ASSOCIATION CANADIENNE DU DROIT DE LA TECHNOLOGIE
CAN TECH
CANADIAN TECHNOLOGY LAW ASSOCIATION

March 13, 2020

Office of the Privacy Commissioner of Canada
30, Victoria Street
Gatineau, Quebec
K1A 1H3

Dear Commissioner Therrien:

Re: Can-Tech Submission to the Office of the Privacy Commissioner ("OPC") Regarding Consultation on the OPC's Proposals for Ensuring Appropriate Regulation of Artificial Intelligence ("Consultation")

Introduction

The Canadian Technology Law Association ("**Can-Tech**") Artificial Intelligence Working Group ("**Can-Tech WG**") welcomes the opportunity to write to the OPC regarding the recent Consultation. Can-Tech was founded more than twenty years ago to bring together Canadian practitioners of computer and technology law. Our association includes leading technology, outsourcing and privacy lawyers in Canada working in both private practice and in-house. The Can-Tech WG has put together the following submission in order to voice its opinion on how the OPC should approach discussions regarding the regulation of artificial intelligence ("**AI**") in the coming year in its consultations with the Innovation, Science and Economic Development Canada ("**ISED**"), provincial Information and Privacy Commissioners and other government and regulatory bodies.

The views and opinions expressed in this submission are the personal views of the Can-Tech WG and its supporting signatories and are not intended to bind nor do they necessarily reflect the official policy or position of Can-Tech's entire membership or any individual or organization that they are affiliated with.

Overarching Themes

We have chosen to provide our views on each of the OPC's proposals outlined in the Consultation. In addition to such views, however, we would like to highlight the following themes which arose within our discussions:

- ***Current Success of the* Personal Information Protection and Electronic Documents Act *("PIPEDA")***

  PIPEDA was enacted two decades ago and has been a resilient piece of legislation in large part because: (1) it is technology-neutral—while PIPEDA predates smart phones, cloud computing and AI, it was drafted purposively in recognition of the increasing use of technology in the circulation

and exchange of information;[1] (2) it is principles-based, rather than being overly prescriptive; and (3) it is intended to protect data subjects' rights while at the same time encouraging trust and responsible use of personal information by organizations. These qualities have afforded data subjects protection, while at the same time reassuring organizations that PIPEDA is future-proof and flexible enough to apply to different processes of varying size and context, and new and emerging technologies.

When weighing recommendations for amendments to PIPEDA, we urge the OPC to retain these critical facets of PIPEDA, particularly in light of the fact that technology changes at a pace that legislation cannot possibly keep up with.

- ***The Importance of Streamlining Privacy Compliance Within the Canadian Market and Within the Global Privacy Landscape***

  Canada is currently an attractive market for the technology sector in part because PIPEDA and provincial privacy laws are substantially similar, meaning that an organization looking to operate in Canada has a relatively straight-forward time understanding the ins and outs of privacy compliance. Without this inter-operability, businesses would have to expend considerable (if not prohibitive) resources to ensure their products and services are compliant with different laws depending on the location of their operations.

  We are concerned that the Consultation does not explain how submissions will be used by the OPC, or how the OPC would work with provincial Information and Privacy Commissioners in order to arrive at a consensus regarding the regulation of AI within Canadian privacy law, if at all. It is imperative that any amendments to PIPEDA be inter-operable with provincial privacy laws in order to provide predictability to organizations and avoid a chilling effect with respect to investment in Canada's technology economy.

  We also urge the OPC to ensure that ISED continues to be the stakeholder leading the effort to update privacy legislation. While we understand the OPC's interest in such amendments, we ask that it be careful not to usurp the government's role in setting overarching policies that are of critical importance to all Canadians.

<u>Can-Tech's Responses to Individual Proposals</u>

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

In large part, Can-Tech WG does not support the addition of a definition of AI within PIPEDA at this time. The technology-neutral character of PIPEDA has permitted it to be broadly applied to emergent technologies. For example, "cloud computing" is not defined in PIPEDA. The OPC published guidance in the early 2010s on cloud computing and privacy to guide industry, which included (among other things) reference to the definition for cloud computing developed by the U.S. National Institute of Standards and Technology[2]; and the regulation of cloud computing by the OPC under this framework is now

[1] *Personal Information Protection and Electronic Documents* Act, SC 2000, c 5, s 3 [PIPEDA].
[2] Office of the Privacy Commissioner of Canada, "Cloud Computing and Privacy" (October 2011), online: *OPC* <https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/online-privacy/cloud-computing/02_05_d_51_cc/>.

commonplace. Similarly, leaving AI undefined in PIPEDA at least, in the short-term and instead issuing guidance on AI-related concerns of the OPC would allow for maximum flexibility in its interpretation and application as AI technology evolves.[3] This is particularly important in light of the fact that the OPC itself acknowledges in the Consultation that there are seemingly endless and even conflicting views on how to define AI.

