# Privacy in Canada - PIPEDA

PIPEDA (the Personal Information Protection and Electronic Documents Act) is a Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business. PIPEDA was passed in the late 1990s to promote consumer trust in electronic commerce. The act was intended to reassure the European Union that Canadian privacy laws were adequate to protect the information of European Citizens.

# PIPEDA

PIPEDA incorporates and makes mandatory provisions of the Canadian Standards Association's Model Privacy Code of 1995. The PIPED Act is broken down into two basic parts; expectations for privacy for individuals and requirements for privacy for businesses and organizations.

# What is personal information?

Information that can be used to identify an individual, or most information about that individual, including, but not limited to:

- Name, age, weight, height
- Medical records
- Income
- Purchasing habits

# Personal Information (cont)

- Race, ethnicity
- Blood type, DNA code, finger prints (PHIA)
- Marital status
- Religion
- Education
- Home address and home phone number

# What information isn’t covered

- Business card info - specifically employee related
  - Name
  - Job Title
  - Business Address
  - Office phone/fax
  - Office email address

# PIPEDA Resources

- The information available on the Office of the Privacy Commissioner (OPC) of Canada website is basically broken into three parts – information for individuals and information for businesses and organizations (the third being legislation and support information). Guides are released for both these two main parts of PIPEDA, and these guides are available on the CourseOffers drive.

# Information for Individuals

The PIPEDA legislation gives individuals right to:

- know why an organization collects, uses or discloses their personal information;
- expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented;
- know who in the organization is responsible for protecting their personal information;
- expect an organization to protect their personal information by taking appropriate security measures;
- expect the personal information an organization holds about them to be accurate, complete and up-to-date;
- obtain access to their personal information and ask for corrections if necessary; and
- complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

Page 2 and 3 of Privacy Guide for Individuals.pdf

# Information for Individuals

- Though the Act requires that affected organizations comply with the CSA (Canadian Standards Association) Model Code for the Protection of Personal Information, there are a number of exceptions to Code where information can be collected, used and disclosed without the consent of the individual. Examples include for investigations related to law enforcement or in the event of an emergency. There are also exceptions to the general rule that an individual shall be given access to his or her personal information.

# Information for Individuals

- Other cases where information may be collected, used, and disclosed without the individual's consent include:
  - An employee's name, title, business address or telephone number (as indicated above)
  - Items covered by the Privacy Act of 1983
  - Agencies that collect and use personal information for journalistic and artistic purposes
  - Individual collections for personal purposes, such as genealogical research or personal greeting card list
  - Employee information – except in the federally regulated sector
  - Each province has their own privacy legislation. These may or may not clash with the federal laws. Most have to do with how the province and its Special Operating Agencies deal with privacy

Last page of Privacy Guide for Individuals.pdf

# Privacy Act

The Privacy Act is Canadian federal legislation that came into effect on July 1, 1983. The act sets out rules for how institutions of the federal government must deal with personal information of individuals. Some salient provisions of the legislation are as follows:

- A government institution may not collect personal information unless it relates directly to an operating program or activity of the institution (section 4).
- With some exceptions, when a government institution collects an individual's personal information from the individual, it must inform the individual of the purpose for which the information is being collected (section 5(2)).
- With some exceptions, personal information under the control of a government institution may be used only for the purpose for which the information was obtained or for a use consistent with that purpose, unless the individual consents (section 7).

# Privacy Act (cont)

- With some exceptions, personal information under the control of a government institution may not be disclosed, unless the individual consents (section 8).
- Every Canadian citizen or permanent resident has the right to be given access to personal information about the individual under the control of a government institution that is reasonably retrievable by the government institution, and request correction if the information is inaccurate (section 12).
- The Privacy Commissioner of Canada receives and investigates complaints, including complaints that an individual was denied access to his or her personal information held by a government institution (section 29).
- More information on the Privacy Act can be found on the OPC website

# Information for Individuals

- Any individual who believes that an affected organization is not following PIPEDA is able to complain to the Privacy Commissioner of Canada, who investigates the complaint. The Commissioner does not have any remedial powers, but issues a report on the investigation. After receiving the report, the individual may proceed to the Federal Court of Canada, which is able to order compliance and award damages.

