



VIA EMAIL

May 28, 2021

Secretariat
Office of the United Nations High Commissioner for Human Rights
Palais Wilson
52 rue des Pâquis
CH-1201 Geneva, Switzerland
privacy-report@ohchr.org, registry@ohchr.org

Dear Colleagues:

Subject: Input for Report on right to privacy in the digital age

I am pleased to have the opportunity to share my office's work on artificial intelligence (AI) in response to the Office of the United Nations High Commissioner for Human Rights' (OHCHR) call for input on the forthcoming report, "right to privacy in the digital age".

AI marks a transformative point in society, introducing novel ways in which personal information is processed. Uses of AI that are based on individuals' personal information can have serious consequences for their privacy.

AI models have the capability to analyze, infer and predict aspects of individuals' behaviour, interests and even their emotions in striking ways. AI systems can use such insights to make automated decisions about individuals, including whether they get a job offer, qualify for a loan, pay a higher insurance premium, or are suspected of suspicious or unlawful behaviour. Such decisions have a real impact on individuals' lives, and raise concerns about how they are reached, as well as issues of transparency, fairness, accuracy, bias, and discrimination. AI systems can also be used to influence, micro-target, and "nudge" individuals' behaviour without their knowledge. Such practices can lead to troubling effects for society as a whole, particularly when used to influence democratic processes.

The Office of the Privacy Commissioner of Canada (OPC) has been engaged in privacy and related human rights issues regarding AI in recent years. In 2018, we co-sponsored the Declaration on Ethics and Data Protection in AI with our international counterparts through the Global Privacy Assembly (GPA).¹ We have since been a member of the GPA working group on

.../2

¹ Global Privacy Assembly, "Declaration on Ethics and Data Protection in AI", 2018
http://globalprivacyassembly.org/wp-content/uploads/2018/10/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf

Ethics and Data Protection in AI, and have co-sponsored the Resolution on Accountability in the Development and Use of AI.² These documents emphasize key principles for the development of AI, such as fairness, accountability, and transparency, and put forth a number of specific measures to achieve them.

In November 2020, my office published recommendations for the reform of Canada's private-sector privacy law to address the unique risks posed by AI.³ This represented the culmination of a multi-stakeholder public consultation in which 86 submissions were received from a range of organizations and experts across Canada. We also commissioned a separate report that informed the recommendations for law reform and accounted for stakeholder feedback.⁴

In our view, an appropriate law for AI would:

- Allow personal information to be used for new purposes towards responsible AI innovation and for societal benefits;
- Authorize these uses within a rights-based framework that would entrench privacy as a human right and a necessary element for the exercise of other fundamental rights;
- Create provisions specific to automated decision-making to ensure transparency, accuracy and fairness; and
- Require businesses to demonstrate accountability to the regulator upon request, ultimately through proactive inspections and other enforcement measures through which the regulator would ensure compliance with the law.

Using Data for Socially Beneficial and Legitimate Commercial Purposes

We acknowledge that consent, which forms the basis of Canada's private-sector privacy law and many other data protection laws globally, is not without its challenges. For individuals, long, legalistic and often incomprehensible policies and terms of use agreements make it nearly impossible to exert any real control over personal information or to make meaningful decisions about consent. For organizations, consent does not always work in the increasingly complex digital environment, such as where consumers do not have a relationship with the organization using their data, and where uses of personal information are not known at the time of collection, or are too complex to explain.

.../3

² Global Privacy Assembly, "Resolution on Accountability in the Development and Use of AI", 2020 <https://globalprivacyassembly.org/wp-content/uploads/2020/11/GPA-Resolution-on-Accountability-in-the-Development-and-Use-of-AI-EN.pdf>

³ Office of the Privacy Commissioner of Canada, "A Regulatory Framework for AI: Recommendations for PIPEDA Reform", 2020. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/req-fw_202011/

⁴ Ignacio Cofone, "Policy Proposals for PIPEDA Reform to Address Artificial Intelligence", 2020. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/

This is why we recommend exceptions to consent for (i) research and statistical purposes to facilitate the training of AI, which relies on statistical functions, (ii) the use of personal information for purposes compatible with the original purpose of collection, and (iii) legitimate commercial interests, which would provide flexibility to authorize unforeseen reasonable purposes but be based on particular and knowable purposes. To ensure the appropriate use of such exceptions, they must be accompanied by safeguards, including: a requirement to complete a [privacy impact assessment \(PIA\)](#), and a balancing test to ensure the protection of fundamental rights. The use of de-identified information would be required in all cases for the research and statistical purposes exception, and to the extent possible for the legitimate commercial interests exception.

