iPP Consulting

Reduce risk for your small business through compliance with privacy regulations

Marilyn Sing, CIPP/C

Victoria International Privacy and Security Summit

March 11, 2025 • 10:45am to 12:15pm • Esquimalt Room

Presenter's background

- Work experience in private, public and non-profit organizations
- Management roles: Risk management, operations, business development, administration, communications and marketing
- 2015: Certified Information Privacy Professional/Canada (CIPP/C)
- 2016: Started IPP Consulting to support small to mid-sized organizations
- Community service:
  - IAPP KnowledgeNet Victoria, Chapter Chair
  - Victoria Foundation, Board member

What about you?

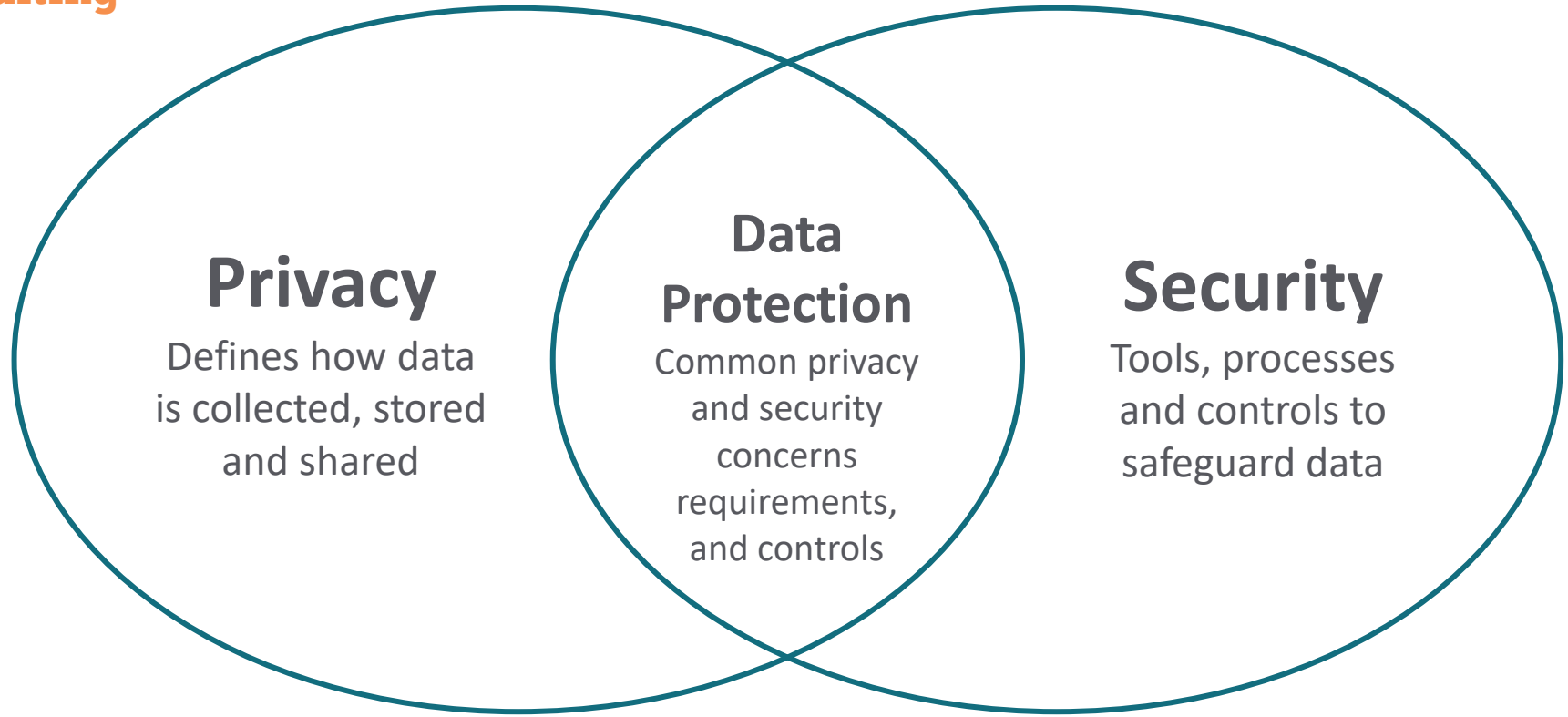
- Public sector or private sector?
- Role at your organization?
  - CEO or owner
  - Executive Director
  - Senior management team member
  - Information Technology
  - Privacy Officer
  - Other

Question:

