Striking the Right Balance

B.C.'s *Personal Information Protection Act*

Jeannette Van Den Bulk and David Padgett
Legislation, Privacy and Policy
Ministry of Technology, Innovation and Citizens' Services
Victoria, April 2014

What we will cover today

- Introductions
- What is privacy?
- What is personal information?
- What is the Personal Information Protection Act (PIPA)?
- Overview of PIPA's principles
- Implementation tools
- Questions

Legislation, Privacy and Policy Branch of the Office of the Chief Information Officer (OCIO)

What we do:

- Responsible for the *Freedom of Information and Protection of Privacy Act (*FOIPPA), *Personal Information Protection Act* (PIPA), *Document Disposal Act* (DDA), and *Electronic Transactions Act* (ETA) and all policy, standards and directives that flow from them.
- Leading strategic privacy initiatives across government
- Establishing government policy, standards and guidelines on access and privacy issues
- Providing services, support and leadership to assist ministries and other public bodies in complying with the FOIPP Act
- Providing input and advice on legislative proposals and reviews
- Supporting information provision and privacy training

Office of the Information and Privacy Commissioner (OIPC)

- Information and Privacy Commissioner is an independent Officer of the Legislature
- Elizabeth Denham is B.C.'s Information and Privacy Commissioner
- The Office of the Information and Privacy Commissioner (OIPC):
  - conducts reviews and investigations to ensure compliance with the FOIPPA and PIPA
  - mediates privacy and access disputes
  - comments on access and privacy implications of proposed legislative schemes or public body programs

Information and Privacy Commissioner

PIPA Resource Page http://www.oipc.bc.ca/for-private-organizations.aspx

What is privacy?

- Not defined in PIPA, or any legislation in Canada
- None of the statutes define "privacy" but aim to achieve it with rules for how personal information is to be collected, used and disclosed

What is privacy?

- Different Types of Privacy
  - Physical
  - Spatial
  - Informational

The foundation of privacy laws

Informational self determination

- an individual's personal information is their own
- to the extent possible, the individual controls how their personal information is collected, used and disclosed

Personal Information Protection of Privacy Act (PIPA)

What is PIPA?

- Protection for personal information held by the private (non-government) sector
- "Common sense" rules for the collection, use, disclosure (sharing), retention and security of personal information
- Recognizes "right" of individuals to protect their personal information and the "need" of organizations to collect, use and disclose personal information for reasonable purposes

PIPA applies to…

- **ALL organizations** (not just those that engage in commercial activities) in BC including:
  - ✓A person (e.g., corporations, partnerships, sole proprietorships)
  - ✓An unincorporated association
  - ✓A trade union
  - ✓Non-profit sector

- **Does not include:**
  - ✘Personal or domestic uses
  - ✘Journalistic, artistic, literary uses
  - ✘The courts
  - ✘A public body or information under the FOIPP Act
  - ✘Information captured by PIPEDA (trans-border transfers)

PIPA is distinct from other legislation

- ***Personal Information Protection Act* (PIPA)**
  - private sector privacy legislation; applies to "organizations" in B.C.
  - primarily consent-based

- ***Freedom of Information and Protection of Privacy Act* (FOIPP Act)**
  - public sector access and privacy legislation; applies to public bodies in B.C.
  - primarily authority-based

PIPA is distinct from other legislation

- ***Personal Information Protection and Electronic Documents Act (PIPEDA)***
  - applies to federal works, undertakings or businesses (banks, airlines, and telecommunications companies)
  - applies to the collection, use and disclosure of personal information in the course of a commercial activity and across borders
- Canada's ***Access to Information Act*** and also the ***Privacy Act***
  - are the federal equivalents to the BC FOIPP Act (FOI and privacy obligations for federal government institutions)

What is personal information?

- Personal Information is **"Information about an Identifiable Individual".**
- Personal information includes:

  Name, age, home address and phone number, SIN, race or ethnic origin, medical information, income, marital status, religion, education, opinions, employment information, photographs, video recordings

What is personal information?