Incorporating a definition of AI is further complicated by the fact that the AI field is in its nascence. In particular, the development of deep learning algorithms and "strong AI" may fundamentally change the way in which humans understand and deploy AI. The wrong definition of AI within privacy legislation may significantly harm industries. For example, a too broad definition of AI may unintentionally apply to technologies that are not truly "intelligent" or impactful on the use of PI such as an anti-virus application that makes autonomous decisions. Conversely, a definition that is too narrow may inadvertently exclude next-generation technologies.

Notwithstanding the above, we recognize as a practical matter that a clear definition for what exactly is being regulated under Canadian privacy law may lead to greater certainty for organizations and possible reductions in the costs of compliance. We believe that this certainty can be achieved in PIPEDA without the use of a stringent definition. One way to do this is by clearly outlining the types of activities that are regulated. The European Union's General Data Protection Regulation 2016/679 ("**GDPR**"), for example, regulates a subset of automated decisions rather than AI itself.[4]

Can-Tech WG requests that the OPC, along with ISED and other stakeholders, first decide the harmful activities Canada should prevent or mitigate rather than the type of technology it should regulate. These discussions may yield the conclusion that no definition is necessary. We urge the OPC to keep in mind that like all technology, AI is not inherently dangerous, and it should not be presumed that AI has intrinsic characteristics (whether moral, immoral or amoral) that are independent of the manner in which it is deployed by humans.

Any definition of AI (if one is introduced) must be carefully considered, and efforts should be made to align any definition of AI in PIPEDA with international privacy laws (such as GDPR) to ensure maximum inter-operability. Regard should also be given to the role that other areas of law (such as tort) might play in the direct or indirect regulation of AI and how this might be addressed by Parliament.[5]

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

Can-Tech acknowledges that AI, if used negligently or maliciously, has the ability to affect Canadian citizens' right to privacy or other fundamental human rights. We do not agree, however, that

[3] Indeed, some scholars question whether AI can even be defined at this stage. See e.g. Ryan Calo, "Artificial Intelligence Policy: A Primer and Roadmap" (2017) 51:2 UC Davis L Rev 399. See also Aviv Gaon & Ian Stedman, "A Call to Action: Moving Forward with the Governance of Artificial Intelligence in Canada (2019) 56:4 Alta L Rev 1137 (ALR).

[4] EC, *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC* (General Data Protection Regulation), [2016] OJ, L 119/1, Art 22 [GDPR].

[5] Matthew U. Scherer, "Regulating Artificial Intelligence Systems: Risks, Challenges, Competencies, and Strategies" (2016) 29:2 Harv JL & Tech 354 at 393 (SSRN).

the emergence of AI signals that an overhaul in PIPEDA is required or that it is necessary or desirable to introduce a rights-based approach in its application.

PIPEDA operates using the lynchpin concept that any collection, use or disclosure of personal information must be reasonable; this in itself is a recognition that privacy is an inherent right to data subjects. As well, PIPEDA is just one of many laws within Canada that are meant to protect data subjects' rights. The lack of framing of PIPEDA as a rights-based law does not negate the fact that use of personal information by organizations using technology such as AI must not, for example, breach human rights laws such as the Ontario *Human Rights Code* or the *Occupational Health and Safety Act*.