- How would you describe your current awareness and knowledge of Canadian privacy law and organization obligations?
  a) I did not know that my organization needed to comply with privacy laws.
  b) I am aware of privacy laws and my organization has a privacy policy.
  c) I am aware of privacy laws, but not what an organization needs to do to be compliant.
  d) I am aware of privacy laws, but compliance is not a priority, given time and resources

Workshop overview

1. Security is not enough on its own to prevent privacy breaches
2. Overview of Canada's private sector privacy laws
3. Risks and costs related to privacy breaches
4. Benefits of compliance
5. Compliance considerations and requirements
6. Steps to becoming a compliant organization



https://csrc.nist.gov/csrc/media/publications/sp/800-53/rev-5/draft/documents/sp800-53r5-draft.pdf
https://www.dashlane.com/blog/what-is-data-privacy-why-is-it-important

Privacy risk focus

- Protect individuals and the organization
  - Minimize and limit data collected
  - Reduce the amount of data held
- Physical and administrative safeguards
- Minimize authorized access
- Minimize human error

Security risk focus

- Protect data held by the organization
- Technical safeguards
- Prevent unauthorized access
- Reduce technical inefficiencies and issues

Canada's private sector privacy law

Personal Information Protection and Electronic Documents Act (PIPEDA)

Enacted in 2000

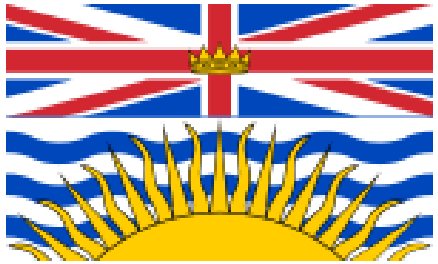
Updates: Breach Notification (2018) and Meaningful Consent (2019)

Note: PIPEDA does not generally apply to:

- Not-for-profit and charity groups
- political parties and associations

- Applies to private-sector organizations that collect, use, or disclose personal information in the course of a **commercial activity**.
- The law defines a commercial activity as any particular transaction, act, or conduct, or any regular course of conduct that is of a commercial character, including the selling, bartering or leasing of donor, membership or other fundraising lists.

British Columbia: Personal Information Protection Act (PIPA)



Enacted in 2004

- Organizations subject to PIPA include:
  - Businesses and corporations, including strata corporations
  - Partnerships
  - Individuals involved in commercial activities
  - Unincorporated associations
  - Co-operative associations, including housing co-ops
  - Societies and charities
  - Churches and other religious organizations
  - Doctors' offices
  - Sports clubs
  - Trade unions
  - Political parties
  - Trusts

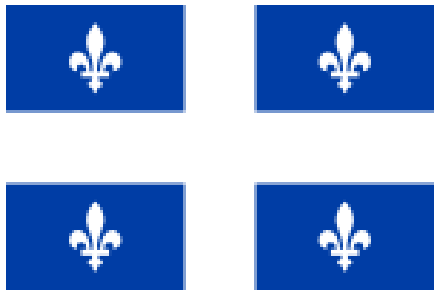
Alberta: Personal Information Protection Act (PIPA)

Enacted in 2004

- Organizations subject to PIPA include:
  - Corporations
  - Unincorporated associations
  - Professional regulatory associations
  - Trade unions
  - Partnerships
  - Private schools or colleges
  - Any individual acting in a commercial capacity

Note: Applies in a limited way to certain defined non-profit organizations and only to the extent that those organizations are involved in commercial activities.

Quebec: Act respecting the protection of personal information in the private sector (Law 25)



Enacted in 1993, updated in 2021

- Enterprise definition (Article 1525 Civil Code):
  - *The carrying on by one or more persons of an **organized economic activity**, whether or not it is commercial in nature, consisting of **producing**, **administering** or **alienating property**, or providing a **service**, constitutes the operation of an enterprise.*
  - Does not distinguish between a self-employed person and a larger enterprise

