PCS 6166 - INTERNATIONAL DATA PROTECTION AND CYBERSECURITY LAW

Part One – Enforcement Agencies

What is Canada trying to do?

Signals

- Digital Charter:

  “Data is now a resource that companies use to be more productive and to develop better products and services, unleashing a digital revolution around the world.

  In this digital world, Canadians must be able to trust that their privacy is protected, that their data will not be misused, and that companies operating in this space communicate in a simple and straightforward manner with their users. This trust is the foundation on which our digital and data-driven economy will be built.”

  “Data is a powerful tool. It has the potential to drive ground breaking research and innovation, supporting robotics, artificial intelligence (AI) and the Internet of things. There are, however, real concerns amongst Canadians about how personal data could be used, and that measures are in place that protect Canadians' privacy and security. Simply put, that the way forward on data collection, management and use must be built on a strong foundation of trust and transparency between citizens, companies and government.”

Signals (cont’d)

- Digital Charter Principles

1. Universal Access
2. Safety and Security
3. Control and Consent
4. Transparency, Portability and Interoperability
5. Open and Modern Digital Government
6. Level Playing Field
7. Data and Digital for Good
8. Strong Democracy
9. Free from Hate and Violent Extremism
10. Strong Enforcement and Real Accountability

Signals (cont'd)

- CPPA vs. PIPEDA – Purpose Statement

  The purpose of this Part is to establish - in an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information ~~technology increasingly facilitates the circulation and exchange of information~~ - rules to govern the protection ~~collection, use and disclosure~~ of personal information in a manner that recognizes the right of privacy of individuals with respect to their personal information and the need of organizations to collect, use or disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances.

- Ministerial Mandate Letters
  - Innovation, Science and Industry:

    Introduce legislation to advance the Digital Charter, strengthen privacy protections for consumers and provide a clear set of rules that ensure fair competition in the online marketplace.

    Establish a digital policy task force to integrate efforts across government and position Canada as a leader in the digital economy and in shaping global governance of emerging technologies.
  - Minister of Justice and Attorney General of Canada:

    Building on previous public consultations and technical engagements amongst experts, continue substantive review of the Privacy Act including engagement with Indigenous partners to develop specific proposals for amendments to the Privacy Act to keep pace with the effects of both technological change and evolving Canadian values.

Why Compare Across Jurisdictions?

JURISDICTIONAL COMPARISON:
PRIVACY PROTECTIONS

Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

	European Union (GDPR)	United Kingdom	New Zealand	Australia	California	Alberta	British Columbia	Quebec	Canada (Bill C-11)
Coming into force/last major update	2018	2018	2020	2018	2020	2014	2004	2021	2020 (introduced)
Defining privacy as a human right	✓	✓	✓	✓	✗	✗	✗	✓	✗
Individual knowledge and understanding	✓	✓	✓	✓	✓	✓	✓	✓	✗
Accountability: compliance with the law as objective standard	✓	✓	✓	✓	N/A	✓	✓	✓	✗
Audit: proactive to verify compliance*◆	✓	✓	✗	✓	✓	✓	✗	✓	✗
Administrative monetary penalties: broad list of violations	✓	✓	N/A	✓	✓	N/A	N/A	✓	✗
Absence of appeal before privacy-specific tribunal	✓	✓	✓	✓	✓	✓	✓	✓	✗
Broad discretion to decline/discontinue complaints*◆	✓	✓	✓	✓	✓	✓	✓	✓	✗
Full discretion for public education and guidance	✓	✗	✓	✓	✓	✓	✓	N/A	✗
Codes approval: under DPA procedures	✓	✓	✓	✓	N/A	✗	N/A	N/A	✗
Trans-border: specific provisions	✓	✓	✓	✓	✗	✓	✗	✓	✗

* MP Nathaniel Erskine-Smith introduced Bill C-413 (42nd Parliament) to provide the OPC with these authorities.
◆ Proposed by Justice Canada in *Respect, Accountability, Adaptability: A discussion paper on the modernization of the Privacy Act* (November 2020).

