CUPE·SCFP | Canadian Union of Public Employees
Syndicat canadien de la fonction publique

Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence

Submission of the

Canadian Union of Public Employees

March 2020

Consultation on the OPC's Proposals for ensuring appropriate regulation of artificial intelligence

The Canadian Union of Public Employees (CUPE) is Canada's largest union, with over 700,000 members. CUPE members take great pride in delivering quality public services in communities across Canada through their work in communications, transportation, municipalities, health care, social services, schools, universities and many other sectors. Some of these services are delivered by federally regulated private sector employees, notably in the transportation and communications sectors. CUPE represents workers in every province.

CUPE welcomes the opportunity to comment on the Office of the Privacy Commissioner's (OPC) proposals to regulate artificial intelligence (AI). This is an important initiative given the expansion of AI in many different settings including workplaces where our members are employed and communities where they live. CUPE members such as those in the communications and port sectors are already experiencing the impact of AI in their workplaces.

The legislative and regulatory environment must address the privacy concerns arising from the commodification of data, artificial intelligence and machine learning. This issue has become even more critical in light of the dangerous and unethical violation of data privacy rights by Cambridge Analytica and Facebook.[1] In this context, we are supportive of the recommendations of the OPC to ensure the *Personal Information Protection and Electronic Documents Act* (PIPEDA) appropriately reflects the current technological reality. Furthermore, we encourage the OPC to conduct a similar analysis with regards to the *Privacy Act*, which applies to the federal public sector, its employees and public service users.

Introduction

In this submission CUPE will respond to a number of the proposals and make recommendations for additional proposals to address the needs of workers. From an overarching perspective, CUPE believes the implementation of new technology should serve the public good and should not degrade workers.

PIPEDA addresses the personal information of private sector employees in federally regulated sectors. With the expanding use of technology such as AI in the surveillance and monitoring of workers, we encourage the OPC to expand legislative and regulatory measures to ensure the principles under PIPEDA including consent and limiting collection are expanded beyond the protection of personal information to other types of data that may generated in workplaces. CUPE strongly encourages the OPC to not weaken any aspects of PIPEDA such as those being considered under proposals 6 (limiting purpose specification and data minimization), 7 (alternative grounds when meaningful consent is not practicable) and 8 (flexibility in using information that has been rendered unidentifiable).

We encourage the OPC to strengthen PIPEDA with regard to the privacy implications of outsourcing work to third party corporations. Furthermore, we recommend that privacy issues facing workers be explicitly addressed in the proposals. More broadly, we recommend legislative and regulatory measures that address the human rights and employment and labour effects of AI.

CUPE strongly supports principle 11, which would give the OPC power to issue binding orders and financial penalties as recommended by the Standing Committee on Access to Information,

Privacy and Ethics.[2] We encourage the OPC to consider how to make all aspects of PIPEDA, including new segments related to AI, enforceable. Measures such as binding orders with significant financial penalties and proactive disclosure of human rights and privacy testing and audits would help ensure greater compliance with PIPEDA. As noted in the OPC's 2017-2018 report, respect for privacy laws "must be enforced by a regulator, independent from industry and the government, with sufficient powers to ensure compliance."[3] Recent data breaches from Equifax, Uber, Nissan and data misuse by Facebook/Cambridge Analytica highlight the need for urgent action.

The needs of workers with regards to data collection, privacy and AI

CUPE encourages the OPC to include proposals on the use of AI and the underlying data collection, storage and use in workplaces. The OPC should require a detailed analysis of potential privacy implications when internet technology (IT) work is outsourced to third parties. This information should be proactively disclosed to workers, their union representatives and the public. In many cases, this outsourcing involves a shift from direct control over data to third party corporations based in other jurisdictions.[4] PIPEDA requires organizations to consider privacy when outsourcing work. This requirement should be strengthened to mandate the disclosure of the privacy implications of outsourcing given the growth of AI and other data intensive technology.

Recommendation: Under PIPEDA, the OPC should require a privacy analysis be proactively disclosed when work involving personal data is outsourced to 3rd parties.

The OPC should address situations where AI is used by employers to assess or monitor workers or potential workers. For example, the use of AI in human resource management is already raising concerns with regard to discriminatory practices.[5] Workers must have access to all data collected about them. Workers and their union representatives must be informed about and be able to provide feedback on any AI systems put in place. This should apply to any data collected, not just the collection of personal information as specified within PIPEDA. Specifically:

- Employers must inform workers and their union representatives clearly and fully before the introduction of information systems and technologies within their workplaces.
- If a collective agreement is in force, the collection, use, storage and destruction of data must be bargained prior to implementation of new technology.
- Workers must consent to the collection, use or disclosure of all data related to their work.
- Workers must be able to obtain, upon request, at reasonable intervals and without excessive delay, confirmation of the processing of data relating to them.
- Workers shall have the right to appeal to the strengthened Privacy Commissioner about possible violations of their privacy and human rights by their employers through AI applications and other technology.
- Employers must limit the collection, use and disclosure of data related to employees.
- Employers must develop and disclose a data retention and destruction timetable.