Canada also has the benefit of learning from the European experience under GDPR, including a reported increase in compliance costs[6] and private privacy litigation subsequent to its adoption.[7] Any proposal to incorporate a rights-based approach to the law must have regard to PIPEDA's purposive requirement that individual privacy rights be balanced against the legitimate needs of businesses to collect, use and disclose individuals' personal information.[8]

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

The Consultation supports that a circumscribed right, similar to the one found in Article 22 of the GDPR, be incorporated into PIPEDA. The OPC views the right to object and to be free from automated decisions as being analogous to Principle 4.3.8 of PIPEDA (the right of an individual to withdraw their consent). Can-Tech WG has the following key concerns with this proposal:

(i) The approach does not necessarily take into account the fact that it would penalize automated decision-making by making it more expensive for organizations to employ. For example, the right to object would require organizations to build redundant processes that do not use AI in order to comply with this requirement for a small subset of individuals who may avail themselves of such a right. As well, most human decision-making processes do not always have an appeal process, and to require one for automated decisions would place an unfair burden on organizations.

(ii) The OPC assumes that human decision-making does not suffer from the same flaws often alleged for automated decisions—namely various types of biases. In fact, it is well documented that human decision-making may actually be more susceptible to biases given cultural or socio-economic influences than automated decisions, which essentially rely on historical data and the ability for coders to identify and potentially remove any biases that are identified.

(iii) The OPC assumes that all automated decision-making is of the same caliber and has the same effect on data subjects when this is not the case—while the effects of some AI on data subjects can be significant (for example, when used to deny right to housing), some AI can be used for entirely innocuous reasons (for example, when used to recommend television shows to an

[6] The accounting firm Ernst & Young estimated that multinational corporations spent $7.8 billion to comply with GDPR: see Jeremy Kahn et al, "It'll Cost Billions for Companies to Comply with Europe's New Data Law" (21 March 2018), online: *Bloomberg Businessweek* <https://www.bloomberg.com/news/articles/2018-03-22/it-ll-cost-billions-for-companies-to-comply-with-europe-s-new-data-law>.

[7] See e.g. Todd Ehret, "Data privacy and GDPR at one year, a US perspective" (22 May 2019), online: *Reuters* <https://www.reuters.com/article/bc-finreg-gdpr-one-year-report-card-part/data-privacy-and-gdpr-at-one-year-a-u-s-perspective-part-one-report-card-idUSKCN1SS2K5>.

[8] PIPEDA, *supra* note 1, s 3 (Purpose).

individual). The law should focus more on the activity it is trying to mitigate (negligent or malicious use of personal information), rather than the perceived method of harm.

Can-Tech WG is supportive of a right to appeal a decision made solely by using AI so long as it meets a minimum threshold. In this regard, Can-Tech supports the development of a private sector impact-level framework similar to that of the Government of Canada's Directive on Automated Decision Making (the "**Directive**"), which measures the impact of AI using various factors such as permanency of the decision and deprivation of certain benefits to the data subject. However, we urge the OPC to be mindful that the Directive was drafted with government agencies in mind, and such entities by default affect the rights of Canadians; this is not the case with the private sector. Any framework for measuring impact threshold by the OPC should take into account the spectrum mentioned by us in item (iii) above and the limited resources available to small businesses, which account for a substantial portion of the Canadian economy.

As well, the OPC should take into consideration the extent to which a decision was automated, on a spectrum of full to no automation, and whether a mandated right of appeal would apply to the entire decision or simply the automated aspects.[9] Can-Tech WG would not support a right of appeal where meaningful human intervention is already part of the process applicable to the data subject.

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

(i) The Right to Explanation

The Consultation proposes the right to explanation for individuals when they are subject to automated processing operations. This right would allow individuals to receive an explanation of the underlying reasoning for the algorithmic decision made about them and the consequences of this reasoning on their rights and interests.

Currently, there is no established definition of what constitutes an "explanation". Scholars[10] have distinguished two types of explanations:

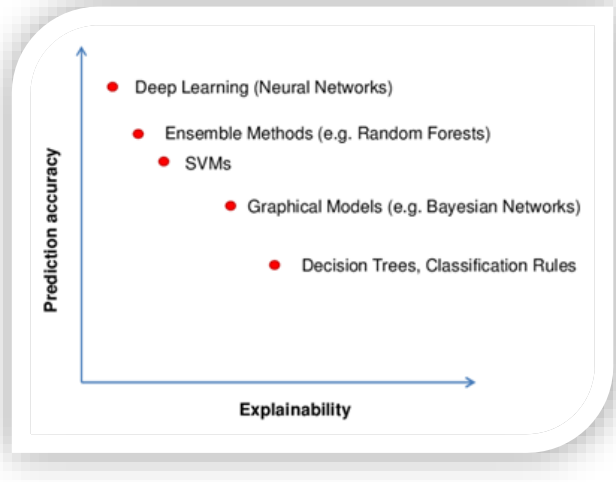
a) Model-Centric Explanations ("MCEs"): provide broad information about the logic, predicted consequences and general functionality of an automated decision-making system. MCEs do not explain specific input-data and decisions.
b) Subject-Centric Explanations ("SCEs"): provide the reasoning of specific input-data and decisions.