- Includes employee (or volunteer) personal information
- Does not include:
  - ✘ Business contact information: information to enable an individual at a place of business to be contacted
  - ✘ Work product information: information prepared by individuals or employees in the context of their work or business, but does not include personal information about other individuals.

What are the rules?

Based on "Fair Information Practices"

1. Identify Purposes
2. Limit Collection
3. Get Consent
4. Limit Use, Disclosure & Retention
5. Reasonable Security
6. Be Accountable
7. Be Open and Transparent
8. Ensure Accuracy
9. Right of Access/ Correction or Annotation
10. Provide Recourse

1. Identifying purposes

- An organization must identify, verbally or in writing,
  - the purposes for which it collects personal information
  - upon request, who can answer questions about the collection

1. Identifying purposes

Examples of purposes might include:

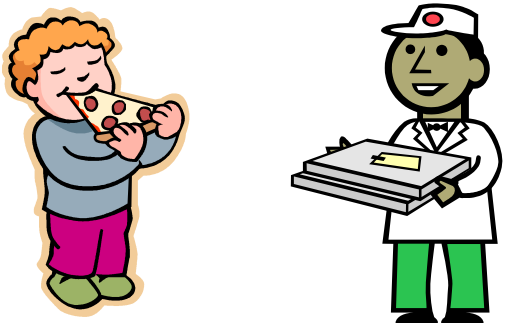
- opening an account
- verifying creditworthiness (or eligibility)
- providing counseling services
- program enrollment
- sending out association membership information
- identifying customer preferences
- providing employee benefits

2. Limit collection of personal information

- Do not collect personal information indiscriminately
- Information must be necessary to fulfill identified purposes (i.e. reasonable and appropriate)

Would the following collection be reasonable???

- Would your doggie daycare company need your home phone number?
- Would a retailer taking your credit card's imprint need your phone number? Your SIN?
- Would a mattress company need your level of income or education on a warranty card?
- Would a sports club need to collect detailed health information from club members?



Ordering Pizza in the 21st century…Created by the American Civil Liberties Union

Link:
http://www.aclu.org/pizza/index.html?orgid=EA071904&MX=1414&H=1

3. Obtain consent

- Consent may be:
  - ✓explicit (written/oral)
  - ✓implicit (i.e., deemed)
  - ✓opt out
- Some circumstances where no consent required

Forms of consent

- **Explicit consent**
  - Can be written or verbal (obtained in person, by phone, by mail, Internet etc.)
  - Must notify individual of purposes
- **Implicit (or deemed) consent**
  - Purpose obvious
  - Personal information voluntarily provided
- **Opt out consent:**
  - Organization provides notice (in form that is understandable) & informs of purpose;
  - gives reasonable amount of time and opportunity to decline;
  - individual does not decline; and
  - the collection, use or disclosure reasonable given sensitivity of personal information.

When consent isn't needed

- In limited circumstances PIPA allows collection without consent. For instance:
  - the collection is clearly in the interests of the individual and consent cannot be obtained in a timely way
  - the collection is necessary for the medical treatment of the individual and the individual is unable to give consent
  - the collection is required or authorized by law
  - for collecting a debt owed to the organization or paying a debt owed by it
  - publicly available from a prescribed source
- Collection must still be reasonable and appropriate in the circumstances

Tips for obtaining consent

- Record the consent received (e.g. note to file, copy of e- mail, copy of check-off box)
- Do not obtain consent by deceptive means
- Do not make consent a condition of supplying a product or service beyond what is necessary to provide the product or service
- Explain to individuals the implications of withdrawing their consent but do not prohibit the withdrawal unless it would frustrate the performance of a legal obligation

Employee personal information

- Recognizes true nature of employee relationship – not consent-based
- May collect use and disclose employee personal information for reasonable purposes that are necessary to establish, manage or terminate the employment relationship without consent as long as the employee is notified
- Some limited exceptions to notification (e.g., for an investigation or proceeding, medical emergency)

Would the following be considered a reasonable collection of employee personal information?