- The implementation of PIPEDA occurred in three stages. 1 Starting in 2001, the law applied to federally regulated industries (such as airlines, banking and broadcasting). In 2002 the law was expanded to include the health sector. Finally in 2004, any organization that collects personal information in the course of commercial activity was covered by PIPEDA

- Privacy Test – OPC website http://www.privcom.gc.ca/quiz/index_e.asp

# Privacy in Canada – Business and Organizational Responsibilities

# Rights for Individuals

The PIPEDA legislation gives individuals right to:

- know why an organization collects, uses or discloses their personal information;
- expect an organization to collect, use or disclose their personal information reasonably and appropriately, and not use the information for any purpose other than that to which they have consented;
- know who in the organization is responsible for protecting their personal information;
- expect an organization to protect their personal information by taking appropriate security measures;
- expect the personal information an organization holds about them to be accurate, complete and up-to-date;
- obtain access to their personal information and ask for corrections if necessary; and
- complain about how an organization handles their personal information if they feel their privacy rights have not been respected.

Page 2 and 3 of Privacy Guide for Individuals.pdf

# Information for Organizations

The PIPEDA legislation requires businesses and organizations to:

- obtain consent when they collect, use or disclose someone's personal information;
- supply an individual with a product or a service even if they refuse consent for the collection, use or disclosure of your personal information unless that information is essential to the transaction;
- collect information by fair and lawful means; and
- have personal information policies that are clear, understandable and readily available.

Page 3 of Privacy Guide for Individuals.pdf

As mentioned earlier, PIPEDA is a Canadian law governing how private sector organizations collect, use and disclose personal information in the course of commercial business.

Since 2004, all companies that collect, store, use, share, and destroy personal data are required to follow the guidelines outlined in the Act

# PIPEDA for Organizations

When looking at how the Act applies to Business and Organizations, it is best to break it down to areas of responsibility, based on the self test for businesses on the OPC website. These include:

- Legacy Data and Grandfathering considerations
  - Includes seeking consent
- Personal Information Holdings
- Accountability of organization and staff
- Information for customers and employees
- Limiting collection, use, etc to specified purposes

# PIPEDA for Organizations

- Consent
- Third Party Transfers
- Accuracy
- Security and protection of data
- Requests for access to information
- Handling Complaints

# Grandfathering Existing data

- Regardless of when personal data is collected, it is covered under PIPEDA. Existing customers, however, do not need to give explicit permission for the continued use of their personal data. Under Principle 4.5 of the Act, an organization should retain personal information only as long as necessary for the fulfillment of the purposes for which it was collected; should develop guidelines and procedures regarding retention, including minimum and maximum retention periods; and should destroy or erase any personal information no longer required to fulfill identified purposes.

# Grandfathering Existing data

- In determining how to treat an existing customer file, an organization should first consider such questions as:
  - Is the information still serving (or has it ever served) any purpose that could reasonably be considered necessary or useful;
  - Is there a legal or contractual requirement to retain the information: and
  - Would the individual reasonably expect the organization to be still holding the information on file?
- If the answer is no to any of these, appropriate actions should be taken

# Grandfathering Existing data

- When to seek consent from existing clients:
  - Whether the organization made a reasonable effort to inform the customer of its purposes at the time of collecting the personal information;
  - Whether the information is still being used or disclosed, and if so whether it is being used or disclosed for the same purposes for which it was collected;
  - Whether the information is being used or disclosed for unidentified secondary purposes; and
  - Whether the customer would reasonably expect the organization to continue using or disclosing the information for its current purposes.

# Personal information holdings

- Do you know what personal information is?
- Do you collect, use or disclose personal information in your day-to-day commercial activities?
- Do you have an inventory of your personal information holdings?
- Do you know where personal information is held (physical locations and files)?
- Do you know in what format(s) the personal information is kept electronic, paper, etc.)?
- Do you know who has access to personal information in and outside your organization?