[9] Consider an example in the criminal context, *State v Loomis*, 881 NW 2d 749 (Wis 2016), where the Wisconsin Supreme Court ruled that use of the COMPAS sentencing algorithm was allowable as long as it was only one factor in the sentencing judge's ultimate decision (for further commentary, see "State v. Loomis: Wisconsin Supreme Court Requires Warning Before Use of Algorithmic Risk Assessment in Sentencing" (2017) 130 Harv L Rev 1530). The OPC should consider: would the right of appeal be specifically targeted towards the automated aspects of the decision or would it be a right to appeal the decision as a whole, regardless of the degree to which automation is involved?

[10] See e.g. Sandra Watcher et al, "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation" (2017) Int'l Data Privacy L (SSRN); Lilian Edwards & Michael Veale, "Slave to the Algorithm? Why a 'Right to an Explanation' is Probably Not the Remedy You are Looking For" (2017) 16 Duke L & Tech Rev 18 (SSRN).

It is unclear to us that explainability is necessary or even desirable in certain cases. For example, a consumer with little technical background is unlikely to gain significant privacy protection or value from a company providing detailed information about the logic underlying its AI.

There are also concerns about the practical feasibility of this right given the complexity of deep learning neural networks. As shown in the chart below, explainability becomes more difficult (or nearly impossible) as the prediction accuracy of AI increases. PIPEDA should not be amended without addressing this practical reality and acknowledging the fact that a right to explainability may be (1) impossible to comply with and (2) may hinder use of deep learning, which has enormous potential for societal good.



Prediction Accuracy Versus Explainability[11]

Can-Tech WG is supportive of the right to explanation that is based on an impact-level framework similar to that of the Directive wherein a higher level of impact on an individual requires a higher level of explanation. Organizations could adopt MCEs for automated decisions with a lower level of impact. This could take the form of providing an explanation through a "Frequently Asked Questions" section on the organization's website that explains the basic information on how the system works. For automated decisions with a higher level of impact, organizations could rely on SCEs. SCEs would provide a more detailed explanation of the decision-making process of the system in particular and how it reached the specific decision in question. The potentially intrusive nature of SCEs poses a risk of exposing organizations' proprietary information. It is important that parameters are put in place to protect such information.

Research has also been growing the area of explanatory AI to tackle the issue of complex machine and algorithms' failure to provide adequate insight into their thought and behaviour processes. We urge the OPC to encourage investment and research into technical methods that could increase explainability of AI and make it feasible for companies to employ.[12]

[11] Albert C, "We are ready for Machine Learning Explainability?" (8 April 2019), online: *Towards Data Science*: <https://towardsdatascience.com/we-are-ready-to-ml-explainability-2e7960cb950d>.

[12] For example, the U.S. Defense Advanced Research Projects Agency (DARPA) devoted $75 million in 2017

(ii) The Right to Transparency

Proponents of algorithmic transparency argue that increasing transparency in source code, inputs and outputs of machine learning systems will naturally reveal malicious intentions of an AI operator and in turn allow regulators to better police harmful effects of AI. While transparency may be helpful in straight-forward cases where an algorithm is static save and except for a few variables,[13] these arguments often fail to take into account the great technical difficulty of gleaning meaningful information from the review of more complex AI systems and their underlying data.[14] While a degree of transparency may be appropriate in certain contexts, business and regulators lack the technical skillset, time and resources to perform analysis on complex computer systems and it is unclear that doing so would yield significant privacy benefits to Canadians.

We do not support the publishing of privacy impact assessments or the public filing of algorithms for the private sector. Calls for the release of proprietary information brush off significant concerns regarding the protection of intellectual property and the potential for bad actors to use revealed information to take advantage of algorithm-driven products and systems.[15] Such measures would put Canada's technology and intellectual property systems at a disadvantage in the global marketplace.

