Modernizing Canada's *Privacy Act*

Brief by the Canadian Association of Research Libraries

February 12, 2021

Personal information protection is a core value of the library and archival community. Libraries and archives preserve the public record, defend unfettered access to information, and advocate on behalf of both research libraries and public interest for fair privacy laws in Canada. CARL would like to thank the Federal government for consulting with Canadians on ways to protect citizens while encouraging innovation and advancement in Canada. It is critical that important federal legislation such as privacy protection is effective, manageable, and relevant.

We recognize that the Privacy Act is strictly limited to the Federal government, its departments, and agencies however, we urge that this reform be undertaken in consultation, and as much as possible, in alignment with other existing privacy legislation in Canada. This will reduce consumer/public confusion on the management of personal information in Canada.

The importance of maintaining exemptions

Library and Archives Canada's (LAC) core business is the preservation and provision of access to historical information from both public and privately-donated sources and therefore requires exemptions to rules that would apply to other government departments. These are needed for LAC to effectively serve as the memory of the Government of Canada, to provide services and access to Canadians, and to manage and grow its vibrant private and government archival holdings.

The special provisions within the Privacy Act that allow LAC to continue to deliver on its mandate of supporting historical research and that must be retained are:

- Paragraph 8(2)(i) - the ability to collect personal information in instances where it is deemed the information is of archival value;
- Section 8.3 and its related Privacy Regulations, in particular, Regulation 6, which covers personal information transferred to LAC and allows LAC to release personal information 110 years after birth in instances where the date of death cannot be confirmed;
- Article 69 (1) (b) which excludes material from sources other than federal institutions and is an essential provision for LAC in the context of its Private (non-Government of Canada) Archives program. LAC's private archives include prime ministerial and ministerial information, parliamentary information, political and party information, judicial information, and commercial information. LAC's private archival holdings can come from and pertain to individuals or organizations and are subject to different restriction regimes than the Privacy Act. Therefore, these exclusions enable access to historical information that does not come directly from a federal institution.

It is important that Section 12 and Section 13 of the LAC Act is not overridden by any changes made to the Privacy Act. Section 12 of the LAC Act prohibits the destruction or disposition of any information without the written consent of the Librarian and Archivist of Canada. Any provisions in the renewed Privacy Act requiring the automatic destruction of information (e.g., after intended use) would therefore come into conflict with Section 12 of the LAC Act, as well as the authority of the Librarian and Archivist under Section 13 to acquire records he or she deems to have historical or archival value. Changes to the Privacy Act must not conflict with the Library and Archives Act, and must also be coherent with the Government of Canada's Information Management policies defined by Treasury Board Secretariat (TBS).

We recommend that changes not be retroactive so as to mitigate any possible conflicts with how information is retained and used in LAC's current federal government records holdings. We note the uniqueness of LAC's role in records retention and the many private records that go beyond the scope and use of other government records and therefore keeping the exemptions in the Act are critical to allowing LAC to meet its mandate.

Broadening the concept of administrative purposes

Privacy and Artificial Intelligence

Effective management of personal information requires organizations to be transparent and citizens to be informed. Reducing transparency on the use of personal information goes against the core tenets of consumer protection and effective management of personal information. This is particularly important when considering the use of artificial intelligence. Increased transparency provides individuals with more comprehensive information on how their data is being and will be used which allows individuals to make informed decisions.

Individuals should be made aware of the risks involved with making de-identified data public and should be given the right to opt out upon request.

Big data can pose risks for consumers in terms of over surveillance, unregulated sharing and misuse of information, exposure to hacking, and data breaches. The larger the amount of consumer information that is being stored, the greater the risk to individuals.

Regulating personal data collection, storage, and usage to data that is relevant, adequate, and absolutely necessary for carrying out the purpose for which the data is processed, would provide protection for individual privacy and human rights by reducing the risk of exposure of individuals' data.

The increasing use of artificial intelligence (AI) brings with it a myriad of concerns related to privacy, some of which are human rights (by reinforcing bias and systemic racism), transparency, an educated society, and a right to explanation. Democracy, laws, and human rights form the basis of our constitution and it is therefore important these principles are reflected into this technology.

By implementing the principles of Privacy by Design[1] and Human Rights by Design into the very basics of AI design and operation, the act of "checking against privacy, human

[1] Cavoukian, A., Privacy by Design "The 7 Foundational Principles) https://www.ipc.on.c /wp-content/uploads/resources/7foundationalprinciples.pdf

rights, and the basic tenets of constitutional democracy" is effectively embedded into the process. Under the EU General Data Protection Regulation (GDPR), businesses are required to build in Privacy by Design to all operations. Having already undertaken this process in this context, expanding design elements to include the foundational components of human rights would be the logical next step. The Government, its departments, and its agencies should be able to implement these same protocols.