# Origins of PIPEDA for Organizations

- Based on the 10 basic principals of the CSA Model Code for the Protection of Personal Information
  1. Accountability
  2. Identifying purposes
  3. Consent
  4. Limiting collection
  5. Limiting use, disclosure, and retention
  6. Accuracy
  7. Safeguards
  8. Openness
  9. Individual access
  10. Challenging compliance

# Accountability of organization and staff

- Have you named a privacy officer who is responsible for your organization's overall compliance with the Act?
- Is this responsibility shared with more than one person?
- If these responsibilities are shared, have they been clearly identified?
- Can your staff respond to internal and external privacy questions on behalf of the organization, or do they know who should respond?
- Does your staff know who receives and responds to:
  - requests for personal information?
  - requests for correction?
  - complaints from the public?

# Accountability of organization and staff (cont)

- Do your customers know whom to contact:
  - for general inquiries regarding their personal information?
  - to request their personal information?
  - to request corrections to their personal information?
  - for complaints?
- Is your privacy officer able to explain to the public the steps and procedures for requesting personal information and filing complaints?
- Has your staff been trained on the Act?
- Will there be ongoing training?
- Is your staff able to explain the purposes for the collection, use and disclosure of personal information to customers in easy to understand terms?
- Is your staff able to explain to customers when and how they may withdraw consent and what the consequences, if any, there are of such a withdrawal?
- Will you inform your employees of new privacy issues raised by technological changes, internal reviews, public complaints and decisions of the courts?

# Consequences for Staff

- Manitoba nurses find: http://www.cbc.ca/news/canada/manitoba/2-manitoba-nurses-fined-1k-each-for-breaching-patient-privacy-1.3275793

# Information for customers and employees

- Do you have documents that explain your personal information practices and procedures to your customers?
- Does this information include how to:
  - obtain personal information?
  - correct personal information?
  - make an inquiry or complaint?
- Does this information describe personal information that is:
  - held by the organization and how it is used?
  - disclosed to subsidiaries and other third parties?
- Do you have a privacy policy for your web site?

# Information for customers and employees (cont)

- Is your privacy policy prominent and easy to find? Is it easily understandable?
- Do your application forms, questionnaires, survey forms, pamphlets and brochures clearly state the purposes for the collection, use or disclosure of personal information?
- Have you reviewed all your public information material to ensure that any sections concerning personal information are clear and understandable?
- Have you ensured that the public can obtain this information easily and without cost?
- Is this information reviewed regularly to ensure that it is accurate, complete and up to date?
- Does this information include the current name or title of the person who is responsible for overseeing compliance with the Act?

# Limiting collection, use, disclosure and retention to identified purposes

- Have you identified the purposes for collecting personal information?
- Are these purposes identified at or before the time the information is collected?
- Do you collect only the personal information needed for identified purposes?
- Do you document the purposes for which personal information is collected?
- If you gather and combine personal information from more than one source, do you ensure that the original purposes have not changed?
- Have you developed a timetable for retaining and disposing of personal information?
- When you no longer require personal information for the identified purposes or it is no longer required by law, do you destroy, erase or make it anonymous?

# Consent

- Does your staff know that an individual's consent must be obtained before or at the time they collect personal information?
- Does your staff know they must obtain an individual's consent before any new use or new disclosure of the information?
- Do you use express consent whenever possible, and in all cases where the information is sensitive or the individual would reasonably expect it?
- Is your consent statement worded clearly, so that an individual can understand the purpose of the collection, use or disclosure?
- Do you make it clear to customers that they need not provide personal information that is not essential to the purpose of the collection, use or disclosure?

# Third Party Transfers

- Do you use contracts to ensure the protection of personal information transferred to a third party for processing?
- Does the contract limit the third party's use of information to purposes necessary to fulfil the contract?
- Does the contract require the third party to refer any requests for access or complaints about the information transferred to you?
- Does the contract specify how and when a third party is to dispose of or return any personal information it receives?

# Ensuring Accuracy

- Is personal information sufficiently accurate, complete and up to date to minimize the possibility that your organization might use inappropriate information?
- Does your organization document when and how personal information is updated, to ensure its accuracy?
- Do you ensure that personal information received from a third party is accurate and complete?

# Safeguards

- Have you reviewed your physical, technological and organizational security measures?
- Do they prevent improper access, modification, collection, use, disclosure and/or disposal of personal information?
- Is personal information protected by security safeguards that are appropriate to the:
  - sensitivity of the information?
  - scale of distribution?
  - format of the information?
  - method of storage?
- Have you developed a "need-to-know" test to limit access to personal information to what is necessary to perform assigned functions?

