Beyond specific data privacy statutes, USA Patriot Act affects many different aspects of data collection and use, across various industries and aspects of society (not just commercial transactions)
- Response to September 11 terrorist attacks
- Congress and President enact measure entitled:
  - *«The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act »*
- *Otherwise known as* ***USA Patriot Act***

USA Patriot Act

- Not a new stand-alone statute
- Instead, Patriot Act amends a number of ***existing*** statutes governing electronic surveillance, financial transactions, immigration, border security, and other issues
- Overall purpose and effect of these changes is to expand authority of law enforcement to monitor, track, investigate, and collect data and other information
- Enacted in 2001, sixteen provisions of the Act were set to expire on December 31, 2005
- Early 2006, Congress reauthorized and extended most of those provisions permanently

USA Patriot Act

- Overall impact of Patriot Act on privacy and data security:
  - Broadens law enforcement powers to investigate and seize data
  - Expands the types and form of data and other information sought
  - Extends scope of persons affected by traditional criminal and foreign intelligence investigations
  - Grants broader immunity from liability to third parties and investigators who undertake investigations
  - Achieves all of these things under a broader cloak of secrecy

USA Patriot Act

- Scope and reach of the Patriot Act
- The Act has 10 titles, each governing separate areas of law:
  - **Title I** - Enhancing Domestic Security Against Terrorism
  - **Title II** - Enhanced Surveillance Procedures
  - **Title III** - International Money Laundering Abatement and Anti-Terrorist Financing Act
  - **Title IV** - Protecting the Border
  - **Title V** - Removing Obstacles to Investigating Terrorism

USA Patriot Act

- Scope and reach of the Patriot Act
- The Act has 10 titles, each governing separate areas of law:
  - **Title VI** - Providing for Victims of Terrorism, Public Safety Officers, and Their Families
  - **Title VII** - Increased Information Sharing for Critical Infrastructure Protection
  - **Title VIII** - Strengthening the Criminal Laws Against Terrorism
  - **Title IX** - Improved Intelligence
  - **Title X** - Miscellaneous

USA Patriot Act

- Cross border data privacy issues most directly implicated by three different titles of the Act:
  - **Title II** - Enhanced Surveillance Procedures
  - **Title III** - International Money Laundering Abatement and Anti-Terrorist Financing Act
  - **Title IV** - Protecting the Border

USA Patriot Act

- Title II - Enhanced Surveillance Procedures
  - Sec. 201 – Expands law enforcement use of wiretapping in criminal investigations; predicate offenses now include terrorism and production or dissemination of chemical weapons;
  - Sec. 202 – Permits law enforcement to intercept oral, wire and electronic communications in cases involving computer fraud and abuse against government;
  - Sec. 203(b) & (d) – Permits sharing of information, obtained from both wiretap and foreign intelligence, if part of criminal investigation, to any other federal law enforcement, intelligence, immigration, national security or national defense officer;

USA Patriot Act

- Title II - Enhanced Surveillance Procedures
  - Sec. 204 – Allows law enforcement under FISA (Foreign Intelligence Surveillance Act) to obtain search warrants to intercept wire, oral or electronic communications (including voice mail);
  - Sec. 206 – Expands surveillance authority under FISA by allowing law enforcement to obtain a "roving" wiretap, without identifying specific location of a target or the device to be monitored;
  - Sec. 207 – Expands duration of surveillance of persons under FISA who are deemed foreign agents, from 45 days to 90 days;

USA Patriot Act

- Title II - Enhanced Surveillance Procedures
  - Sec. 209 – Allows law enforcement to obtain voice mail messages pursuant to a search warrant by amending the definition of wire communications;
  - Sec. 212 – Voluntary and Mandatory Disclosures:
    - ***Voluntary***: Allows communications providers (ISPs) to disclose information about a customer to the FBI if potential emergency involving serious danger to any person;
    - ***Mandatory***: Requires communications providers to disclose the contents of any wire or electronic communication when directed by the government under a warrant.
  - Sec. 214 – Pen register/trap & trace order (used to determine phone numbers of calls to and from a location) may be used with US citizens and foreign agents;

USA Patriot Act

- Title II - Enhanced Surveillance Procedures
  - Sec. 215 – Expands FISA access to "tangible" items; extending scope of prior statute which permitted access only to "business records";
  - Sec. 217 – Allows law enforcement to intercept communications of a computer trespasser using a protected computer;
  - Sec. 218 – Broadens the use of a wiretap order under FISA; previous statute required law enforcement to show that the "***primary***" purpose for the order is for intelligence reasons, post-Patriot Act the statute requires only that foreign intelligence constitutes a "***significant***" purpose.