Canada's Changing Privacy Landscape

- Provincial
  - Quebec Bill 64
    - New requirements for businesses(via BLG)
      - Appointment of a Privacy Officer
      - Breach reporting
      - Establish/implement various policies and practices
      - Privacy impact assessments
      - Automated processing
      - Cross-border transfers
      - Outsourcing
      - Transparency
      - Consent
      - Privacy by default
      - Retention and destruction
      - De-indexation
      - Data portability
    - Also introduces significant new powers for Quebec CAI

Canada's Changing Privacy Landscape (cont'd)

- Provincial
  - Ontario
    - Consultation One (August – October 2020): Strengthening privacy protections in Ontario
      - Eight proposals:
        - Increased **transparency** for individuals, providing Ontarians with more detail about how their information is being used by businesses and organizations
        - Enhanced **consent** provisions allowing individuals to revoke consent at any time, and adopting an "opt-in" model for secondary uses of their information
        - Right for individuals to request information related to them be **deleted**, subject to limitations (this is otherwise known as "Erasure" or "the right to be forgotten")
        - Right for individuals to obtain their data in a standard and **portable** digital format, giving individuals greater freedom to change service providers without losing their data (this is known as "Data Portability")
        - Increased **enforcement** powers for the Information and Privacy Commissioner to ensure businesses comply with the law, including the ability to impose penalties
        - Introducing requirements for data that has been **de-identified and derived** from personal information to provide clarity of applicability of privacy protections
        - Expand the **scope and application** of the legislative framework beyond the private sector and commercial organizations, and
        - Create a legislative framework to enable the establishment of **data trusts** for privacy protective data sharing

Canada's Changing Privacy Landscape (cont'd)

- Provincial
  - Ontario
    - Consultation Two (June – September 2021): Modernizing privacy in Ontario
      - Themes:
        - rights-based approach to privacy;
        - safe use of automated decision making;
        - thoughtful consent and lawful uses of personal data;
        - data transparency for Ontarians;
        - protecting children and youth;
        - a fair, proportionate and supportive regulatory regime; and
        - support for Ontario businesses and innovators.

Canada's Changing Privacy Landscape (cont'd)

- Provincial
  - Alberta
    - Public survey on *Personal Information Protection Act* and *Freedom of Information and Protection of Privacy* (FOIP) *Act*
      - Survey closed August 20, 2021; asked for feedback on:
        - enhancing the rights of Albertans to access and control their own privacy when interacting with government, other public bodies, and private sector organizations (examples include ensuring clear and informed consent, data portability, requesting deletion of personal information)
        - establishing stronger transparency requirements (for example, mandatory reporting, plain language privacy statements)
        - establishing parameters and legal requirements for collecting, using, and disclosing data that has been de-identified
        - enhancing oversight to ensure the Government of Alberta, public bodies, and/or private sector organizations will protect personal information and privacy as new technologies and/or digital business models are implemented

Canada's Changing Privacy Landscape (cont'd)

- Provincial
  - British Columbia
    - Special Committee to Review the Personal Information Protection Act (est. February 2020)
      - Report: Modernizing British Columbia's private sector privacy law (December 2021)
        - Recommendation themes:
          - Alignment and Harmonization with Other Privacy Laws
          - New and Emerging Technologies
          - Meaningful Consent
          - Mandatory Breach Notification
          - Disclosure of Personal Information
          - Employer Accountability
          - Health Information
          - Office of the Information and Privacy Commissioner

Where do these similarities come from?

Influence of the GDPR

- Provincial
  - Ontario
    - "… Ontario may also consider, like Europe's **GDPR** and Quebec's Bill 64, providing a definition for sensitive information …"
    - "… The right of individuals to obtain and transfer their own information, known as "data mobility" or "data portability," is now found in Europe's **GDPR** …"
    - "Ontario is considering following the model of the **GDPR** to prohibit the use of ADS in situations of significant impact …"
  - British Columbia

    1. Ensure that PIPA meets **GDPR** and anticipated federal adequacy requirements

    2. Update PIPA with a focus on prioritizing interoperability with other provincial and international legislation, including the **GDPR**

    3. Ensure that PIPA includes definitions of pseudonymized information as personal information, and anonymized information as outside the scope of PIPA, similar to the definitions in the **GDPR**.

    …

    10. Align the exemptions to consent in PIPA with those of the **GDPR**.

    …

    etc.

