

# Effective privacy and access to information legislation in a data driven society

## Resolution of the Federal, Provincial and Territorial Information and Privacy Commissioners

Charlottetown, PEI, October 1-2, 2019

### CONTEXT

Privacy and access to information are quasi-constitutional rights that are fundamental to individual self-determination, democracy and good government. New technologies have numerous potential benefits for society but they have impacted fundamental democratic principles and human rights, including privacy, access to information, freedom of expression and electoral processes.

Increasingly, the public is concerned about the use and exploitation of personal information by both governments and private businesses and, in particular, the opaqueness of information handling practices. Security breaches are happening more often and have impacted millions of citizens.

While it is important to acknowledge that there have been legislative advances made in some Canadian jurisdictions, there is still ongoing work required to enhance and establish consistent modernization. Most Canadian access and privacy laws have not been fundamentally changed since their passage, some more than 35 years ago. They have sadly fallen behind the laws of many other countries in the level of privacy protection provided to citizens.

### THEREFORE

Canada's Information and Privacy Commissioners call on their respective governments to modernize legislation that strives to meet the following principles:

#### **In terms of privacy:**

- All public and private sector entities, including political parties, engaged in collecting, holding, using and disclosing personal information are subject to privacy laws;
- All public and private entities are required to establish and implement privacy management frameworks that include at minimum policies and practices designed to comply with relevant privacy laws and stand ready to demonstrate accountability;
- Transparency requirements to the public are strengthened with respect to privacy practices of public and private entities, including information sharing initiatives;
- Public and private entities are bound to practice data minimization and limited use, and use advanced privacy protection techniques, such as de-identification, whenever possible;
- Privacy impact assessments are mandated for all initiatives that involve personal information. They are a criterion for all public funding of such initiatives;
- Individuals are protected from the intrusive use of technology and ubiquitous surveillance;

- Public and private entities are required to establish appropriate security measures safeguarding personal information they hold;
- Public and private entities are mandated to notify regulators and individuals affected by privacy breaches;
- Individuals have control over their personal information including real choice and meaningful consent, except for specific circumstances included in privacy legislation. Any new exception is limited to circumstances where the societal benefits clearly outweigh the privacy incursions, and is accompanied by prescribed legal conditions that could be used to demonstrate accountability;
- Individuals are able to access and correct any personal information, including information that is inferred or attributed to the individual that is created by a public or private entity;
- Entities are obligated to use verified, up to date and accurate data;
- Digital literacy is part of training and awareness, especially for children;
- Artificial intelligence and machine learning technologies are designed, developed and used in respect of fundamental human rights, by ensuring protection of privacy principles such as transparency, accountability, and fairness.

**In terms of access to information:**

- Coverage of public entities is as broad as possible, particularly when the entities are performing public functions or substantially financed by public funds;
- Duty to document actions and decisions made by public entities is mandatory;
- Access is free or at minimal cost;
- Responses to access requests are timely and the basis for refusals are clearly explained;
- Exceptions to the right of access are limited and subject to a public interest override;
- Information that is in the public interest is proactively disclosed;
- The right of access applies to information held by public entities in any format, including emails, text messages, etc.

**With respect to enforcement:**

- Individuals have effective means to assert their access and privacy rights and to challenge entities' compliance with their legislated obligations;
- Effective independent oversight offices are sufficiently funded and can rely on extensive and appropriate enforcement powers adapted to the digital environment, such as the power to conduct own-motion investigations and audits, the power to compel records and witnesses as necessary for reviews and investigations, the power to issue orders, and the power to impose penalties, fines or sanctions;
- Commissioners are consulted on changes to legislation that impact access to information or privacy rights.

**Canada's Information and Privacy Commissioners commit to:**

- Engage, collaborate and make recommendations to government, Legislatures and Parliament based on their areas of expertise;
- Continue to study and make public how access and privacy laws impact all Canadians;
- Continue to evaluate innovative privacy and access to information legislation to recommend relevant changes.