Instead of a blanket requirement for transparency, we would suggest that the OPC collaborate with policymakers and computer scientists to develop different mechanisms that could be used in a flexible manner to allow organizations to demonstrate that their decision-making system complies with Canadian privacy law. If the system is simple enough, transparency may be an appropriate mechanism. However, it should not be a mandatory requirement of compliance when demonstrated adherence to standardized guidelines for designing decision-making systems, for example, may be sufficient.[16]

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

In principle, Can-Tech WG supports the introduction of Privacy by Design in phases of processing, particularly since doing so has the potential to decrease risks of breaches involving personal information. Additionally, one of the framework's main principles is the accommodation organizations' legitimate

---

to research explainable AI: see Cliff Kuang, "Can AI Be Taught to Explain Itself?" (21 November 2017), online: *The New York Times* <https://www.nytimes.com/2017/11/21/magazine/can-ai-be-taught-to-explain-itself.html>.

[13] See e.g. Caleb Watney, "When it Comes to Criminal Justice AI, We Need Transparency and Accountability" (1 December 2017), online: *R Street Institute*< https://www.rstreet.org/2017/12/01/when-it-comes-to-criminal-justice-ai-we-need-transparency-and-accountability/>.

[14] See e.g. Joshua New & Daniel Castro, "How Policymakers Can Foster Algorithmic Accountability" (2018) Center for Data Innovation Working Paper, online: < http://www2.datainnovation.org/2018-algorithmic-accountability.pdf>. The paper highlights an example wherein expert programmers at the University of Michigan were unable to determine what the purpose of a piece of the website Reddit's algorithm was even with complete transparency. This implies that transparency does not go hand in hand with ease of analysis or detection of misbehaviour.

[15] Google, for example, is very secretive with respect to algorithms used to present results to queries particularly because previously more transparent versions allowed bad actors to game the system in order to increase their visibility in search results: see John Faber, "How to Future-Proof Your Search Ranking" (2 April 2018), online: *ChapterThree* <https://www.chapterthree.com/blog/how-to-future-proof-your-search-ranking>.

[16] We recommend the OPC review the research paper "Accountable Algorithms" by Joshua A Kroll et al (2017) 165 U Penn L Rev (SSRN), which proposes technological tools that can be used in decision-making processes in both the public and private sector which do not rely on total transparency.

interests to use personal information in a positive-sum, "win-win" manner. We would like to point out, however, that most of the principles of the Privacy by Design framework are already incorporated in PIPEDA's 10 fair information principles.[17] In fact, the only Privacy by Design principles that are not currently represented within PIPEDA are:

- Principle 1: Proactive not Reactive / Preventative, not Remedial;
- Principle 3: Privacy Embedded into Design; and
- Principle 4: Full Functionality, Positive-Sum, not Zero-Sum.

We would recommend that the OPC focus on how to encourage organizations to implement Principles 1, 3 and 4 into their business practices and use of AI tools, as requiring demonstration of adherence to Privacy by Design as a whole may be unnecessary or may result in redundant compliance mechanisms and expenditures by organizations. As well, if the OPC incorporates a Privacy by Design requirement, we would urge that this be done in a contextual manner similar to that of the GDPR Article 25,[18] which specifies that compliance take into account the following factors:

- the state of the art;
- the cost of implementation;
- the nature, scope, context and purposes of processing; and
- the risks of varying likelihood and severity for rights and freedoms of individuals.

In the Consultation, the OPC suggests that testing of AI for privacy and human rights impact should be required before a product goes to market. We believe this requirement would overstep the OPC's mandate. The OPC should be focused on mitigating activities that lead to harmful use of personal information using automated decision-making systems, not whether companies are able to bring products to market, as the latter can and is enforced by other regulatory bodies. As well, there is currently no international consensus on what standard or method can be used to measure impact to human rights. We do not support the OPC adopting its own standard, as this may be internationally inoperable and burdensome on organizations wishing to do business in Canada.

Lastly, if the OPC does adopt requirements such as a certification mechanism, adherence should be reviewed by an organization with the appropriate skillset and a balanced viewpoint. For example, the Canadian Bar Association ("**CBA**") in its response to the Strengthening Privacy for the Digital Age consultation document released by ISED,[19] recommends that the Standards Council of Canada, rather than the OPC, be given the authority for any certification scheme. We support this recommendation.