A quick trip through Europe

Privacy / Data Protection in Europe – A Snapshot

In force now

- General Data Protection Regulation (GDPR)
  - Plus various implementing acts
- ePrivacy Directive (and future regulation?)
- Law Enforcement Directive

Being considered

- Data Governance Act (via European Strategy for Data)
- Digital Services Act
- Digital Markets Act
- Artificial Intelligence Act
- …

Regulatory / Data Protection Authorities

- European Data Protection Supervisor
- European Data Protection Board
  - Previously, Article 29 Working Party
- DPAs in each nation

Charter of Fundamental Rights of the EU

Article 8: Protection of personal data

1. Everyone has the right to protection of personal data concerning him or her.
2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.
3. Compliance with these rules shall be subject to control by an independent authority.

OECD -> GDPR

- OECD Privacy Principles (1980) ->

  Data Protection Directive (Directive 95/46/EC) ->

  General Data Protection Regulation (EU Regulation 2016/679)

OECD Principles (1980)

- Collection limitation
- Data quality
- Purpose specification
- Use limitation
- Security Safeguards
- Openness
- Individual participation
- Accountability

GDPR Principles (Article 5)

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality
- Accountability

GDPR Influence on Canadian Reform Proposals (examples)

Grounds for Processing

GDPR Article 6

- 1. Processing shall be lawful only if and to the extent that at least one of the following applies:
  - (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
  - (b) processing is **necessary for the performance of a contract** to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
  - (c) processing is **necessary for compliance with a legal obligation** to which the controller is subject;
  - (d) processing is **necessary in order to protect the vital interests of the data subject** or of another natural person;
  - (e) processing is **necessary for the performance of a task carried out in the public interest** or in the exercise of official authority vested in the controller;
  - (f) processing is **necessary for the purposes of the legitimate interests pursued by the controller** or by a third party, **except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child.

Canada

C-11

Consent required

- **15 (1)** Unless this Act provides otherwise, an organization must obtain an individual's valid consent for the collection, use or disclosure of the individual's personal information.

Exceptions to Consent

- **Business Operations:** Sections 18 – 28
  - See in particular the overlap between s.18 (Business Activities) and GDPR 6(1)(f)
- **Public interest**: Sections 29 – 39

See also Ontario's discussion of "thoughtful consent and lawful uses of personal data", and BC's "align the exemptions to consent in PIPA with those of the GDPR."

Grounds for Processing (cont'd)

GDPR Article 6(1)(f)

- Processing shall be lawful only if and to the extent that at least one of the following applies:
  - … **for the purposes of the legitimate interests pursued by the controller** or by a third party, **except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject** which require protection of personal data, in particular where the data subject is a child.

Canada

s.18 – Business Activities

Collection/use is permissible if it is for a described business purpose, and a reasonable person would expect such a collection or use for that activity …

(e) an activity in the course of which obtaining the individual's consent would be impracticable because the organization does not have a direct relationship with the individual; and

De-identification (definitions)

GDPR Article 4

- '**pseudonymisation**' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;

Anonymous or anonymized information is defined less directly in Recital 26, as:

> "... information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable."

Canada

C-11

> ***de-identify*** means to modify personal information — or create information from personal information — by using technical processes to ensure that the information does not identify an individual or could not be used in reasonably foreseeable circumstances, alone or in combination with other information, to identify an individual.

Ontario

> "**de-identified information**" means information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information.
>
> **Anonymized information**: this Act does not apply to information [that] has been altered irreversibly, according to generally accepted best practices, in such a way that no individual could be identified from the information, whether directly or indirectly by any means or by any person.

De-indexing

GDPR

Article 17 – Right to Erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

> (c) the **data subject objects** to the processing pursuant to Article 21(1) and there are **no overriding legitimate grounds** for the processing, or the data subject objects to the processing pursuant to Article 21(2);

See also Google Spain decision.

Canada

Quebec Bill 64

The person to whom personal information relates may require… an enterprise to cease disseminating that information or to de-index any hyperlink attached to his name … where the following conditions are met:

(1) the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;

(2) the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and

(3) the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury

vs. C-11. s. 55 (Disposal at individual's request)

De-indexing

GDPR

Article 17 – Right to Erasure

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

> (c) the **data subject objects** to the processing pursuant to Article 21(1) and there are **no overriding legitimate grounds** for the processing, or the data subject objects to the processing pursuant to Article 21(2);

See also Google Spain decision.

