CARL response to Modernizing Privacy in Ontario Empowering Ontarians and Enabling the Digital Economy

SEPTEMBER 3, 2021

Mark Swartz & Katherine McColgan
info@carl-abrc.ca

www.carl-abrc.ca

CARL ABRC
CANADIAN ASSOCIATION OF RESEARCH LIBRARIES
ASSOCIATION DES BIBLIOTHÈQUES DE RECHERCHE DU CANADA

Table of Contents

Introduction and Context **2**

Comments on the Consultation Paper **4**

Rights-based approach to privacy 4

Safe use of automated decision-making 5

Enhancing consent and other lawful uses of personal information 7

Data transparency 9

Data management 10

Conclusion 11

Introduction and Context

The Canadian Association of Research Libraries (CARL) would like to thank the Ontario government for consulting with Canadians on ways to protect the privacy of citizens while encouraging innovation and advancement in Canada. Canadian libraries support the assertion in the paper that digital privacy is essential in order to foster an "advanced digital jurisdiction" and that Ontarians should have the authority and "power to control what personal data they share, when they share it and with whom they share it". CARL submitted a response to the Consultation on Strengthening Privacy Protections in Ontario as well as a response to the Consultation on Developing Ontario's Artificial Intelligence (AI) Framework. Many of the issues raised in this submission were highlighted in our previous responses.

As stated in our previous submissions, personal information protection is a core value of the library and archival community. Libraries and archives preserve the public record, defend access to information and advocate on behalf of research libraries and public interest for fair privacy laws in Canada. Libraries champion strong privacy rights, as is reflected in the IFLA Code of Ethics for Librarians and other Information Workers. This Code - which is offered as a series of ethical propositions for the guidance of individual librarians as well as other information workers - has also been adopted by the Canadian Federation of Library Associations.

As described in position statement 3 in the code:

> Librarians and other information workers respect personal privacy, and the protection of personal data, necessarily shared between individuals and institutions.
>
> The relationship between the library and the user is one of confidentiality and librarians and other information workers will take appropriate measures to ensure that user data is not shared beyond the original transaction.
>
> Librarians and other information workers support and participate in transparency so that the workings of government, administration and business are opened to the scrutiny of the general public. They also recognise that it is in the public interest that misconduct, corruption and crime be exposed by what constitute breaches of confidentiality by so-called 'whistleblowers'.[1]

[1] "IFLA -- IFLA Code of Ethics for Librarians and Other Information Workers (Full Version)," accessed August 19, 2021, https://www.ifla.org/publications/node/11092#privacy).

As research libraries now primarily offer digital collections, protecting library user privacy is essential and becoming much more complicated. In this new digital world, research libraries now license the vast majority of the works in their collections. With licensed content, libraries cede control over elements of library user privacy to both publishers and aggregators, as much of the content licensed for use by libraries is made available through cloud-based platforms. Because of this, vendors and aggregators of library content get unprecedented access to library user data and can "…use a combination of license terms and technological controls to track their use and collect their data without oversight. This raises a host of privacy issues, including potential chilling effects on those who would seek out controversial or revealing subjects such as medical treatments, sexuality, or unpopular belief systems."[2]

A major issue for research libraries is the academic surveillance tools that now proliferate on our campuses. The use of these tools has expanded significantly during the COVID-19 pandemic, as universities search for ways to replicate the in-person learning experience in an online environment. CARL flagged the following examples for consideration in our submission to the Ontario Consultation on Developing Ontario's Artificial Intelligence (AI) Framework:

- Addressing the Alarming Systems of Surveillance Built By Library Vendors
- Elsevier Has Deployed an End-user Tracking Tool for Security. Should Users Be Concerned About Their Privacy?
- Student Privacy and the Fight to Keep Spying Out of Schools: Year in Review 2020
- Cheating-detection companies made millions during the pandemic. Now students are fighting back. One of the companies mentioned in this story (Proctorio) is in litigation with an educational developer, Ian Linkletter, from the University of British Columbia for posting a series of tweets linking to Proctorio faculty training videos, which the company considers to be confidential. Linkletter is a vocal critic of "academic surveillance software" tools, and this action demonstrates the aggressive stance that this industry can take in silencing its critics.[3]

Research libraries believe that strong privacy laws are essential as we strive to protect our users from unfettered data collection and surveillance. Libraries can put in place

[2] Aaron Perzanowski, *The End of Ownership: Personal Property in the Digital Economy*, The Information Society Series (Cambridge, Massachusetts: The MIT Press, 2016), 342.