Recognizing Privacy as a Human Right

While the law should allow for more flexible uses of personal information, it should only do so within a rights-based regime that recognizes privacy in its proper breadth and scope. Privacy is a fundamental right, and is necessary for the exercise of other human rights. This is particularly relevant in the context of AI, where risks to fundamental rights, such as the right to be free from discrimination, are heightened. Privacy law should prohibit using personal information in ways that are incompatible with our rights and values.

Despite the right to privacy being internationally recognized in both the Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights, many domestic privacy laws, including Canada's, are drafted largely as data protection statutes rather than as laws that protect and promote the exercise of a broad range of rights. Privacy is not limited to consent, access and transparency. These are important mechanisms, but they do not define the right itself nor acknowledge its quasi-constitutional status. Our laws must be reframed to recognize that privacy is nothing less than a prerequisite for freedom: the freedom to live and develop independently as individuals, away from the watchful eye of surveillance by the state or commercial enterprises, while participating fully in the regular, day-to-day activities of a modern society. This sentiment is echoed by the international data protection and privacy commissioner community as reflected in its International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights, adopted in October 2019.⁵ Currently, my Office is chairing an international working group of the GPA that has brought together representatives of twenty-two Data Protection Authorities from all regions of the world to develop a narrative or treatise on privacy as a human right and its relationship to other rights and freedoms. This work is in progress. We expect to present it at the forthcoming GPA conference in Mexico City this Autumn.

.../4

⁵ Global Privacy Assembly (formerly the International Conference of Data Protection and Privacy Commissioners), "International Resolution on Privacy as a Fundamental Human Right and Precondition for Exercising other Fundamental Rights", 2018
<http://globalprivacyassembly.org/wp-content/uploads/2019/10/Resolution-on-privacy-as-a-fundamental-human-right-2019-FINAL-EN.pdf>

The OPC considers profiling or categorization that leads to unfair, unethical or discriminatory treatment contrary to human rights law, as an inappropriate data practice for which organizations are prohibited from collecting, using and disclosing personal information.⁶ This stems from the overarching requirement in Canada's private-sector privacy law that *an organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances*. This is consistent with the spirit of the [International Resolution on Big Data](#) adopted by the GPA in 2014, where we committed to calling on all parties to demonstrate that decisions around the use of Big Data are fair, transparent and accountable; that results from profiling be responsible, fair and ethical; and that injustice for individuals due to fully automated false positive or false negative results be avoided.⁷

An important measure related to a human-rights approach would be to ensure the definition of personal information explicitly includes inferences drawn about individuals. Inferences refer to a conclusion that is formed about an individual based on evidence and reasoning. In the age of AI and big data, inferences can lead to a depth of revelations, such as those relating to political affinity, interests, financial class, race, etc. This is important because the misuse of such information can lead to harms to individuals and groups in the same way as collected information. In fact, as noted by the former European Article 29 Data Protection Working Party, “[m]ore often than not, it is not the information collected in itself that is sensitive, but rather the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern.”⁸

General support for the idea that inferences constitute personal information can be found in past OPC decisions and Canadian jurisprudence. However, despite this, there remains some debate as to how inferences are regarded. Some view them as an output derived from personal information, like a decision or an opinion might be, and argue these are outside the purview of privacy legislation. Given that inferences are typically drawn using an analytical process, such as through algorithms, others claim that these are products created by organizations using their own estimations, and that they do not belong to individuals. Such debate should be clarified by ensuring inferences are explicitly captured under privacy law.

Importantly, even where there is agreement that inferences are personal information, the fact that they could reveal commercial trade secrets is used by some as a basis to deny individuals

.../5

⁶ Office of the Privacy Commissioner of Canada, “Guidance on inappropriate data practices: Interpretation and application of subsection 5(3)”, 2018

https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/

⁷ Global Privacy Assembly, “International Resolution on Big Data”, 2014

<http://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-Big-Data.pdf>

⁸ See Article 29 Working Party, “Opinion 03/2013 on Purpose Limitation”, 2013

https://iapp.org/media/pdf/resource_center/wp203_purpose-limitation_04-2013.pdf

certain privacy rights, such as to access or correction. In scenarios where trade secrets may prevent explanations from being provided using the standard described above, organizations could use the following three factors, based on suggestions made by the UK Information Commissioner's Office (ICO), to provide an adequate explanation:⁹

- the type of information collected or used in creating the profile or making the automated decision;
- why the information is relevant; and
- what the likely impact is going to be.

