WeirFoulds LLP

Privacy in the AI Era? OPC Launches Consultation on Regulation of AI

March 23, 2020

By James G. Kosa, Lisa Danay Wallace

American writer Kurt Vonnegut once penned the line, "You asked the impossible of a machine and the machine complied." Our society has voraciously devoured the possibilities offered by artificial intelligence ("**AI**") systems, urging them to new heights in areas of engineering, medicine, cybersecurity, and art. The machine has complied. Now what? AI systems are capable of processing and analyzing vast amounts of personal information. It is important to recognize that without proper regulation, this developing industry may present significant privacy risk.

The Office of the Privacy Commissioner of Canada ("**OPC**") has stepped in to provide insight on these risks. On January 28, 2020, the OPC launched a consultation paper to solicit comments on its proposal for strengthening private sector privacy law for AI. The paper sets out eleven recommendations to the Government and Parliament to ensure the appropriate regulation of AI.

Summary of the OPC's Proposals

1. **Include a definition of "artificial intelligence"**. Currently, the *Personal Information Protection and Electronic Documents Act* ("***PIPEDA***" or "***Act***") is technology-neutral and a statute of general application. If, as suggested in the paper, there is a need for certain rules to be limited to AI due to its specific risks to privacy, "artificial intelligence" should be defined in *PIPEDA* to clarify when such rules apply.
2. **Adopt a rights-based approach.** *PIPEDA* should be given a rights-based foundation that recognizes privacy in its proper breadth and scope, which will provide direction on how the rest of the provisions in the Act should be interpreted.
3. **Create a right to object to automated decision-making, subject to exceptions.** To meaningfully protect privacy as a human right, *PIPEDA* should permit the ability to object to decisions made by computers and to request human intervention. The OPC recommends adopting the approach in the European Union's *General Data Protection Regulation* ("**GDPR**"), which grants individuals the right not to be subjected to automated decision-making, including profiling, except when an automated decision is necessary for a contract, an automated decision is authorized by law, or where explicit consent is obtained.
4. **Provide a right to explanation and increased transparency.** The OPC proposes that the openness principle under *PIPEDA* should include a right to the explanation that will provide individuals with the reasoning underlying any automated processing of their data, and the consequences of such reasoning for their rights and interests. In addition, the OPC suggests "algorithmic transparency" by mandating public filings of algorithms, similar to US Securities and Exchange Commission filings, with penalties for non-disclosure and non-compliance.
5. **Adopt a "human rights by design" approach.** The purpose of a "human rights by design" approach would be to avoid any potential biases, including unintentional or hidden biases, and the risk of discrimination or other adverse impacts on human rights and fundamental freedom of data subjects.
6. **Make data minimization principles realistic and effective.** A challenge in the AI privacy regime is the tension between purpose specification and data minimization. Organizations relying on AI for advanced data analytics may not necessarily know ahead of time how the information processed by AI systems will be used or what insights they will discover. This has put

into question the practicality of the purpose specification principle, which requires "specifying purpose" to individuals at the time of collecting information and "limiting use and disclosure" of personal information to the purpose for which it was first collected. The OPC has recognized this challenge and recommends continued discussion on exploring alternative grounds for processing.

7. **Include alternative grounds for processing where obtaining meaningful consent is not practicable.** The OPC recommends that meaningful consent should be required in the first instance for transparency. However, where obtaining meaningful consent is not possible, alternative grounds for processing should be available, such as: (i) when processing is necessary in the public interest; or (ii) when processing is necessary for the "legitimate interests" of the controller or a third party.
8. **Allow flexibility in using de-identified information.** The OPC proposes that *PIPEDA* continue to apply for anonymized or de-identified data, but that there be flexibility to use de-identified information under a new privacy act. The OPC further proposes that the law include penalties for negligent or malicious actions that result in re-identification of personal information from de-identified datasets.
9. **Require organizations to ensure algorithmic traceability.** The OPC recommends the inclusion of an algorithmic traceability requirement for AI that will ensure the accuracy and integrity of information throughout the AI system lifecycle.
10. **Mandate demonstrable accountability.** Principle 4.1 of *PIPEDA* requires organizations to be accountable for personal information under their control. OPC proposes that this principle be reframed to require "demonstrable" accountability, which would require organizations to provide evidence of adherence with legal requirements on request. The OPC also recommends the law require independent third-party auditing throughout the lifecycle of AI systems.
11. **Empower the OPC to issue binding orders and financial penalties.** To incentivize compliance with the law, *PIPEDA* must provide for meaningful enforcement with real consequences for organizations found to be non-compliant. Organizations in breach of the GDPR, for example, can be fined up to the higher of 4% of their annual global turnover or €20 million. The OPC proposes that the OPC be empowered to make binding orders and impose financial penalties for non-compliance with the law.

With advanced AI technology systems taking off, the need for robust data protection laws is greater than ever. The definition of "privacy" should not continue to be a moving target and our legal systems should reflect the complexity of machinic technologies. Although the OPC paper is still in the public consultation stage, the proposals are a step towards a privacy-centered approach to AI.

Published in the Electronic Healthcare Law Review, Volume 9, Number 4, May 2020.

For more information or inquiries:

James G. Kosa

Toronto
416.947.5043

Email:
jkosa@weirfoulds.com

James Kosa is a partner at WeirFoulds with a practice focused on information technology and intellectual property law.

Lisa Danay Wallace

Toronto
416.947.5041

Email:
ldanay-wallace@weirfoulds.com

Lisa Danay Wallace is a partner in the information technology and intellectual property law practice group at WeirFoulds LLP. She acts for clients when procuring and selling software and technology related services.

WeirFoulds LLP

www.weirfoulds.com

Toronto Office
4100 – 66 Wellington Street West
PO Box 35, TD Bank Tower
Toronto, ON M5K 1B7

Tel: 416.365.1110
Fax: 416.365.1876

Oakville Office
1320 Cornwall Rd., Suite 201
Oakville, ON L6J 7W5

Tel: 416.365.1110
Fax: 905.829.2035