Recommendation: Workers, and their union representatives, must consent to the collection, use or disclosure of all data on them. Workers and their unions must have access to and influence over the data collected about them through AI systems and other technology.

Proposal 1: Incorporate a definition of AI within the law that would serve to clarify which legal rules would apply only to it, while other rules would apply to all processing, including AI

While it may be useful to include a definition of AI within the law, CUPE recommends that the proposals recommended by the OPC and CUPE be applied to all technologies, rather than directed solely at AI. The underlying concern with AI and related technology is the collection, storage, use and destruction of large datasets. If this collection, storage, use and destruction of data is adequately addressed, privacy risks related to AI can be minimized.

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

CUPE agrees that a rights-based approach should be implemented. Personal data should be protected as an extension of the right to privacy.

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

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

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

CUPE supports Proposals 3, 4 and 5, which would give workers and the public greater assurances about the use of AI. In response to proposal 3, CUPE contends that final decisions should be made by humans rather than automated processes. This will limit the potential for AI to jeopardise our safety, privacy or autonomy.[6] Many work functions require a human connection and human judgement that cannot be automated without harming service delivery. Decisions made through AI can have serious consequences and should be subject to oversight.[7]

As for proposal 4, workers, their union representatives and the general public should know when they have been subject to automated decision-making and must have a right to an explanation of the reasoning involved in the decision. This is particularly important given the possibility of algorithmic design biases that result in discriminatory decision making.[8] Workers, their union representatives and the public should also have a right to challenge the results of an automated decision-making process.

CUPE encourages the OPC to pursue a Privacy and Human Rights by Design requirement for all technology as recommended in proposal 5. Research shows that companies tend to deploy new technology prior to adopting security measures.[9] Furthermore, machine learning systems can affect human rights beyond privacy and data protection, including the right to freedom of expression and association, to participation in cultural life, equality before the law, and access to effective remedy.[10] Those who build AI systems are subject to human biases, which can end up in algorithms underpinning AI. The regulation of AI needs to include processes by which these biases can be identified and remedied prior to the implementation of new technology. CUPE supports creating an obligation for manufacturers to test AI products and procedures for privacy and human rights impacts as a precondition of access to the market. This testing should be proactively disclosed so it can be reviewed publicly.

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

CUPE strongly recommends the OPC remain consistent with existing PIPEDA requirements to identify the purpose of data collection and limit the collection, use, disclosure and retention of data. CUPE is already concerned with the number of large datasets that exist, as well as the public availability of datasets from social media platforms. These are often purchased and used by other corporations without the awareness or consent of users. This is not acceptable.

Proposal 7: Include in the law alternative grounds for processing and solutions to protect privacy when obtaining meaningful consent is not practicable

CUPE is concerned about meaningful consent not being received prior to workers and the public being exposed to AI processing systems. Workers, their union representatives and the public should always know what kinds of data is collected and how this data is used. Furthermore, workers, their union representatives and the public should have the right to withhold or withdraw consent to data collection without being deprived of the service. Organizations and corporations collecting data must be required to define, in clear language, the purpose for which they intend to collect and/or use data.

Any exceptions to consent for data use must be tightly regulated and need to be in the public interest. Any automated processes must be approved before they are put into practice. CUPE suggests establishing an independent oversight committee linked to the Office of the Privacy Commissioner which will:

- process these demands for exception
- assess whether the exception is in the public interest
- disclose information publicly about the corporations or organizations involved, how the data will be collected, used, stored and destroyed, and
- administer a complaints and redress procedure prior to and after the implementation of the new technology.

Proposal 8: Establish rules that allow for flexibility in using information that has been rendered non-identifiable, while ensuring there are enhanced measures to protect against re-identification

As previously mentioned, CUPE is concerned about the collection of large datasets, regardless of whether they are rendered non-identifiable. CUPE strongly encourages the OPC to not institute exceptions or relaxation of the PIPEDA principles related to AI.

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

Proposal 10: Mandate demonstrable accountability for the development and implementation of AI processing

CUPE strongly supports proposals 9 and 10 as they institute accountability into the use of data and AI processes. Workers, their union representatives and the public should always be able to trace decisions made through AI systems in order to understand how and why they were made.