USA Patriot Act

- Title III - International Money Laundering Abatement and Anti-Terrorist Financing Act
  - Sec. 311 – US Treasury Secretary authorized to take special measures if suspected money laundering activities; including require domestic financial agencies to ***maintain records*** *and* ***file reports identifying individuals actually involved in suspect transactions***, beneficial owners of funds involved, and information relating to accounts inside and outside of the United States;
  - Sec. 319 – Requires financial institutions to ***disclose information and account documentation*** for any account opened, maintained, administered, or managed in the United States upon request by a US banking agency for information related to anti-money laundering compliance by a covered financial institution or customer;

USA Patriot Act

- Title III - International Money Laundering Abatement and Anti-Terrorist Financing Act
  - Sec. 326 – Financial institutions must follow mandated procedures in obtaining and maintaining information about customers; including procedures to verify customer identity, and maintain records of such verification, and to compare this information to government lists of known or suspected terrorists or terrorist organizations agents;
  - Sec. 361 - Establishes the Financial Crime Enforcement Network ("FinCEN"), previously created by Treasury Order 105-08 in 1990, as a bureau of the Treasury Department, with the duties to ***maintain a government-wide data access service regarding suspicious and criminal financial activity*** including money laundering, and to support intelligence or counterintelligence to protect against international terrorism.

USA Patriot Act

- Title IV – Protecting the Border
  - Sec. 413 –Secretary of State may, on the basis of reciprocity, disclose to foreign governments information in the Department of State's visa lookout database and other related information either to prevent crimes by, investigate, or punish individual aliens for crimes and terrorist acts, and to cooperate with foreign governments that agree to use the information for the above purposes, or to deny visas to persons who would be inadmissible to the United States;
  - Sec. 414 - Attorney General and Secretary of State must implement an integrated entry and exit data system for airports, seaports and land border ports of entry and appropriates funds to develop a system that: utilizes ***biometric technology***; develops tamper-resistant documents readable at ports of entry; and interfaces with federal law enforcement databases ***to identify and detain individuals who pose a threat to national security***;
  - Sec. 416 - Attorney General and Secretary of State must implement a system to ***integrate information on foreign students*** in higher education and other approved educational institutions (including air flight schools, language schools and vocational schools), with ***information on dates of entry and ports of entry.***

USA Patriot Act

- Courts Have Largely Affirmed Expanded Powers Under Patriot Act
  - Case law under the Patriot Act is still relatively limited
  - However, those courts that have reviewed challenges to the expansive powers under the Patriot Act have largely affirmed such powers:
    - *Global Relief Foundation, Inc. v. O'Neil*, 207 F.Supp.2d 779 (N.D. Ill. 2002).
    - *In re Sealed Case*, 310 F.3d 717 (U.S. Foreign Int. Surv. Ct. 2002).
    - *United States v. Sattar*, 2003 U.S. Dist. LEXIS 16164 (S.D.N.Y. 2003).
    - *In re Use of Pen Register and Trap & Trace Device on E-mail Account*, 416 F.Supp.2d 13 (D.C.D.C. 2006).
  - What this tells us:
    - Patriot Act reaches broadly across many industries, whether communications, financial or otherwise; also touches many aspects of non-commercial transactions, including education, travel, etc.
    - Courts unlikely to interfere with broad mandate under Patriot Act

Conclusion on transfer personal information from Canada to the U.S.

- There exist formal bilateral agreements between Canada and the U.S. that provide for mutual cooperation and for the exchange of relevant information.
- In a decision currently under appeal to the British Columbia Court of Appeal, the BC Supreme Court in *British Columbia Government and Services Employees' Union v. British Columbia (Minister of Health Services)** rejected the Union's challenge of the BC Government's decision to outsource the administration of the province's medical records to the Canadian affiliate of a U.S. company.
- The Union was concerned that this decision would potentially allow U.S. law enforcement officials to scrutinize the medical records of British Columbians.