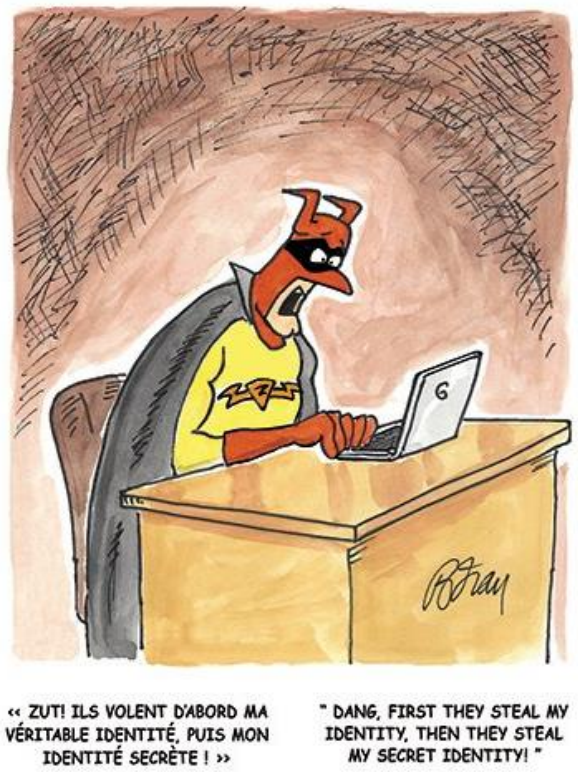
Which privacy laws apply to my organization?

Depends first on where your business is based.

Then, considers where you have employees and customers.

For example, applicable law for BC-based organizations:

- BC's PIPA
- May need to consider other applicable privacy laws:
  - Canada's PIPEDA
  - Alberta's PIPA and Quebec's Law 25
  - European Union's General Data Protection Regulation (GDPR)
  - U.S. State laws e.g., California's Consumer Protection Act (CCPA)
  - Other jurisdictional privacy law



What is personal Information?

Any information that can be used to identify someone – either by itself or in combination with other information.

What are examples of personal information?

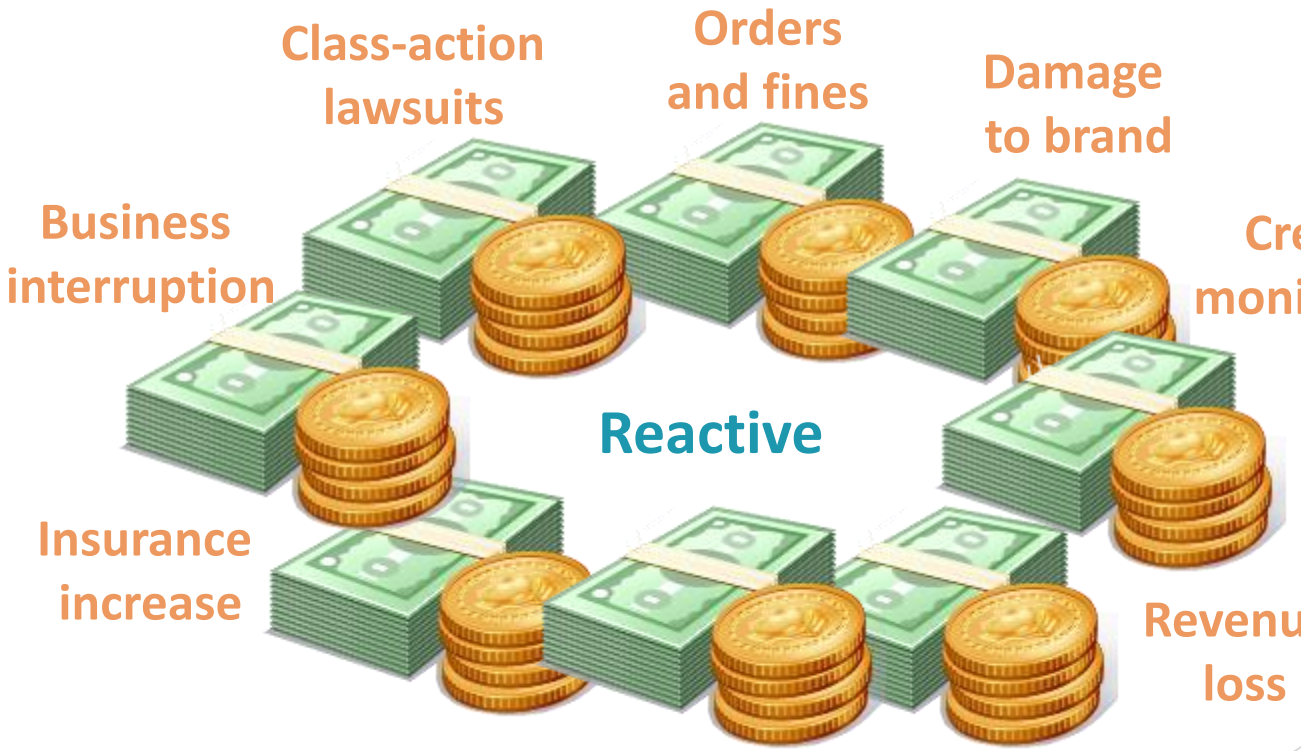
What personal information is considered to be sensitive?