[3] "Ed-Tech Specialist Fights Proctorio Lawsuit | Inside Higher Ed," accessed August 19, 2021, https://www.insidehighered.com/quicktakes/2020/10/20/ed-tech-specialist-fights-proctorio-lawsuit.

policies and practices to protect users, but there must also be strong legislation to reinforce the principles articulated in our policies at both the federal and provincial level. Libraries believe that strong privacy rights in the digital environment are essential for all Canadian citizens, and we support the efforts of the Ontario government to modernize their laws with this as a cornerstone.

Comments on the Consultation Paper

CARL generally supports many of the recommendations in the consultation paper and offers the following comments:

Rights-based approach to privacy

We agree that Ontario should establish a fundamental right to privacy as the underpinning principle for a provincial privacy law, ensuring that Ontarians are protected, regardless of commercial interests.

To help foster public trust and confidence in data practices, CARL supports genuine transparency requirements with strong, independent oversight and significant penalties for breaches as essential elements in the establishment of such a right.

The "fair and appropriate" purposes articulated in the paper would be a step in the right direction, in that organizations should be required to de-identify information when necessary, and that Ontarians should have the right to access, correct, transfer, and dispose, their personal data. CARL supports "privacy by design" and agrees with the proposal on page 5 of the consultation paper, that the Government of Ontario should adopt the "less is more" principle of data minimization that would implement general requirements for organizations to "limit their collection, use and disclosure of data to only that personal information that is necessary to carry out its intended purpose". We have included such principles in our other government submissions, including our privacy related submission to the federal government.[4]

CARL believes that Ontario should introduce the right to be forgotten (RTBF)providing for de-indexing of search results, as is suggested in the sentence "enshrining a requirement for organizations to de-index search results that contain personal information about an individual that has been posted by others" on page 9 of the consultation paper. However, in order to balance individual privacy rights and the importance of maintaining a public record, particularly for archival purposes, it must:

[4] "Modernizing Canada's Privacy Act" (Canadian Association of Research Libraries, February 12, 2021), https://www.carl-abrc.ca/wp-content/uploads/2021/02/210212_CARL_Brief_Modernizing_Canada_Privacy_Act.pdf

1. **Aim to balance 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.

2. **Protect from the over-removal of content.** If RTBF is encoded in legislation, lawmakers and/or regulators must be proactive in reducing the incentives of platforms like Google or Facebook to simply de-list information upon any request. It is important to remember that, for each time that an individual's privacy is protected through a RTBF request, it may muffle freedom of expression rights of those whose content is being delisted, thereby increasing the spectre of censorship.

3. **Respect 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.

More information on the international library community's recommendations on RTBF noted above are reflected in the IFLA Statement on the Right to be Forgotten. In addition, Quebec's Bill 64 (s.28.1) may be a model to examine, as the RTBF in this legislation is subject to countervailing freedom of expression concerns and considerations.

Safe use of automated decision-making

As CARL stated in our response to the Consultation on Developing Ontario's Artificial Intelligence (AI) Framework, AI poses a significant risk to the rights of all Ontarians, and we applaud the government in taking steps towards understanding and mitigating the risks involved. Additional information on CARL's perspective related to privacy and AI can also be found in our Submission to the Office of the Privacy Commissioner's Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence.

We strongly agree with the Government of Ontario that individuals must be protected from AI systems when their use could have serious implications. CARL included a number of examples of harm in the submission linked above, particularly as they relate to biometric information such as facial recognition. Notably, one recent example of extreme harm that the mismanagement of this type of information can cause is currently happening in Afghanistan, where the Taliban have seized "U.S. military biometrics devices that could aid in the identification of Afghans who assisted coalition forces".[5] CARL therefore supports, at minimum, the prohibition, as described in the paper, as it applies to automated data systems (ADS) and profiling, and Ontario should consider a moratorium or extremely limited exceptional use by the government of AI algorithms and associated tools. ADS may be suitable for repetitive, structural processes, but under no circumstances where the harms of discrimination and bias are possible. There must be a recourse for individuals, beyond the organization, to dispute an ADS decision.

Data traceability, allowing research reproducibility, has been the longstanding underpinning of research and is used to validate studies through the process of scientific merit and rigor and to allow other investigators to independently verify findings. It is the basis in which trust is placed in the published findings of research.

CARL supports the principles expressed on pages 13-14 of the consultation paper that are designed to give Ontarians "greater knowledge and control over the use of their data by ADS" and in addition, "enhanced recordkeeping and traceability measures" would help to support the research enterprise.[6] However, we caution that the complex nature of many AI applications may make this unworkable in practice. Steps must be taken to ensure that these efforts do not fall into the same trap as End-User-License Agreement or privacy policies, where the end result is incomprehensible for users. Companies must also be required to document how these complex systems use personal information throughout their development cycle, as this information may get lost over time due to transitions and staff turnover.