# Safeguards (cont)

- Has your staff been trained about security practices to protect personal information? For example, is staff aware that personal information should not be left displayed on their computer screens or desktops in their absence?
- Is your staff aware that they should properly identify individuals and establish their right to access the personal information before disclosing it?
- Do you have rules about who is permitted to add, change or delete personal information?
- Is there a records management system that assigns user accounts, access rights and security authorizations?
- Do you ensure that no unauthorized parties may dispose of, obtain access to, modify or destroy personal information?

# Requests for access to personal information

- Is your staff aware of the time limits the law allows to respond to access requests?
- Can you retrieve personal information to respond to individual access requests with a minimal disruption to operations?
- Do your information systems facilitate the retrieval and accurate reporting of an individual's personal information, including disclosures to third party organizations?
- Do you provide personal information to the individual at minimal or no cost?
- Do you advise requesters of costs, if any, before personal information is retrieved?

# Requests for access to personal information (cont)

- Do you record an individual's response to being notified of the cost of retrieving personal information?
- Do you provide personal information in a form that is generally understandable? (For example, do you explain abbreviations?)
- Does your organization have procedures for responding to requests for personal information in an alternate format (such as Braille or audio tapes)?

# Handling complaints

- Can an individual easily find out how to file a complaint with you?
- Do you deal with complaints in a timely fashion?
- Do you investigate all complaints received?
- Are your customer assistance and other front-line staff able to distinguish a complaint under the law from a general inquiry? If unsure, do they discuss this with the individual?

# Handling complaints (cont)

- Do you advise individuals about all available avenues of complaints, including the Privacy Commissioner of Canada?
- Are staff responses to public inquiries, requests and complaints reviewed to ensure they are handled fairly, accurately and quickly?
- When a complaint is found to be justified, do you take appropriate corrective measures, such as amending your policies and advising staff of the outcome ?

# Global Privacy and how it relates to Canadians

# American Privacy

- Data privacy is not highly legislated or regulated in the U.S.. In the United States, access to private data is culturally acceptable in many cases, such as credit reports for employment or housing purposes. Although partial regulations exist, for instance the Children's Online Privacy Protection Act and HIPAA, there is no all-encompassing law regulating the use of personal data. The culture of free speech in the U.S. may be a reason for the reluctance to trust the government to protect personal information.

# Federal US Privacy Laws

- No uniform or common privacy laws in the US. Courts seem to lean towards the publics right to access information over the right of the individual. Only clear federal laws governing privacy revolve around health care and child online protection. Only state that has active privacy is California. Some individual state supreme courts have overturned even this.

# From Wikipedia

- Data privacy is not highly legislated or regulated in the U.S.. In the United States, access to private data is culturally acceptable in many cases, such as credit reports for employment or housing purposes. Although partial regulations exist, for instance the Children's Online Privacy Protection Act and HIPAA, there is no all-encompassing law regulating the use of personal data. The culture of free speech in the U.S. may be a reason for the reluctance to trust the government to protect personal information. In the U.S. the first amendment protects free speech and in many instances privacy conflicts with this amendment. In many countries privacy has been used as a tool to suppress free speech.

# Privacy in the US

- Interesting and unfolding article on Wikipedia: https://en.wikipedia.org/wiki/Privacy_laws_of_the_United_States

# European Convention on Human Rights

- The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence.

# US Safe Harbor Agreement

- Developed by the US Department of Commerce in 1995 in response to the Directive on Data Collection of the European Commission
- Directive states that personal data may only flow from EU to countries that provide a level of privacy protection equivalent to that of the EU.
- Provides a means for US companies to show compliance with the EC directives.
- Under this program, the European Commission agreed to forbid European citizens from suing US companies for transmitting personal data into the USA.