Specific Provisions for Automated Decision-Making

Automated decision-making powered by AI systems introduces unique risks that warrant distinct treatment in the law. As Professor Cofone notes in his paper:¹⁰

“Under automated decision-making, discriminatory results can occur even when decision-makers are not motivated to discriminate.” Automated decision-making processes reflect and reinforce biases found in the data they are fed (trained with) into the decisions they yield. They reproduce and amplify the inevitably biased scenarios they were trained with. Protected categories that decision-makers are prohibited from considering, such as gender or race, are often statistically associated with seemingly inoffensive characteristics, such as height or postal code. Algorithmic decision-making can easily lead to indirect discrimination on the basis of gender or race by relying on these characteristics as proxies for the prohibited traits.”

The algorithms used to reach a decision concerning an individual can be a black box, leaving an individual in the dark as to how the decision was determined.

We recommend that individuals be provided with two explicit rights in relation to automated decision-making. Specifically, they should have a right to a meaningful explanation of, and a right to contest, automated decision-making.

The right to a meaningful explanation relates to existing privacy principles of accuracy, openness, and individual access. This right would allow individuals to understand decisions made about them and would facilitate the exercise of other rights such as to correct erroneous personal information, including inferences. The right would be similar to what is found in Article 15(1)(h) of the GDPR, which requires data controllers to provide individuals with “meaningful information about the logic involved” in decisions.

.../6

⁹ Information Commissioner's Office, “What else do we need to consider if Article 22 applies?” <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/>

¹⁰ Supra, note 4

Additionally, individuals should be provided with a right to contest automated decisions. Technology is not perfect, and individuals should not be bound by automated decisions without a way to seek human intervention, particularly when such decisions can be based on inaccurate data, reflect bias, or otherwise result in a decision that a human would deem inappropriate. This right would apply both to those scenarios where an individual has provided consent for the processing of their personal information as well as those where an exception to consent was used by the organization. The right to contest would be in addition to the ability to withdraw consent. It is necessary to have both rights, as withdrawal of consent is an all-or-nothing decision, whereas contestation provides individuals with recourse even when they choose to continue to participate in the activity for which automated decision-making was employed.

Demonstrable Accountability

Finally, privacy laws are hollow if they lack the necessary mechanisms to incentivize and enforce compliance. The role of the regulator in upholding the privacy rights of individuals in the marketplace is of utmost importance in light of the increasing complexity of information flows. Individuals should have a privacy regulator with effective enforcement powers to ensure they are able to enjoy the benefits of AI safely.

Integrating privacy and human rights into the design of AI algorithms and models is a powerful way to prevent negative downstream impacts on individuals. PIAs are useful tools when designing for privacy and human rights in AI. They help organizations meet legislative requirements and identify and mitigate negative impacts that programs and activities may have on individuals' privacy. They allow the privacy regulator to review the documented assessments, which can show the due diligence the organization took before implementing the AI activity.

To meaningfully implement proposed rights to explanation and contestation, organizations should be required to log and trace the collection and use of personal information in order to adequately fulfill these rights for the complex processing involved in AI. Traceability supports demonstrable accountability as it provides documentation that the regulator could consult through the course of an inspection or investigation, to determine the personal information fed into the AI system, as well as broader compliance.

Demonstrable accountability must include a model of assured accountability pursuant to which the regulator has the ability to proactively inspect an organization's privacy compliance. In today's world where business models are often opaque and information flows are increasingly complex, individuals are unlikely to file a complaint when they are unaware of a practice that might cause them harm. This challenge will only become more pronounced as information flows gain complexity with the continued development of AI.

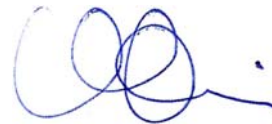
.../7

The significant risks posed to privacy and human rights by AI systems require a proportionally strong regulatory regime. To incentivize compliance, laws must provide for meaningful enforcement with real consequences for organizations found to be non-compliant. To guarantee compliance and protect human rights, laws should empower privacy regulators to issue binding orders and financial penalties.

Conclusion

I would like to thank the OHCHR for its continued work on privacy and human rights. This is important work that has the potential to set in motion action that will improve law and policy around the world, which is particularly relevant in an age where personal information increasingly flows across borders. We look forward to the OHCHR's report.

Sincerely,



Daniel Therrien
Commissioner