What is not personal Information?

Risks related to non-compliance

Compliance

Proactive and preventative approach



Benefits of compliance

1. Clarifies responsibility for compliance
2. Identifies vulnerabilities to address them
3. Considers risks and threats to prevent theft, weaknesses or lapses in security
4. Builds a strong privacy culture
5. Increases business value for mergers, acquisitions and sale of business

Basic requirements for compliance

1. Accept responsibility for protecting the personal information under your control and custody
2. Designate one or more individuals to be responsible for ensuring compliance and make contact information publicly available
3. Develop and follow policies and practices to meet compliance obligations
4. Obtain meaningful consent from individuals for the collection and use of their personal information
5. Respond to access and correction requests, as well as questions, concerns and complaints about personal information within time limits
6. Make policies information and the complaint process available upon request

How does an organization know if it is compliant?

Privacy Management Program

- **Part A: Building Blocks**
  - Organizational commitment
  - Program controls
- **Part B: Ongoing assessment and revision**
  - Develop an oversight and review plan
  - Assess and revise program controls

https://www.oipc.bc.ca/guidance-documents/1435

Office of the Privacy Commissioner of Canada

Office of the Information and Privacy Commissioner of Alberta

OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

Part A: Organizational commitment

- Board and senior management commitment and support
- Privacy Officer – designated and responsible for the *privacy management program* (PMP)
- Privacy Office – defined with adequate resources, dependent on the size of the business
- Reporting – internal reporting mechanism to ensure the PMP is functioning as expected

Part A: Program Control 1

Personal Information Inventory (PII)

This documents what every organization needs to know:

- what personal information it holds and where it is held;
- why it is collecting, using or disclosing personal information;
- the sensitivity of the personal information it holds; and
- how the personal information is safeguarded

Each collection of personal information is documented in the inventory.

Safeguards

- Physical
  - Locked cabinets and offices, alarm systems, etc.
- Administrative
  - Policies, training, codes of conduct, employee handbooks, criminal record checks, employee screening, etc.
- Technical
  - Password protocols and requirements, data encryption, restrictions on use of work devices, anti-virus software, multifactor authentication, etc.

Part A: Program Control 2

Privacy Policies

Five key privacy policies that organizations must have in place:

1. Collection, use and disclosure of personal information;
2. Access to and correction of personal information;
3. Retention and disposal of personal information;
4. Responsible use of information and information technology; and,
5. Challenging compliance.

Other common privacy policies that you may also need:

- BYOD, Remote work and video surveillance

Part A: Program Control 3

Risk assessment tools

Risk assessments ensure that you consider and mitigate privacy risks before you implement or update a system, product or service.

1. Privacy Impact Assessment (PIA)
2. Security Threat Risk Assessment (STRA)

Part A: Program Control 4

Training and Education

Employees must be actively engaged in privacy protection and need privacy training.

1. General privacy training (mandatory for all employees)
2. Additional role training for those handling personal information directly

Part A: Program Control 5

Breach and incident management response protocols

Organizations need to have a procedure in place and a person responsible for managing a personal information breach.

1. Responsibilities for internal and external reporting of the breach must be clear.
2. Reporting to privacy commissioners and notification of affected individuals may also be required.

What is a privacy breach?

Unauthorized access to or collection, use, disclosure or disposal of personal information.

- Common privacy breaches:
  - Personal information is mistakenly emailed to the wrong person
  - A computer containing personal information is stolen
  - A USB stick containing personal information is lost
  - An employee doesn't verify identity of the person requesting to update, change or access personal information
  - Other patients, customers or employees are revealed in a group email, when addresses should have been put in the BCC area of the email

Human error accounts for the majority of privacy breaches

Part A: Program Control 6

Service provider management

Your organization remains responsible for the personal information it transfers to service providers. Requirements for them need to include:

- Privacy provisions in contracts or agreements setting out requirements for compliance;
- Training for all service provider employees with access to personal information;
- Sub-contracting;
- Audits; and agreements with service provider employees stating that they will comply with the organization's privacy policies and protocols.

Part A: Program Control 7

External communication

To establish and maintain trust, inform individuals of their rights and your organization's privacy program controls in a clear and understandable way.

- Provide information on the purpose of collection, use and disclosure of personal information, safeguards and retention periods;
- Notify individuals about personal information transferred outside of Canada;
- Include information on who to contact with questions or concerns; and
- Make information easily available to individuals.