# EU-US Privacy Shield

- In October of 2015, based on individuals challenging the Safe Harbour agreement, the agreement was declared invalid by the European Court of Justice.  As such, a new poicy was needed.
- This lead to the EU-US Privacy Shield framework for transatlantic exchange of personal information

# EU-US Privacy Shield

- Act went into effect when signed by the European Commission on 12 July 2016
  - May not resolve original challenge to the Safe Harbour agreement.
- https://en.wikipedia.org/wiki/EU-US_Privacy_Shield

# US Privacy Laws

- Usually handled state by state
- An inalienable right to privacy is enshrined in the California Constitution's article 1, section 1, and the California legislature has enacted several pieces of legislation aimed at protecting this right. The California Online Privacy Protection Act (OPPA) of 2003 requires operators of commercial web sites or online services that collect personal information on California residents through a web site to conspicuously post a privacy policy on the site and to comply with its policy.

# US Privacy Laws (cont)

- The Supreme Court of Connecticut interpreted the Constitution to grant a right of privacy to individuals in Griswold v. Connecticut.
- Privacy laws by state: http://www.epic.org/privacy/consumer/states.html
- Privacy Act of 1974
  - Response to Nixon Administration's privacy abuse
  - The Privacy Act mandates that each United States Government agency have in place an administrative and physical security system to prevent the unauthorized release of personal records.
  - Individuals permitted to view and amend personal info

# USA PATRIOT ACT

- **Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001**
  - Passed with minimal debate only 43 days after the September 11, 2001 attacks on the World Trade Center in New York City, the Act dramatically and many say unconstitutionally expanded the authority of U.S. law enforcement agencies for the stated purpose of fighting terrorism in the United States and abroad. Among its provisions, the act increased the ability of law enforcement agencies to search telephone and e-mail communications and medical, financial, and other records; …

# USA PATRIOT ACT (cont)

- … eased restrictions on foreign intelligence gathering within the United States; expanded the Secretary of the Treasury's authority to regulate financial transactions, particularly those involving foreign individuals and entities; and enhanced the discretion of law enforcement and immigration authorities in detaining and deporting immigrants suspected of terrorism-related acts. The act also expanded the definition of terrorism to include "domestic terrorism", thus enlarging the number of activities to which the Patriot Act's expanded law enforcement powers can be applied.

# EU Privacy

- The right to data privacy is heavily regulated and rigidly enforced in Europe. Article 8 of the European Convention on Human Rights (ECHR) provides a right to respect for one's "private and family life, his home and his correspondence", subject to certain restrictions. The European Court of Human Rights has given this article a very broad interpretation in its jurisprudence.

# EU Privacy

- European Commission decided to harmonize data protection regulation and proposed the Directive on the protection of personal data, which member states had to transpose into law by the end of 1998.
- The directive contains a number of key principles which must be complied with. Anyone processing personal data must comply with the eight enforceable principles of good practice.
- They say that data must be:

# 8 Enforceable Principals

- Fairly and lawfully processed.
- Processed for limited purposes.
- Adequate, relevant and not excessive.
- Accurate.
- Not kept longer than necessary.
- Processed in accordance with the data subject's rights.
- Secure.
- Not transferred to countries without adequate protection.

# Right to be Forgotten

- EU has instructed search engines like Google to give everyone in the EU the right to request search engines to remove links to “determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past”
- https://en.wikipedia.org/wiki/Right_to_be_forgotten

# Right to be Forgotten

- Implementation in Canada uncertain at this time, but experts seem to believe it unlikely
  - Seems existing privacy rights already cover the ability to ask Google to manage Canadians personal information
  - http://www.mcmillan.ca/The-Internet-Never-Forgets-Google-Incs-right-to-be-forgotten-EU-ruling-and-its-implications-in-Canada
  - http://www.cbc.ca/news/technology/right-to-be-forgotten-how-canada-could-adopt-similar-law-for-online-privacy-1.2676880

# Privacy Collection Methods

- Some on-line activities that would be covered by PIPEDA
  - Register for a free draw
  - Registration for a conference – real or virtual
  - Downloading software or data files
  - Enrollment in some Web 2.0 apps (forums, blogs, wikis)
  - Any activity that gives personal information

# Personal Information Handling

- Handling of the PIPEDA covered information must be outlined in the organization's Privacy Policy
- Policy must cover provincial, state, and international privacy policy considerations
- Policy must be kept up to date and current with changes in information handling practices and requirements.

# Activity

- Create a privacy policy and add it to the Stung Eye blog website. Include it in navigation. Don’t reinvent the wheel, find one that suits your needs, and modify.