---

[17] Please see this mapping of Fair Information Principles to Privacy by Design Principles by Dr. Ann Cavoukian during her time as the Information and Privacy Commissioner: Ann Cavoukian, "Privacy by Design: The 7 Foundational Principles" (January 2011) online: *IPCO* <https://www.ipc.on.ca/wp-content/uploads/resources/pbd-implement-7found-principles.pdf>.

[18] GDPR, *supra* note 4, Art 25.

[19] Canadian Bar Association Privacy and Access Law Section "Strengthening Privacy for the Digital Age: Response to Proposals to Modernize PIPEDA" (December 2019), online: *CBA* <http://cba.org/CMSPages/GetFile.aspx?guid=ef901bd8-d329-4d36-87e5-2298290a2b84>.

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

Can-Tech WG feels that it is very important not to allow data minimization and purpose specifications to limit access to wholly or partially de-identified or anonymized personal information for vital secondary purposes that are strongly in the public interest such as health-related research. In such situations it is not possible to state every single purpose for which personal information may be used. When assessing this proposal we urge the OPC to review long-standing policies adopted by other regulatory bodies dealing with sensitive personal information such as health information.

For example, the Information and Privacy Commissioner of Ontario[20] ("**IPCO**") has recognized the importance of making de-identified health information available for use for secondary purposes and how data minimization within health research applied in the same manner across the board can lead to degradation of a dataset's quality, greatly decreasing its usefulness. In order to allow meaningful secondary use of the data, IPCO recommends that data custodians perform an evaluation of the risk of re-identification on a proposed dataset based on factors such as:

- the re-identification probability;
- the mitigating controls that are in place;
- the motives and capacity of the data recipient to re-identify the data; and
- the extent to which an inappropriate disclosure would be an invasion of privacy.

Based on this assessment, IPCO outlines how organizations can put in place varying mitigating controls, such as a robust data sharing agreement. Can-Tech recommends that the OPC adopt such guidance in order to encourage the use of personal data using automated decision-making systems for secondary purposes in a responsible manner. The OPC should also consider guidelines on "go" and "no go" zones within such activities similar to the ones found in its Guidance on Inappropriate Data Practices.[21]

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

The desirability of enabling alternative grounds for processing that align with GDPR is well recognized. Any new grounds for processing in PIPEDA should be framed broadly, such as the GDPR's legitimate interests,[22] and not limited to certain services or situations.

Article 6(1) of GDPR provides several lawful bases for processing, including but not limited to consent. By contrast, the OPC has proposed that meaningful consent should be required in the first instance for transparency and to preserve human agency, and that alternative grounds for processing should only be used under prescribed conditions such as after conducting a privacy impact assessment demonstrating that obtaining consent was impracticable. Such burdens are not imposed by the GDPR and should not be imposed on Canadian businesses. With respect to emergent technologies like AI, regard

---

[20] Information and Privacy Commissioner of Ontario and the CHEO Research Institute and University of Ottawa "Dispelling the Myths Surrounding De-Identification: Anonymization Remains a Strong Tool for Protecting Privacy" (June 2011), online: *IPCO* <https://www.ipc.on.ca/wp-content/uploads/2016/11/anonymization.pdf>.

[21] Office of the Privacy Commissioner of Canada: "Guidance on Inappropriate Data Practices: Interpretation and Application of Subsection 5(3)" (May 2018), online: *OPC* https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805>.

[22] GDPR, *supra* note 4, Art 6(1)(f).

must be had to the fact that most successful technology companies begin as small businesses that do not have compliance counsel. We feel that such stringent requirements for the use of alternative bases would be a drain on resources, make Canada an unfavourable jurisdiction in which to do business, and make alternative grounds so inaccessible as to render their existence ultimately useless.

While consent will always be necessary in certain circumstances regardless of the technology at play, recent research assessing the post-GDPR landscape has exposed weaknesses in consent mechanisms.[23] At least in some cases, these weaknesses result largely from problematic (and oftentimes paradoxical) human behaviour such as users who have a default expectation of privacy, but are willing to accept tracking over mechanisms that require them to take positive steps.[24] While the OPC asserts that meaningful consent theoretically increases transparency and preserves human agency, it is instructive that many individuals do not have the time, interest or resources to meaningfully exercise the agency afforded to them by the GDPR.