Canada

C-11. s. 55 (Disposal at individual's request)

"If an organization receives a written request from an individual to dispose of personal information that it has collected from the individual, the organization must, as soon as feasible, dispose of the information …"

Fines

GDPR Article 83

General conditions for imposing administrative fines

5. "... up to 20 000 000 EUR or ... up to 4% of the total worldwide annual turnover"

Canada

C-11: $25M or 5% of global gross revenue*

Quebec Bill 64: $25M or 4% of worldwide turnover

Ontario: $25M or 5% of gross global revenue

British Columbia: AMPs "set at an amount that is a sufficient deterrent to contraventions of the Act."

California Privacy Rights Act

Section 1798.155

Any business, service provider, contractor or other person that violates this title shall be liable for an administrative fine of not more than two thousand five hundred dollars (**$2,500**) for each violation, or seven thousand five hundred dollars (**$7,500**) for each intentional violation or violations involving the personal information of consumers whom the business, service provider, contractor or other person has actual knowledge is under 16 years of age ...

GDPR Influence on Organization Practices

Extra-territorial Scope

Article 3(2)

2. This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union.

- Similar: PIPEDA applies where there is a “real and substantial connection” to Canada.

Adequacy

Article 45 – Transfers on the basis of an adequacy decision

1. A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

2. When assessing the adequacy of the level of protection, the Commission shall, in particular, take account of the following elements:

a) the rule of law, respect for human rights and fundamental freedoms, relevant legislation …

b) the existence and effective functioning of one or more independent supervisory authorities in the third country or to which an international organisation is subject …

c) the international commitments the third country or international organisation concerned has entered into …

- The point is not to "mirror point by point the European legislation, but to establish the essential, core requirements of that legislation."
- Canada has "partial adequacy", based on evaluation of PIPEDA in 2001; others listed here

Regulatory Approaches – Co-regulation

GDPR Approaches

Article 36 – Prior consultation

- Where a Data Protection Impact Assessment indicates a high risk in the absence of mitigating measures, the controller shall consult the supervisory authority.

Article 40 – Codes of Conduct

- Member states, supervisory authorities, etc. shall encourage the development of code of conduct.

Article 42 – Certification

- Member states, supervisory authorities, etc., shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks ….

“Privacy is a right not a privilege. In a world where our personal data can drive everything from the healthcare we receive to the job opportunities we see, we all deserve to have our data treated with respect.

“My role is to work with those to whom we entrust our data so they are able to respect our privacy with ease whilst still reaping the benefits of data-driven innovation. I also want to empower people to understand and influence how they want their data to be used, and to make it easy for people to access remedies if things go wrong.”

ico.
Information Commissioner's Office

John Edwards
Information Commissioner

Link

UK ICO – Guiding Organizations

- Supporting industry-developed condes of conduct under the UK GDPR
  - "Codes of conduct are voluntary accountability tools, enabling sectors to identify and resolve key data protection challenges in their sector with assurance from ICO that the code, and its monitoring, is appropriate."
  - ICO role:
    - Provide advice and guidance to bodies considering or developing a code;
    - check that codes meet the code criteria;
    - accredit (approve) monitoring bodies;
    - approve and publish codes of conduct; and
    - maintain a public register of all approved UK codes of conduct.
    - See: Codes of conduct
- ICO-led Codes of Practice:
  - Age appropriate design code ("Children's code", September 2020)
  - Data sharing code (September 2021)
  - Anonymisation code
    - To be updated based on data sharing code; consultation on-going

Codes of Practice, cont'd

- EU has only approved one code under the GDPR: the Cloud Code of Conduct
  - Focuses on protection of data in cloud services
  - Lengthy development and approval process – started in 2012; Belgian DPA involved as of 2016; approved in 2021
- No approved Certification Programs
  - Required guidance from the EDPB
  - Some in process, such as EuroPriSe

Canada

C-11: s.76-81 set out a scheme by which an entity may … apply to the Commissioner for approval of a code of practice that provides for substantially the same or greater protection of personal information as some or all of the protection provided under this Act.