* 2005 BCSC 446 (CanLII)

FASKEN MARTINEAU

Conclusion on transfer personal information from Canada to the U.S.?

- The Assistant Privacy Commissioner, in Decision # 313, specifically stated that a company in Canada that outsources information processing to the U.S. should notify its customers that this information may be available to the U.S. government under a lawful order made in the U.S.
- *PIPEDA* cannot prevent the outsourcing of services to U.S. based companies, nor can it prevent U.S. authorities from lawfully accessing information held by organizations in Canada or the U.S. What *PIPEDA* demands is that the organizations be **transparent** about their personal information handling practices.

Conclusion on transfer personal information from Canada to the U.S.?

- What is important is transparency: the organization must inform its clients of the risk that their personal information may be legally accessible by the U.S. government pursuant to the USA PATRIOT ACT.
- Fact to keep in mind: 81.6% of Canadian merchandise exports in 2006 were destined for the U.S (second positions goes to U.K. and Japan with a little over 2%).
  - Statistics Canada: *Canada's Merchandise Exports* available online at www.international.gc.ca/eet

Should Canadians Fear the Patriot Act?

- It's a business decision
  - 64% of Canadians have serious concerns about companies transferring their personal information to the U.S.
- Make sure it is an informed decision!
- If outsourcing, including personal information communication, is the solution, keep in mind:
  - Consent provisions and exceptions;
  - Contractual requirements.

Biographies

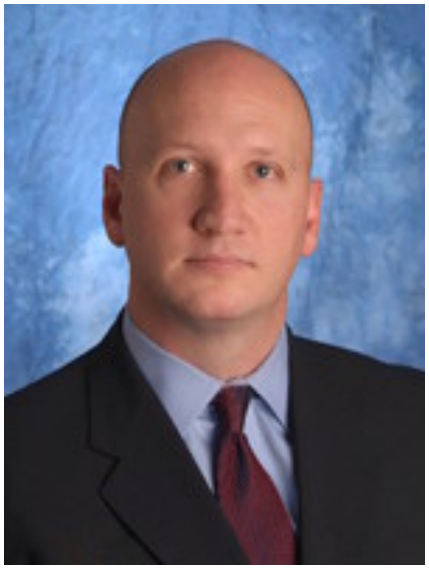
Antoine Aylwin

Antoine Aylwin practices in civil litigation, as well as commercial and administrative law. He works mainly in civil liability, estate litigation, and the protection of personal information in the public and private sectors. He is a member of Fasken Martineau's national Privacy and Information Protection Group, and of the Labour, Employment, Human Rights and Public Law Group.

In the course of his practice, Antoine frequently pleads before all levels of Québec courts.

Biographies

K.C. Halm



K.C. Halm counsels competitive telecommunications, Voice over Internet Protocol (VoIP), and broadband service providers on a wide range of telecommunications competition and broadband policy matters including interconnection, use of number resources, intercarrier compensation, licensing and tariff obligations. Represents VoIP providers, cable operators and CLECs before federal and state courts and administrative agencies on various regulatory issues arising under the Telecommunications Act of 1996.

He has significant experience with the negotiation, arbitration and litigation of interconnection agreements, traffic exchange, and intercarrier compensation arrangements on behalf of competitive telecommunications and VoIP providers, as well as negotiating and securing franchise or license authority to install fiber and facilities in public rights-of-way.

K.C. also advises communications companies and other entities on subscriber privacy and security issues under federal and state communications law, involving CALEA, CPNI and cable privacy statutes. Drafts subscriber agreements, privacy policies, acceptable use policies and other related documents for communications entities and other companies.

Antoine Aylwin
Fasken Martineau DuMoulin
Suite 3400, P.O. Box 242
800, Place Victoria
Montréal (Québec)
Canada H4Z 1E9
aaylwin@mtl.fasken.com
Tel.: 514 397 5123
Fax: 514 397 7600

K.C. Halm
Davis Wright Tremaine LLP
1919 Pennsylvania Avenue NW, Suite 200
Washington, DC 20006
kchalm@dwt.com
Tel: (202) 973-4287
Fax: (202) 973-4499