- Asking prospective employees for a retail store whether they are smokers, because of cigarette smoke odour concerns
- Videoing or monitoring employees where there is no known employment issue
- Use of credit checks in the employee hiring process

4. Limit use, disclosure and retention to identified purposes

- Organizations may use or disclose personal information:
  - for the purposes provided to the individual when the information was collected
  - for other limited purposes authorized by PIPA
- For new uses or disclosure, get consent
- Use and disclosure must be reasonable and appropriate in the circumstances

Would the following use or disclosure be okay?

- Could an organization notify the police about a client that they have seen in a wanted poster?
- Could an organization use photos of people relaxing at the beach in their promotional material?
- Could an organization use personal information to do a reference check from job applicants on references provided?
- Could an organization use an employee's SIN as a password for daily timekeeping

Limit Retention

Personal information must be retained for one year if used to make a decision.

Organizations must destroy personal information when purposes of collection no longer being served and there are no legal or business purposes for keeping it.

5. Reasonable security

- An organization must make reasonable security arrangements to protect personal information
- Should be appropriate and proportional to the sensitivity of the personal information
- Safeguards should include:
  - Physical measures (locked file cabinets, restricted access to offices)
  - Technological measures (user IDs, passwords, encryption)
  - Organizational measures (security clearances, "need to know" policy)

Protect personal information throughout its lifecycle (e.g. storing inactive records, destroying records – certificate of destruction)

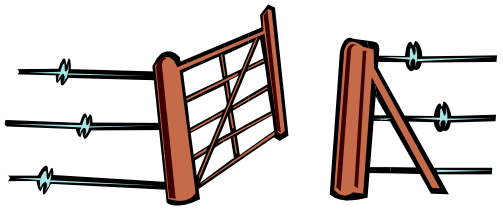
Security Tips

- Train staff, conduct periodic reviews, ensure all staff are aware of obligations and understand privacy policies and procedures
- Ensure sufficient monitoring and supervision is given to staff
- Ensure employees have access to managers or other experts when questions arise
- Ensure an emergency plan is in place to deal with unintentional disclosure (do employees know who to report problems to?)

Information Incidents

Information Incidents are ALL unauthorized event(s) that threaten the privacy or security of information

Includes privacy breaches: a collection, use, disclosure, disposal, storage of or access to personal information, whether *accidental or deliberate*, that are not authorized by the *Personal Information Protection Act*



Examples of how Information Incidents occur

- *Employee errors such as mis-stuffed enveloped or incorrect email addresses*
- *Hacking or phishing*
- *Sale of unwiped hardware or blackberries*
- *Wrong fax numbers or addresses*
- *Deliberate employee misconduct*

When things go wrong...

- Doctor inadvertently faxes medical records to a newspaper whose fax number was on speed dial.
- Law firm stores files, awaiting pick up for shredding, in an unlocked storage bin in a back alley, where they are captured on videotape blowing down the alleyway.
- National bank puts un-wiped hard drives, containing detailed financial information on clients, up for sale on the web.
- Hospital janitor disposes of old hospital records by lighting a bonfire on a public beach - a ferry passes by, sending waves onto the beach that put out the fire and wash the half-burned records down the shoreline
- Closed case files end up as props on the set of the TV series X-Files.
- An AIDS patient list, including addresses, is accidentally emailed to more than 800 unauthorized recipients.

Information Incident Response

- All organizations should create their own policy and process.

➢ See the Office of the Government Chief Information Officer website for information:

- http://www.cio.gov.bc.ca

➢ OIPC Breach Resources for Private Organizations at:

- http://www.oipc.bc.ca

It's better to prevent a privacy breach in the first place!