UK ICO – Guiding Organizations (cont'd)

- Audits
  - ICO auditors review whether an organization has "effective controls in place alongside fit for purpose policies and procedures to support your data protection obligations."
  - Based on agreed upon scope of work; can be issue-specific
  - Organization receives comprehensive report; ICO publishes executive summary
- Advisory check-ups
  - Aimed at SMEs; up to 2-hour session to review practices and develop a plan for privacy as the organization grows.

Canada – C-11

s.10: An organization must, on request of the Commissioner, provide the Commissioner with access to the policies, practices, and procedures that are included in its privacy management program.

s.109(e): The Commissioner must on request by an organization, provide guidance on the organization's privacy management program.

UK ICO – Guiding Organizations (cont'd)

Regulatory Sandboxes

- Essentially, an opportunity to do a live, supervised test of an innovative product, service, or technology
- 2019 beta phase chose applicants that were (see summary here):
  - innovative in the use of personal data
  - of demonstrable public benefit, and
  - operating in a genuinely challenging or 'grey area' of data protection law.
- Also adopted by Norway: Sandbox for responsible artificial intelligence

Further reading: Centre for Information Policy Leadership, Regulatory Sandboxes in Data Protection: Constructive Engagement and Innovative Regulation in Practice

Canada – Ontario IPC has expressed significant interest in this concept.

Regulatory Approach - Enforcement

GDPR Approaches

Article 57 – Tasks [of the supervisory authority]

57(1) Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory:

(a) monitor and enforce the application of this Regulation;

…

Article 58 – Powers

58(2) – (a) Issue warnings

(b) Issue reprimands

(c) Order the controller to comply with data subject requests to exercise rights

(d) Order the controller to bring operations into compliance

(f) Impose a temporary or definitive limitation, including a ban on processing

…

(i) Impose an administrative fine (see **Article 83(2)** for considerations)

(j) Order the suspension of data flows to a recipient in a third country

FTC and Privacy

- Acts with privacy elements:
  - s.5 of the FTC Act;
  - Fair Credit Reporting Act;
  - Gramm-Leach-Bliley Act
  - Children's Online Privacy Protection Act (COPPA)
  - Health Breach Notification Rule of *HIPAA*
- S.5 FTC Act is of particular interest:
  - "Unfair or deceptive acts or practices in or affecting commerce … are … declared unlawful"
  - An act or practice is **unfair** if
    - (1) it causes or is likely to cause substantial injury,
    - (2) the injury is not reasonably avoidable by consumers, and (3) the injury is not outweighed by benefits to consumers or competition.
  - A representation, omission, or practice is **deceptive** if it is likely to mislead consumers acting reasonably under the circumstances and is material to consumers – that is, it would likely affect the consumer's conduct or decisions with regard to a product or service.

US Federal Trade Commission

- Arguably, principally a public education / enforcement role
  - See, for instance, PrivacyCon
- Going forward, have indicated a focus on:
  - Providing notice to harmed consumers
  - Obtaining monetary remedies for harmed consumers
  - Obtaining non-monetary remedies for harmed consumers
  - Not allowing companies to benefit from illegally collected data

Comparing Enforcement Outcomes

- Consider Facebook / Cambridge Analytica case (links in course outline)

- Outcomes:
  - UK ICO: £500K fine (maximum available under previous version of Data Protection Act)
  - US FTC: $5B fine, plus variety of orders (settlement)
  - OPC: Application to Federal Court

But, per Houle and Sossin – what makes an effective regulator?

- Focus on outcomes in egregious circumstances? Overall compliance?

Regulatory Strategy

- Irish Data Protection Commission's Regulatory Strategy for 2022-2027
  - Strategic goals:
    - Regulate consistently and effectively
    - Safeguard individuals and promote data protection awareness
    - Prioritise the protection of children and other vulnerable groups
    - Bring clarity to stakeholders
    - Support organizations and drive compliance

- UK ICO's (draft) Regulatory action plan
  - Includes specific sections on "Assessing the outcomes of our regulatory actions"

Proposals to improve privacy regulation

Houle and Sossin – Ombudsman Effectiveness Study

- **Recommendation #2**: Leverage ombudsmodel to achieve compliance with PIPEDA, especially from large businesses; continue to target medium and small business sectors for outreach, education and incentives for compliance
- **Recommendation #3:** Hybrid model (Ombuds model enhanced with limited order-making power)
- **Recommendation #4**: Explicit guideline-making power.
- **Recommendation #5**: Certification program.