CARL recommends that the government of Ontario also consult the following resources:

- Read all of the reports created by the AI Now Institute at New York University. This is an interdisciplinary research center dedicated to understanding the social implications of artificial intelligence. See their list of publications here: https://ainowinstitute.org/reports.html

[5] Ken Klippenstein and Sara Sirota, "The Taliban Have Seized U.S. Military Biometrics Devices," *The Intercept* (blog), August 17, 2021, https://theintercept.com/2021/08/17/afghanistan-taliban-military-biometrics/.

[6] Ministry of Economic Development Government of Ontario, "Public Consultation - Modernizing Privacy in Ontario" (Government of Ontario, Ministry of Economic Development, Job Creation and Trade), accessed August 19, 2021, https://www.ontariocanada.com/registry/view.do?postingId=37468.

- Carefully consider the points raised by the EFF in their Covid-19 and Digital Rights post referenced above: https://www.eff.org/issues/covid-19 and their general page on AI: https://www.eff.org/issues/ai

- Examine the critiques of systems in place in other jurisdictions, for example, AlgorithmWatch has a comprehensive critique of the shortcomings of trustworthy AI here: https://algorithmwatch.org/en/trustworthy-ai-is-not-an-appropriate-framework/ While writing from a European perspective, many AlgorithmWatch publications can help inform what we are doing in Ontario: https://algorithmwatch.org/en/publications/

In the book chapter "AI and "Equality by Design": Automated (In) Justice, (In) Equality, and the Rule of Law", Bita Amani posits that Canada could adopt "Equality by Design", a similar approach to privacy by design which would "would seek to provide the same recognition and design oriented safeguards for protecting equality and inclusivity as normative regulatory values integral to AI governance in general, and to predictive analytics and machine learning in particular."[7]

Enhancing consent and other lawful uses of personal information

CARL agrees with the assertions in the discussion paper that strengthen the authority of consent. We also agree that broad consent requirements can lead to a proliferation of legal notices and dense privacy policies, leading to consent fatigue, as noted on page 16 of the discussion paper. These comments mirror those that we included above that relate to AI.

Studies show that privacy policies are hard to read, are read infrequently, and do not support rational decision making. In a study conducted by researchers at Carnegie Mellon University exploring how users treated privacy policy statements published on corporate websites, the researchers concluded that the length of privacy policies is a primary reason they are regularly ignored.[8] Similarly, the New York Times conducted an analysis of 150 privacy policies. In their analyses of Facebook's privacy policy, which takes about 18 minutes to read, they found that, when comparing with a number of classic texts, "only Immanuel Kant's famously difficult 'Critique of Pure

[7] Bita Amani, "AI and 'Equality by Design'" ch. 11 in Artificial Intelligence and the Law in Canada (Toronto: LexisNexis Canada, 2021) at 270.

[8] Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society 2008 Privacy Year in Review issue*, http://www.is-journal.org/.

Reason' registers a more challenging readability score than Facebook's privacy policy."[9]

If solutions can be found to reduce the time needed to read such policies, it may result in more users reading them and using them to inform their decisions.

Another study that reviewed the effectiveness of informed consent in clinical research discovered that "although informed consent is an important process in clinical research, its effectiveness and validity are always a concern. Issues related to understanding, comprehension, competence, and voluntariness of clinical trial participants may adversely affect the informed consent process. Communication of highly technical, complex, and specialized clinical trial information to participants with limited literacy, diverse sociocultural background, diminished autonomy, and debilitating diseases is a difficult task for clinical researchers".[10]

CARL supports the inclusion of specific exceptions in Ontario legislation rather than a "catch all" category like "any other prescribed activity" as is provided in Bill C-11. CARL believes that the permitted categories and concepts listed from page 18-23 must be carefully scoped and defined, in order to prevent the misuse of personal information. The two examples that are most applicable to the function of research libraries are those for public interest research and records of historic or archival value, as specified on page 22. CARL believes that, even in cases where these categories would benefit our users, questions remain as to the scope of public interest research and who determines if the criteria are met.

Libraries and their users are not immune to the impacts of surveillance technologies. As described in the Addressing the Alarming Systems of Surveillance Built By Library Vendors article that we included as a resource in the introduction to this paper, two major third party library vendors (RELX and Thomson Reuters) have implemented "online tracking technologies, massive aggregation of user data, and the sale of services based on this tracking, including to governments and law enforcement". If Ontario strengthens the framework of authority that permits organizations to collect, use and disclose the personal data of individuals, it will provide leverage for libraries and other related organizations to remove the ability for these organizations to collect data that is not integral to the provision of services for the library or its users.

