Canadian Association of Research Libraries' submission on the Office of the Privacy Commissioner of Canada's Proposals for ensuring appropriate regulation of artificial intelligence

March 13, 2020

Libraries preserve the public record, defend access to information and advocate on behalf of both research libraries and public interest for fair privacy laws in Canada, particularly in the context of technology and technological advancements. We agree, in principle, that there is a need for legislative or regulatory guidance for AI, not only as it relates to the use of technologies, but also for the treatment of data, including the management and preservation of data. We are cognizant of the fact that AI is a rapidly evolving area, and that many of the potential advancements (and their implications) are hard to predict and are therefore very difficult to consider in legislation.

The Canadian Association of Research Libraries (CARL) welcomes the opportunity to provide the perspective of the library community on the implications of artificial intelligence (AI) and its relation to Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA). Our submission to this consultation looks at the following selection of questions from the consultation paper.

Proposal 2: Adopt a rights-based approach in the law, whereby data protection principles are implemented as a means to protect a broader right to privacy—recognized as a fundamental human right and as foundational to the exercise of other human rights

1. *What challenges, if any, would be created for organizations if the law were amended to more clearly require that any development of AI systems must first be checked against privacy, human rights and the basic tenets of constitutional democracy?*

   Democracy, laws, and human rights form the basis of our constitution and it is therefore important these principles are enveloped into this new 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

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

privacy, human rights, and the basic tenets of constitutional democracy" is effectively embedded into the process.

Businesses must, under the EU General Data Protection Regulation (GDPR), now 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.

Proposal 3: Create a right in the law to object to automated decision-making and not to be subject to decisions based solely on automated processing, subject to certain exceptions

"Based solely" on automated processing is a topic that remains open for discussion.

As noted in the GDPR "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her." and goes further to provide specific circumstances where "based solely" would not apply:

> "A primary limitation is the narrow definition of automated decision-making in Article 22(1),91 defined as:
>
> a decision based solely on automated processing, including profiling, which produces legal effects concerning [the data subject] or similarly significantly affects him or her."[2]

It has also been determined in the *Directive on Automated Decision-Making*[3] that departments must use the *Algorithmic Impact Assessment*[4] to assess and mitigate the impacts associated with deploying an automated decision system" and requires human oversight to those areas that are deemed to have a high impact level. Parameters will need to be developed to determine what is an acceptable level of human oversight that will allow for solely automated decision-making to occur.

1. *Should PIPEDA include a right to object as framed in this proposal?*

   Although the above notes there is likely going to be human oversight to automated decision-making, there should be, nonetheless, the right to object clause. The right to object, however, assumes that the subject (or user) understands the processes undertaken by AI in order to be able to assess whether the analysis is valid or not.

[2] Art. 22 GDPR Automated individual decision-making, including profiling, https://gdpr-info.eu/art-22-gdpr/
[3] Government of Canada, Directive on Automated Decision-Making https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592
[4] Government of Canada https://open.canada.ca/aia-eia-js/?lang=en

With the right to object comes the need for explainability which is discussed later in this paper.

2. *If so, what should be the relevant parameters and conditions for its application?*

The GDPR states "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her"[5] however, there are questions to consider with this directive.

Can the objection be overruled? If so, what are the circumstances that would allow this to occur? The GDPR provides exceptions where objections would not stand; "is necessary for entering into, or performance of, a contract between the data subject and a data controller; is authorized by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or is based on the data subject's explicit consent."[6]

It is important to note that these exceptions, however, may infringe on rights of the subject such as intellectual property for example.

Proposal 4: Provide individuals with a right to explanation and increased transparency when they interact with, or are subject to, automated processing

"Algorithmic decision-making, enabled by machine learning, is ubiquitous, powerful, often opaque, sometimes invisible, and, most importantly, consequential."[7] The pervasiveness of AI and the lack of understanding of its depth, reach and authority is what has created the need for explainable AI (XAI) or the right to explanation.

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." [8]

In addition, as mentioned previously in this document, the right to object is meaningless if the subject does not understand how the decision was taken and therefore the right to explanation is critical.

1. *What should the right to an explanation entail?*

[5] Art. 22 GDPR Automated individual decision-making, including profiling, https://gdpr-info.eu/art-22-gdpr/
[6] Ibid
[7] Ridley, M. *Explainable Artificial Intelligence* https://www.google.com/url?q=https://publications.arl.org/18nm1df/&sa=D&ust=1583765950963000&usg=AFQjCNH8V0DL3Stfjfb0kmBnP0GVD3ffNw
[8] Ibid

The GDPR requests a subject has the "right to explanation"[9] but omits details of what a right to explanation should include, leaving industry the responsibility to determine that explanation. The US Defense Advanced Research Projects Agency (DARPA) has developed a definition for XAI that is referenced heavily; "... enable end users to understand, appropriately trust, and effectively manage the emerging generation of Artificial Intelligence (AI) systems."[10]

The questions then are to determine what information needs to be provided for users to understand and what is deemed to be an appropriate level of trust?