The pervasiveness of AI and the lack of understanding by Canadians of its depth, reach and authority[2] demonstrates the need for explainable AI (XAI) or the right to explanation. According to M. Ridley, author of the 2019 article entitled Explainable Artificial Intelligence, "Algorithmic decision-making, enabled by machine learning, is ubiquitous, powerful, often opaque, sometimes invisible, and, most importantly, consequential."[3] The right to explanation is seen as a method for transparency and accountability for artificial intelligence and other automated systems "that (have) for too long been defined by its opacity."[4]

Protections such as the right to object are meaningless if a person does not understand how the decision was taken and therefore the right to explanation is critical. The OECD AI Principles provide an example of some of the questions that should be considered by industry to be transparent and explainable.[5]

Privacy and Open Government

CARL believes in the direction of open by default/open data/open science as a means to make available information to the public, for the public good--especially that which has been captured or created with public funds. World events in 2020 (e.g., COVID, Blacklivesmatter, etc.) have demonstrated to us the importance of open, unfettered access to research, data, and public policy. For the most part, governments have adopted eight principles of open data as defined by Opengovdata.org : We commend Canada's governments for the movement toward transparency, civic engagement, and e-governance by adopting an open by default perspective.

Governments collect a tremendous amount of information and much of it is personal information about individuals. This can create large datasets of information that can be anonymized and released as open data. However, privacy must be at the forefront of these decisions.

Anonymization is unfortunately not failsafe. One of the main ways of anonymizing data is deidentification, but the 2010 study *Broken Promises Of Privacy: Responding To The*

---

[2] A Deloitte study surveyed 1,000 Canadians and found only 4 percent of survey participants reported they were able to explain what AI is and how it works. The Deloitte study also uncovered that 65 percent reported privacy concerns over the use of the data, 86 percent of Canadians said they don't think they currently use AI technology and 50 percent said they don't believe they will use them in the five years. Nearly a third of those surveyed in the Deloitte research don't think they will ever use AI in their lives. However, according to Statistics Canada 76 percent of Canadians own a smartphone. Deloitte. Canada's AI imperative Overcoming risks, building trust. P. 4, https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/deloitte-analytics/ca-overcoming-risks- building-trust-aoda-en.pdf
Statistics Canada. Life in the fast lane: How are Canadians managing?, 2016. https://www150.statcan.gc.ca/n1/daily-quotidien/171114/dq171114a-eng.htm?HPA=1

[3] Ridley, M. *Explainable Artificial Intelligence*
https://www.google.com/url?q=https://publications.arl.org/18nm1df/&sa=D&ust=1583765950963000&usg=AFQjCNH8V0DL3Stfjfb0kmBnP0GVD3ffNw

[4] Ibid

[5] OECD. Transparency and explainability (Principle 1.3), https://oecd.ai/dashboards/ai-principles/P7

Surprising Failure Of Anonymization[6] discusses a variety of techniques that re-identified personal information in several large datasets that had been made publicly available. According to CIPPIC, "First, when combined with other datasets, anonymous data can be re-identified. Second, personal data can be directly released in "anonymized" datasets, though often accidently. Finally, third parties can use their own data to re-identify anonymous open data."

Sensitive data and data trusts

A public data trust would be acceptable if it is developed with rules of consent, transparency, and the right to explanation. Sharing data through a data trust would need to be disclosed as a purpose and would need consent from individuals when personal data is collected.

This leads to providing the justification for the sharing of data to obtain proper consent. While there are privacy risks associated with open data and data sharing, there is great benefit for governments to continue moving towards open by default. The privacy risks can be managed by implementing 'privacy by design" and its attendant policy and protocols.

The library and archival community considers research data management to be a key component to ensuring appropriate protection of individual privacy while, at the same time, enabling more data to be openly accessible and allowing technology-based research that mines anonymized or aggregated data sets. Research libraries play an increasing role in research data management and are very engaged in defining, practicing, and supporting ethical management of sensitive data, especially personal data.

CARL Portage Network's Sensitive Data Expert Group is composed of a broad membership from research communities – including research ethics professionals, representatives of funding agencies, and members of Indigenous organizations with direct interests in this subject. This group is working to develop practical guides and tools for the management of sensitive research data in the Canadian landscape. The group recently released three guides as part of its Sensitive Data Toolkit for Researchers[7]: Glossary of Terms for Sensitive Data used for Research Purposes, Human Participant Research Data Risk Matrix, and Research Data Management Language for Ethics Approval and Informed Consent. Such tools will support researchers in adhering to current and future privacy laws. The development of technology and policy-based tools to facilitate ethical management of, and appropriate access to, sensitive data supports Canadian research participants by creating new opportunities to contribute data for the public good.