Prevent breaches through compliance with the general PIPA requirements, for example:

- Awareness of the disclosure authorities and other provisions of PIPA
- Reasonable policy and procedures for disposition of personal information (not selling old hard-drives; etc)
- Reasonable security arrangements, including physical, technical and policy measures (encryption; establishing sound access user profiles; etc)

6. Be accountable

- appoint an individual responsible for privacy (a privacy officer)
- be responsible for all personal information under your control, including contractors

7. Be open and transparent

- Write policies and make them available upon request
  - ✓ Addresses obligations under the Act (e.g., collection, use, disclosure, consent, security, retention, access, etc.)
- Personal information collection notices
- Brochures or other information explaining personal information policies and practices

8. Ensure accuracy

- Reasonable effort to ensure personal information collected is accurate and complete, if:
  - Used to make a decision affecting the individual it is about, or
  - Is likely to be disclosed to another organization

9. Access, correction/annotation

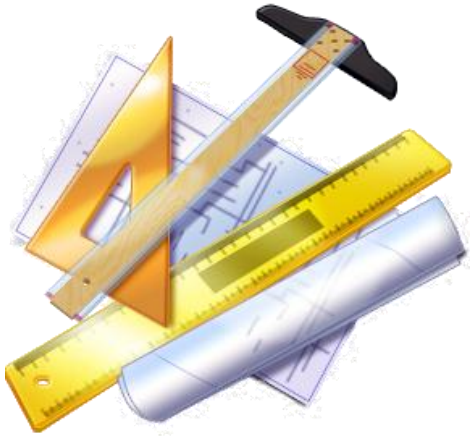
- Upon request, provide individuals with access to or correction of their personal information

  - Explain how their personal information is being used
  - Identify organizations to which their personal information has been disclosed

10. Recourse and oversight

- Organization must have process for responding to complaints
  - simple and accessible complaints handling procedures
  - Investigate all complaints; take corrective measures
- Oversight by BC Commissioner – order making power (but emphasis on mediation – 92% settlement rate)
  - May require an individual to attempt to resolve dispute with organization before begins or continues a review or investigation
  - PIPA provides for offences/penalties, right to sue

Privacy Tools



Implementation tools

http://www.cio.gov.bc.ca/cio/priv_leg/pipa/index.page?

- Ten steps to compliance
- "How do I know if I'm covered?"
- "What is a Privacy Officer?"
- Ten Principles for the Protection of Privacy
- Conducting a Privacy Audit of Your Personal Information Holdings
- Privacy Compliance Assessment Tool
- Setting Up a Complaint Handling Process
- Model Privacy Policy
- Model contract language

Summary:
Ensuring your business is compliant with privacy requirements, and privacy is protected

- Assign responsibility
- Become familiar with the Ten Privacy Principles
- Conduct a Privacy Audit and make appropriate changes
- Develop a Privacy Policy
- Train staff
- Develop or revise forms and communication materials
- Review and revise service contracts

Contact Information

BC Privacy and Access Helpline: 250-356-1851

(Enquiry BC 1 800 663-7867)

Privacy.Helpline@gov.bc.ca

Useful links and contact information

- Legislation, Privacy and Policy Branch:
  http://www.cio.gov.bc.ca/cio/priv_leg/pipa/index.page?
  - ✓ Implementation tools for organizations:
    http://www.cio.gov.bc.ca/cio/priv_leg/pipa/impl_tools/tool_index.page?
  - ✓ **Privacy and Access Helpline:**
    (250) 356-1851 or Privacy.helpline@gov.bc.ca

- Office of the Information and Privacy Commissioner:
  http://www.oipc.bc.ca/
  - ✓ PIPA Guide for Organizations:
    http://www.oipc.bc.ca/pdfs/private/GuidePIPA(Apr2012).pdf
  - ✓ PIPA Resources for Organizations:
    http://www.oipc.bc.ca/sector_private/resources/index.htm

Personal Information Protection Act
http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Questions?