The OECD AI Principles provide an example of some of the questions that should be considered by industry to be transparent and explainable:[11]

1. foster a general understanding of AI systems,
2. make stakeholders aware of their interactions with AI systems, including in the workplace,
3. enable those affected by an AI system to understand the outcome, and,
4. enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

2. *Would enhanced transparency measures significantly improve privacy protection, or would more traditional measures suffice, such as audits and other enforcement actions of regulators?*

Increased transparency provides subjects with more comprehensive information on how their data is being and will be used which allows subjects to make better informed decisions.

In a recent study, researchers conducted an online experiment with mobile users to determine the effect transparency had toward their decisions and comprehension of the permission that was being requested.[12]

The researchers determined that "Increased transparency is an essential requirement for making informed consent decisions and might fundamentally

[9] GDPR. Recital 71, Profiling, https://gdpr-info.eu/recitals/no-71/
[10] DARPA. Broad Agency Announcement, Explainable Artificial Intelligence (XAI) DARPA-BAA-16-53 (August 10, 2016), p.5, https://www.darpa.mil/attachments/DARPA-BAA-16-53.pdf
[11] OECD. Transparency and explainability (Principle 1.3), https://oecd.ai/dashboards/ai-principles/P7
[12] Betzing, J.H., Tietz, M., vom Brocke, J. et al. The impact of transparency on mobile privacy decision making. Electron Markets (2019). https://doi.org/10.1007/s12525-019-00332-3

influence users' behavior regarding (mobile) privacy decision making in the long run"[13] and that it did not alter or influence the decisions made.

While creating this environment for users to understand how their data is being used and protected will strengthen accountability from industry, this would not remove the need for audits and other enforcement actions. There would still need to be mechanisms in place to ensure that industry is abiding by its privacy agreements, that every effort is made to inform users to changes in those agreements, and that data is being managed properly.

Proposal 5: Require the application of Privacy by Design and Human Rights by Design in all phases of processing, including data collection

1. *Should Privacy by Design be a legal requirement under PIPEDA?*

   Article 25 of the GDPR "Data protection by design and by default"[14] requires that industry incorporate this process into their data collection activities. Canada would want to consider this as a legal obligation under PIPEDA which would help ensure compliance with international practices and provide privacy protection for Canadians.

2. *Would it be feasible or desirable to create an obligation for manufacturers to test AI products and procedures for privacy and human rights impacts as a precondition of access to the market?*

   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.[15] 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.[16]

   Recognizing the significant gap in knowledge of how AI works and what it can do, manufacturers should be obligated to provide these protections for consumers.

---

[13] Ibid
[14] Art. 25 GDPR. https://gdpr-info.eu/art-25-gdpr/
[15] 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
[16] 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

Proposal 6: Make compliance with purpose specification and data minimization principles in the AI context both realistic and effective

1. *Can the legal principles of purpose specification and data minimization work in an AI context and be designed for at the outset?*
2. *If yes, would doing so limit potential societal benefits to be gained from use of AI?*
3. *If no, what are the alternatives or safeguards to consider?*

According to Article 5 of the GDPR[17] "1. Personal data shall be: c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization');"

"Big Data" provides tremendous financial benefits for industry. It allows companies to analyze consumer behaviour, identify gaps in consumer needs, in order to develop new services and products to sell. However, big data poses inherent risk for consumers. Industry is seeing increases in data breaches exposing consumers' personal information. The larger the amount of consumer information that is being stored,, the greater the risk to individuals.

By 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, it would provide protection for individual privacy and human rights both by reducing the risk of exposure of consumers' data, but also by minimizing the exploitation by industry of consumers' data for the purposes of financial gain.

Proposal 9: Require organizations to ensure data and algorithmic traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle

1. *Is data traceability necessary, in an AI context, to ensure compliance with principles of data accuracy, transparency, access and correction and accountability, or are there other effective ways to achieve meaningful compliance with these principles?*

Data traceability 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.

As a part of accountability and transparency, this too should prevail with algorithmic traceability. This will be a challenge. As previously referenced in this document, the

[17] Art. 5 GDPR Principles relating to processing of personal data https://gdpr.eu/article-5-how-to-process-personal-data/

inherent opacity of algorithmic data is creating challenges for explainability and transparency.

Big Data, AI, 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. [18] 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.

The Canadian Association of Research Libraries (CARL) is a national, bilingual association of twenty-nine major university research libraries as well as two Federal institutions – Library and Archives Canada and the National Research Council's National Science Library. CARL is a member of the International Federation of Library Associations and a founding member of the Canadian Federation of Library Associations (CFLA). CARL's aims are three-fold: to enhance research library capacity to support academic research and higher education; to promote effective and sustainable knowledge creation, dissemination, and preservation; and to ensure public policy that enables broad access to information.

[18] Statista. Volume of data/information created worldwide from 2010 to 2025 https://www.statista.com/statistics/871513/worldwide-data-created/