[9] Kevin Litman-Navarro, "Opinion | We Read 150 Privacy Policies. They Were an Incomprehensible Disaster.," *The New York Times*, June 12, 2019, sec. Opinion, https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.

[10] Rashmi Ashish Kadam, "Informed consent process: A step further towards making it meaningful!." Perspectives in clinical research vol. 8,3 (2017): 107-112. doi:10.4103/picr.PICR_147_16

Data transparency

CARL believes that stronger transparency laws are a critical cornerstone of modern privacy law, and that, as is asserted in the consultation paper, “privacy rights cannot be meaningful unless individuals are provided with the knowledge needed to exercise them.”[11]

We also support the proposal outlined on pages 26 and 27 that organizations be required to implement a privacy management program that governs the collection, use, disclosure, retention, and destruction of personal information. The program developed should be available for review, and the consent process should include clear, concise information that helps users easily understand the implications of consent and make informed decisions.

As stated above, while CARL supports transparency generally, the complex nature of many AI applications may make transparency unworkable in practice. Steps must be taken to therefore ensure that efforts at transparency do not fall into the same trap as End-User-License Agreement or privacy policies, where the end result is incomprehensible for users.

With this in mind, Big Data, AI, and the Internet of Things have created a society where the amount of data being produced worldwide has increased from 2 zetabytes in 2010 to 41 zetabytes in 2019. This is expected to increase 175 zetabytes by 2025.[12] Being able to effectively manage this data is becoming increasingly difficult at the same time as becoming increasingly important. It would be difficult to imagine that ensuring compliance with principles of data accuracy, transparency, access and correction and accountability, could be met without having data management systems in place to ensure the traceability of the data being used in the decision-making process.

In addition, balancing transparency and privacy is critical and requires careful consideration of the risk of data being re-identifiable. In a 2015 article[13] Conroy and Scassa explore the implications of open government and open data in relation to privacy. The article proposes three considerations for effective governance in this area

[11] Ministry of Economic Development Government of Ontario, “Public Consultation - Modernizing Privacy in Ontario” (Government of Ontario, Ministry of Economic Development, Job Creation and Trade), accessed August 19, 2021, https://www.ontariocanada.com/registry/view.do?postingId=37468.

[12] “Total Data Volume Worldwide 2010-2025,” Statista, accessed August 31, 2021, https://www.statista.com/statistics/871513/worldwide-data-created/.

[13] Amy M. Conroy and Teresa Scassa, “Promoting Transparency While Protecting Privacy in Open Government in Canada,” *Alberta Law Review* 53, no. 1 (2015): 175, https://canlii.ca/t/6vm.

that could help the Ontario government in making data transparent referred to on Page 25 of the consultation paper:

1. **Purpose-driven approach -** "…considers the purpose for the collection of the data in the first place in order to search for guidance as to whether and to what extent such data should be disclosed proactively or as open data".

2. **Re-identification risk -** ensuring there is sufficient expertise in public institutions to engage in a re-identification risk analysis of the data prior to release. This principle would have to apply also to the private sector, could benefit from evolving codes of best practices to be developed by the Office of the Information and Privacy Commissioner of Ontario in consultation, and would need systems in place to ensure compliance.

3. **Unpacking transparency rationales for disclosure -** "…that the rejection of speculative approaches and erring on the side of transparency are clear indicators that transparency will trump privacy unless the risks for identifiable individuals can be demonstrated. The challenge is therefore to develop a principled approach to the release of government information that recognizes the privacy-transparency spectrum and ensures adequate consideration is given to each value."

Data management

Although not mentioned in the consultation document, CARL sees research data management as key 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. The NDRIO 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 and 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: 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 of 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.

We also would like to reiterate our previous comments on the requirements of Indigenous communities, who are entitled to full sovereignty over their data under the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP). Data sovereignty would require that governments and researchers recognize Indigenous Peoples' own governance mechanisms to address management, ownership, and control of their own data, and that any use of this data be fully transparent and used only after thorough consultation and with consent.

More information is available here:

- The First Nations Principles of OCAP® | The First Nations Information Governance Centre
- Indigenous Data Sovereignty: Towards an Agenda
- United Nations Declaration on the Rights of Indigenous Peoples

Conclusion

Personal information protection is a core value of the library and archival community. Libraries and archives preserve the public record, defend access to information and advocate on behalf of both research libraries and public interest for fair privacy laws in Ontario. CARL would like to thank the Ontario government for consulting with Canadians

on ways to protect citizens while encouraging innovation and advancement in Canada. We look forward to continued discussions and welcome the opportunity to expand on any of the points provided in this document should further clarity be needed.