CIPL – Regulating for Results

- Centre for Information Policy Leadership: Washington-based think tank, founded in 2001
- Published *Regulating for Results: Strategies and Priorities for Leadership and Engagement* in 2017
- Principles for a Results-based Approach (excerpts):
  - The goal of a DPA should be to produce cost-effective outcomes which protect individuals in practice, promote responsible data use and facilitate prosperity and innovation.
  - Each DPA should adopt a risk-based approach to all its activities, basing priorities on activities that create the most harm to individuals or to democratic and social values.
  - An approach of constructive engagement with the emphasis on leadership, information, advice, dialogue and support will be more effective than excessive reliance upon deterrence and punishment.
  - Emphasis on information and advice is especially important in the field of data protection due to its broad impact on so many organisations and the nature of the requirements that are either not precise or are context driven and require judgement in specific situations
  - Open and honest relationships with organisations handling personal information, based on constructive dialogue and mutual co-operation, but without blurred responsibilities, will improve overall compliance outcomes
  - Organisations trying to behave responsibly and to "get it right" should be encouraged to identify themselves, for example by transparently demonstrating their accountability, their privacy and risk management programmes, the influence of their DPOs and their use of seal / certification programmes, BCRs, CBPR and other accountability frameworks.

Axel Voss – GDPR 2.0

Section V: The guardians (EDPB & DPAs)

“Data protection authorities are too onesided and too much focused on the protection of personal data. Although this is of course their main purpose, they should be obliged to also take other elements such as fairness, equality, health, security, competition, prosperity and innovation into consideration. “

“[DPAs] should also concentrate their resources on major cases.”

“The powers of intervention of DPAs are in fact unprecedented if compared to other regulatory offences. They even exceed the highest possible fines under criminal law. Moreover, the DPAs have access to all information and personal data as well as to all the controller’s premises and data processing equipment, allowing them to effectively shut down businesses by banning their data processing or by imposing lengthy investigation and compliance procedures, which can place a company at a disadvantage on the market.”

“To balance out the EDPB, which has shown itself to be one-sided, a European Data Innovation Board should be established. It should feature representatives from research and industry, and have a statutory remit to issue comments, interpretations and guidelines on how to balance the fundamental right to privacy against the rights to life, liberty, security, and the freedom to conduct business in Europe.”

Alternative approaches to privacy

Single-issue approaches

Single-issue regulation

- Often associated with US-style “patchwork”
  - Video Privacy Protection Act, Children’s Online Privacy Protection Act (COPPA), Fair Credit Reporting Act, Health Information Portability and Accountability Act, …

- Occurs at the State-level, too
  - See, for instance, Illinois Biometric Information Privacy Act

A tool for local regulation / issues?

- UK Surveillance Camera Commissioner
  - Surveillance Camera Code of Practice
  - Third-party certification scheme
- City-level bans on facial recognition / "surveillance technology"
  - For instance: Alameda, CA; Baltimore, MD; Berkeley, CA; Boston, MA; Brookline, MA; Cambridge, MA; Jackson, MS; King County, WA; Minneapolis, MN; New Orleans, LA; Northampton, MA; Oakland, CA; Portland, ME; Portland, OR; San Francisco, CA; Somerville, MA; Springfield, MA
- On-going discussions around ride-sharing data (and the Mobility Data Specification)
  - See also: "Cities, mobility companies agree to 7 guidelines to keep rider data private"

Does AI Warrant Single-Issue Regulation?

- **EU**: Artificial Intelligence Act

- **Australia**: As part of an overall roadmap for responsible innovation, the Australian Human Rights Commissioner called for the creation of an AI Safety Commissioner, "focused on promoting safety and protecting human rights in the development and use of AI in Australia."

- **China**: Three approaches – rules for online algorithms, tools for testing and certification of AI systems, establishing AI ethics principles and creating tech ethics review boards (see summary from Carnegie Endowment for International Peace)

For consideration:

Are there issues that might warrant moving away from Canada's broad sectoral approach?