CUPE also recommends that all social service AI processes be regulated to include audit trails for all decisions being made at each step of the logic or decision tree. An individual should be able to audit where the decision that deviates from their expectation was made and be able to appeal the specific decision at that point in the process.

CUPE is encouraged to see "demonstrable accountability" proposed which would require organizations to provide evidence of adherence with legal requirements on request. However, CUPE urges the OPC to go one step further and recommend organizations pro-actively publish privacy and human rights impact assessments and independent third party privacy audits. Proactive inspections by the OPC, as proposed in the consultation document, would also provide an incentive for compliance.

Proposal 11: Empower the OPC to issue binding orders and financial penalties to organizations for non-compliance with the law

Empowering the OPC to issue binding orders and financial penalties to organizations who violate the law is critical to foster compliance with PIPEDA. CUPE supports the OPC's recommendation enabling it to impose "consequential penalties". There is much money to be made through the commodification and sale of workers' and the public's data. Many corporations are not likely to respect PIPEDA without a financial incentive to do so. The consultation document notes that organizations who violate the General Data Protection Regulation in the EU can be fined up to 4% of annual global turnover or 20 million Euros. A similar enforcement measure should be applied in Canada.

Conclusion

CUPE is pleased the OPC is considering updates to PIPEDA to reflect changing technology such as AI. We encourage the OPC to follow up on this initiative with an update to the *Privacy Act*.

Workers, and the public, need to give informed consent prior to automated decision-making systems being put in place. Workers, their union representatives and the public need assurance on how and why data is being collected, stored and used. Mass datasets exist and are already being used in ways that violate human rights and privacy rights. The expansion of AI and other technologies involving large datasets could result in even greater privacy and human rights breaches. The role of the OPC needs to be strengthened in order to encourage compliance with the current provisions of PIPEDA and any additional provisions to address AI and other technologies.

CUPE encourages the OPC to consider more fully how PIPEDA can be applied to the use of technologies, including AI in the workplace. Furthermore, when data is shifting hands through outsourcing, PIPEDA should require the organization to conduct and release an audit evaluating the privacy implications.

[1] See discussion and recommendations for Canada: Standing Committee on Access to Information, Privacy and Ethics (June 2018) Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process. House of Commons. 42nd Parliament, 1st session.
[2] Standing Committee on Access to Information, Privacy and Ethics (June 2018) Addressing digital privacy vulnerabilities and potential threats to Canada's democratic electoral process. House of Commons. 42nd Parliament, 1st session.
[3] Office of the Privacy Commissioner of Canada (2017-2018) Trust but verify: Rebuilding trust in the digital economy through effective, independent oversight. https://www.priv.gc.ca/media/4831/ar_201718_eng.pdf
[4] See concerns about the jurisdiction of data storage: Heidi Bohaker, Lisa Austin, Andrew Clement and Stephanie Perrin (2015) Seeing Through the Cloud – National Jurisdiction and Location of Data, Servers, and Networks Still Matter in a Digital Interconnected World. University of Toronto; Lisa M. Austin and Daniel Carens-Nedelsky (May 31st 2015) Why Jurisdiction Still Matters. University of Toronto.
[5] Allen Smith, J.D. (December 12, 2019) "AI: Discriminatory Data In, Discrimination Out". SHRM. Retrieved from https://www.shrm.org/resourcesandtools/legal-and-compliance/employment-law/pages/artificial-intelligence-discriminatory-data.aspx
[6] European Economic and Social Committee (2017) Artificial Intelligence: Europe needs to take a human-in-command approach, says EESC. Retrieved from https://www.eesc.europa.eu/en/news-media/press-releases/artificial-intelligence-europe-needs-take-human-command-approach-says-eesc
[7] See discussion of the dangers of the digital welfare state: Ed Pilkington (October 14, 2019) Digital dystopia: how algorithms punish the poor. The Guardian. Retrieved from https://www.theguardian.com/technology/2019/oct/14/automating-poverty-algorithms-punish-poor
[8] Sarah Myers West, Meredith Whittaker, Kate Crawford (April 2019) Discriminating Systems: Gender, Race and Power in AI. AI Now Institute. Retrieved from https://ainowinstitute.org/discriminatingsystems.html.
[9] Ginger Zhe Jin (December 18, 2017) Artificial intelligence and Consumer Privacy, University of Maryland, NBER Working Paper No. 24253
[10] Rights groups, technologists and researchers (2018) The Toronto Declaration: Protecting the right to equality and non-discrimination in machine learning systems.