Part B: Ongoing assessment and revision

Once established, your privacy management program must be maintained through:

- An annual oversight and review plan;
- Monitoring, periodically auditing and where necessary, revising program controls;
- Other tasks:
  - Responding to access and correction requests, as well as personal information questions, concerns and complaints within the 30-day time limit;
  - Ongoing staff privacy training; and,
  - Maintaining compliance as laws are updated or changed.

Compliance guidance

Office of the Privacy Commissioner of Canada

- For businesses: https://www.priv.gc.ca/en/for-businesses/
- PIPEDA: https://laws-lois.justice.gc.ca/eng/acts/P-8.6/index.html

Office of the Information and Privacy Commissioner for British Columbia

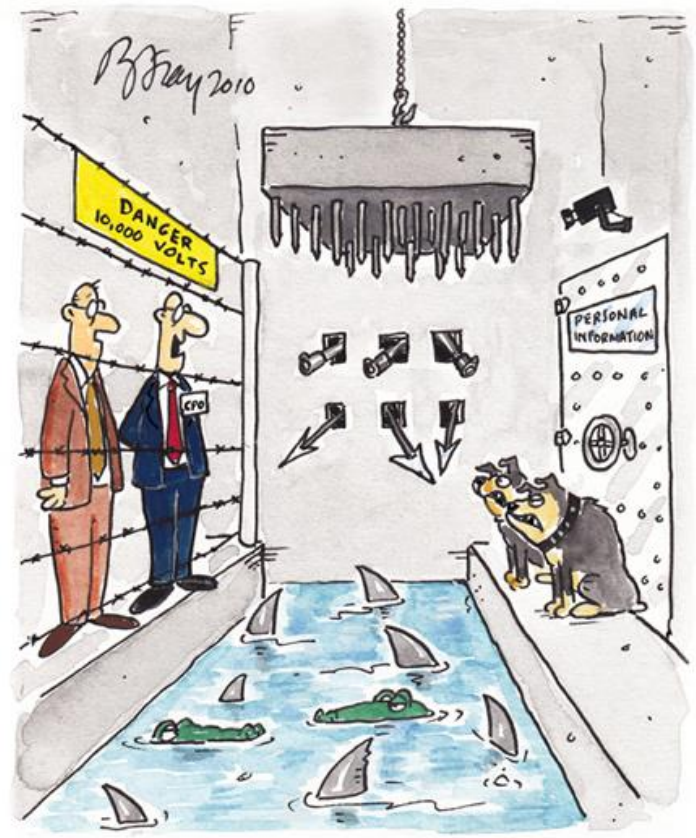
- Resources for private organizations: https://www.oipc.bc.ca/for-private-organizations/
- PIPA: https://www.bclaws.gov.bc.ca/civix/document/id/complete/statreg/00_03063_01

Office of the Information and Privacy Commissioner of Alberta

- PIPA Guide: https://oipc.ab.ca/wp-content/uploads/2022/02/PIPA-Guide-2008.pdf
- PIPA: : https://kings-printer.alberta.ca/documents/Acts/P06P5.pdf

Commission d'accès à l'information du Québec

- Privacy obligations for business: https://www.cai.gouv.qc.ca/english?
- Law 25: https://www.legisquebec.gouv.qc.ca/en/document/cs/P-39.1



"I THINK YOU'LL FIND OUR SAFEGUARDS FOR PROTECTING YOUR PERSONAL INFORMATION MORE THAN ADEQUATE!"

Questions?

Final question from me:

- Do you feel you have the information you need become a compliant organization?
  - Yes
  - No

- If you answered no, let me know what you think would be helpful for you to meet compliance.

Thank you for attending this workshop!

Interested in receiving my weekly privacy update?
Email me to get added to the list: msing@ippconsulting.ca

Workshop sources

Office of the Information and Privacy Commissioner for BC:

A Guide to B.C.'s Personal Protection Act for Businesses and Organizations:

- https://www.oipc.bc.ca/guidance-documents/1438

Does the GDPR apply to your BC-based organization?:

- https://www.oipc.bc.ca/news/does-the-gdpr-apply-to-your-bc-based-organization/

Getting Accountability Right with a Privacy Management Program

- https://www.oipc.bc.ca/guidance-documents/1435

IAPP publication: *Canadian Privacy Data Protection Law and Policy for the Practitioner, Third Edition*

BC Law:

Personal Information Protection Act

- http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01

Office of the Privacy Commissioner of Canada:

What you need to know about mandatory reporting of breaches of security safeguards

- https://www.priv.gc.ca/en/privacy-topics/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/

Guidelines for Obtaining Meaningful Consent

- https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/

Cartoons

- https://www.priv.gc.ca/en/about-the-opc/publications/illustrations/