Accountability approaches

(aka – What if we accept that consent is the "biggest lie on the Internet")

IAF – FAIR and OPEN USE Act

- Basis: "… this is observational age where individuals' information can be obtained and used without them knowing about it, and the data obtained through that observation drives advanced analytics … which, in turn, drives today's digital society and economy."
- Intention: Create a "Model Data Protection Law fit for 2030"
- Three principles to the FAIR and OPEN USE Act
  - **Accountable and Measurable**: Organizations must be responsible for how data are used and be answerable to others for the means taken to be responsible.
  - **Informing and Empowering**: Organizations have a proactive obligation to inform stakeholders about the data processed, the processes used to assess and mitigate risk, and an individual's ability to exert control and make choices.
  - **Competency, Integrity, and Enforcement**: Organizations are evaluated by the competency they demonstrate in reaching decisions to process data, their honesty, disclosures and actions. A well-resourced and capable regulatory enforcement mechanism is necessary to help ensure trust and compliance … but the Model Legislation contemplates that there is a difference between systematically bad decisions and anomalies.

Data availability approaches

EU Data Governance Act

- Key regulatory aims (per November 30, 2021 EC press release)
  - Measures to increase trust in data sharing as the lack of trust is currently a major obstacle and results in high costs;
  - New EU rules on neutrality to allow novel data intermediaries to function as trustworthy organisers of data sharing;
  - Measures to facilitate the reuse of certain data held by the public sector. For example, the reuse of health data, under clear conditions, could advance research to find cures for rare or chronic diseases;
  - Tools to give Europeans control over the use of the data they generate by making it easier and safer for companies and individuals to voluntarily make their data available for the wider common good under clear conditions.

Australian Data Commissioner

- Data Availability and Transparency Act (currently before Australian Parliament) would establish means for organizations to request controlled access to government data for"
  1. Improving government service delivery
  2. Informing government policy and programs
  3. Research and development
- Data Commissioner assesses request based on: Why the data is being used (Projects Principle); Who is using the data (People Principle); Where the data is being used (Settings Principle); What data is appropriate (Data Principle); How the results of the project are used (Outputs Principle)
  - Based on the "5 Safes" framework
- Data Commissioner will also accredit users and data service provides

(Recall that Canada's 2021 Federal Budget included $17.6M to establish a Data Commissioner, which "would inform government and business approaches to data-driven issues to help protect people's personal data and to encourage innovation in the digital marketplace."

Data subject empowerment approaches

A Human-Rights Based Approach to Data

- Established by the United Nations Office of the High Commissioner for Human Rights (OHRCR)
- As part of 2030 Agenda for Sustainable Development, developed set of principles for a human-rights based approach to data.
  - **Participation**: Participation of relevant population groups in data collection exercises, including planning, data collection, dissemination and analysis of data.
  - **Data Disaggregation**: Disaggregation of data allows data users to compare population groups, and to understand the situations of specific groups. Disaggregation requires that relevant characteristics are collected
  - **Self-Identification**: For the purposes of data collection, populations of interest should be self-defining. Individuals should have the option to disclose, or withhold, information about their personal characteristics.
  - **Transparency**: Data collectors should provide clear, openly accessible information about their operations, including research design and data collection methodology. Data collected by State agencies should be openly accessible to the public.
  - **Privacy**: Data disclosed to data collectors should be protected and kept private, and confidentiality of individuals' responses and personal information should be maintained.
  - **Accountability**: Data collectors are accountable for upholding human rights in their operations, and data should be used to hold States and other actors to account on human rights issues.

First Nations Principles of OCAP®

- Established / overseen by the First Nations Information Governance Centre
- **Ownership** refers to the relationship of First Nations to their cultural knowledge, data, and information. This principle states that a community or group owns information collectively in the same way that an individual owns his or her personal information.Access:
- **Control** affirms that First Nations, their communities, and representative bodies are within their rights in seeking control over all aspects of research and information management processes that impact them. First Nations control of research can include all stages of a particular research project, from start to finish. The principle extends to the control of resources and review processes, the planning process, management of the information and so on.

First Nations Principles of OCAP®

- **Access** refers to the fact that First Nations must have access to information and data about themselves and their communities regardless of where it is held. The principle of access also refers to the right of First Nations communities and organizations to manage and make decisions regarding access to their collective information. This may be achieved, in practice, through standardized, formal protocols.
- **Possession** While ownership identifies the relationship between a people and their information in principle, possession or stewardship is more concrete: it refers to the physical control of data. Possession is the mechanism by which ownership can be asserted and protected.

End Part One