Research libraries are embedded in the research ecosystem. With sensitive data in particular, research libraries work on the front-line -- at the intersection of researchers, institutional policies, data repository requirements, publisher specifications, funder policies, research ethics principles, privacy law, and other competing and overlapping policy frameworks. As technology continues to increase research capacity, the inclusion

[6] 57 UCLA LAW REVIEW 1701 (2010), https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1016&context=hightechevents

[7] Sensitive Data Expert Group publications https://portagenetwork.ca/network-of-experts/sensitive-data-expert-group/

of research libraries as stakeholders in the development of privacy law and policy will ensure strong understanding and representation of research data management considerations, improve Canadian research quality, protect Canadian research participants, and expand appropriate discovery and use of sensitive data.

The Right to be Forgotten (RTBF)

In 1987, CARL adopted a freedom of expression statement which confers responsibility on Canadian research libraries to "facilitate access to all expressions of knowledge, opinion, intellectual activity, and creativity, from all periods of history to the current era, including those which some may consider unconventional, unpopular, unorthodox, or unacceptable."[8] This statement echoes the fundamental right to expressions of knowledge, creativity, and intellectual activities, as embodied in the Canadian Charter of Rights and Freedoms.

The RTBF is a complex ethical and technological issue, which demands a careful balancing of fundamental rights that can at times appear to be in conflict. When considering use of personal information and broadening the administrative scope of that use, the following need to be considered:

- Balancing an individual's right to privacy with others' freedom of expression. Any RTBF approach must ensure that the privacy rights of an individual who is the subject of content on the Internet does not unduly impinge on the expression rights of creators of the content, such as authors or publishers.
- Protecting the over-removal of content. It is important to remember that, for each time that an individual's privacy is protected through a RTBF request, it may muffle the speech of those whose content is being delisted, thereby increasing the spectre of censorship.
- Respecting the integrity of the historical record. Information on the Internet may have future value for both the public and for researchers. We believe an expert assessment of the impact on the historical record, preserved for future generations of Canadians, and ways to mitigate that impact, should form part of every decision to remove information. In recommending this, research librarians recognize that the digital age has increased both the ephemeral nature and the accessibility of historical records that might otherwise have persisted only in physical library or archival repositories.

The Right to be Forgotten should not be able to be too casually invoked by individuals. There are complex considerations to be weighed and rights to be balanced, very likely requiring case-by-case assessment. In most cases, a review by an informed but impartial party is essential.

Privacy Commissioner and administering the *Privacy Act*

Assigning responsibility for the management of the Privacy Act and the provisions contained within is an important role and critical to effectively carrying out the rules in the Act.

The library community's experience with the unintended consequences of the decentralized administration of Crown Copyright, and our resulting advocacy for changes, can assist the Government in avoiding the pitfalls associated with decentralizing

[8] CARL Principles https://www.carl-abrc.ca/about-carl/governance/principles/

oversight. In a 2019 presentation at the ABC Copyright Conference, Amanda Wakaruk notes " Crown copyright applies to a wide range of government agencies with various mandates, some of which rely on cost recovery to finance the production of information and content. The current practice gives flexibility to different governmental branches and agencies to adopt the most appropriate way to handle the content they produce or publish."[9] Unfortunately, this decision by government has in reality created an environment where "Interpretations of existing government terms of use and licenses by government employees are inconsistent and confusing, especially since closure of Crown Copyright Licensing program in 2013"[10]

This example illustrates the value of having a strong centralized area of responsibility for safeguarding privacy. Centralization fosters the consistent and transparent management of personal information, limiting the potential for the misuse and mismanagement of data, and removing confusion from within government departments.

Conclusion

Centralized responsibility for privacy will provide perspective and balance, to respond to the tensions between individual rights and the public good, increasing levels of risk related to AI and big data, and competing interests among various sectors.

About CARL

CARL is the voice of Canada's research libraries. Our members include Canada's 29 largest university libraries and two federal institutions. CARL enhances its members' capacity to advance research and higher education; promotes effective and sustainable knowledge creation, dissemination, and preservation; and advocates for public policy that enables broad access to scholarly information. CARL's two federal member institutions contribute to Canada's research enterprise and collaborate in coordinated efforts with the academic library community, but do not engage in CARL's federal advocacy.

[9] Wakaruk, A., Crown copyright: More than just an outdated provision, p. 18 https://harvest.usask.ca/bitstream/handle/10388/12161/abc%20crown%20copyright_%20more%20than%20just%20an%20outdated%20provision%20may%202019.pdf?sequence=1&isAllowed=y

[10] Ibid