Even where users do wish to exercise agency, the lack of consumer understanding of the "downstream" effects of consent (such as how one's consent to any particular service impacts others) often prevents users from giving meaningful and informed consent.[25] This is particularly the case with AI, even the "weak" AI that exists today.

As the collection and processing of data becomes increasingly ubiquitous, Can-Tech WG believes it is time to consider alternative methods for protecting privacy rights such as appropriate constraints on dataflow that triage the situations requiring consent. This type of model, which forces an organization to assess the impact of its services on consumers, has the potential to better distribute costs and benefits fairly so that data subjects are not required to unnecessarily navigate and digest extensive privacy policies. Rather than rewarding businesses merely for seeking consent, businesses should be rewarded for duly considering the impact of their services and placing only an appropriate burden on consumers.

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

Can-Tech WG strongly believes that there should be flexibility in the manner in which PIPEDA is applied to personal information that is rendered non-identifiable in an acceptable manner. We believe that to do otherwise, that is to apply the same requirements to personal information and properly de-identified information, would mean there is less incentive to de-identify, as the same restrictions and requirements would apply regardless of the level of de-identification. This would in turn have a chilling effect on the use of de-identification, which is a powerful tool for privacy protection.

[23] See e.g. Helen Nissenbaum, "A Contextual Approach to Privacy Online" (2011) 140:4 Daedalus 32-48 (SSRN).
[24] See e.g. Christine Utz et al, "(Un)informed Consent: Studying GDPR Consent Notices in the Field" (Paper delivered at the 2019 ACM SIGSAC Conference on Computer and Communications Security (CCS '19), November 11–15, 2019, London, United Kingdom) (DOI).
[25] See e.g. Daniel J Solove, "Privacy Self-Management and the Consent Dilemma" (2013) 126 Harv L Rev 1880 (SSRN).

Can-Tech WG supports the proposal by the Canadian Anonymization Network ("**CANON**") in its comments to ISED regarding PIPEDA modernization,[26] where it argued for the adoption of a risk-based framework for de-identification based on a "spectrum of identifiability":

> "[I]nformation that poses no serious risk of re-identification could remain outside of PIPEDA, while information with a low risk of re-identification could be covered by PIPEDA, potentially exempted from consent (see below), but subject to other fair information principles as appropriate, including accountability, safeguarding and transparency. Such risk gradations would be determined in accordance with developed guidelines or standards and could be achieved using a variety of different technical methods and appropriate governance models."

We support the relaxation of principles such as the right to access, consent and breach notification once personal information is properly de-identified in order to incentivize use of de-identification techniques and reduce undue burdens on organizations. IPCO has done a thorough job[27] of laying out the reasons as to why the aforementioned rights should be relaxed when proper de-identification protocols are enforced, and we suggest that the OPC consider adopting these same proposals.

Proposal 9: Requiring that organizations ensure data and algorithmic traceability, particularly with regard to datasets, processes, and decisions made during the AI system lifecycle

The Consultation proposes that PIPEDA should have a requirement for data and algorithmic traceability to meet goals of accountability, accuracy, transparency, data minimization, as well as access and correction. While data and algorithmic traceability is an important matter, it is ultimately one that may be unnecessary in order to protect someone's privacy or other rights. It may also pose an undue burden on a business that outweighs an individual's right to privacy in that particular context, for example, where the impact of the AI use on the individual is minimal, but the cost of employing traceability for an organization is prohibitive.

We believe data and algorithmic traceability may be helpful in a scenario where use of the AI with respect to personal information meets a particular threshold. We would support use of an impact-level framework similar to that of the Directive, while taking into account the special considerations that should be applied to the private sector under our response to Proposal 3 above. In situations where someone is denied the right to travel, for example, having the ability to trace may be helpful to appeal that particular decision.

We would urge the OPC to consider this requirement holistically in light of the other proposals and existing PIPEDA requirements. For example, if Privacy by Design is a requirement, sufficient protections may be in place so as to not require use of traceability.

---

[26] Letter from the Canadian Anonymization Network (15 October 2019) Submission re: ISED's ""Strengthening Privacy for the Digital Age" online: <https://deidentify.ca/wp-content/uploads/2019/10/CANON-Submission-ISED-Strengthening-Privacy-for-the-Digital-Age.pdf>.

[27] See Cavoukian, *supra* note 17.

Proposal 10 – Mandate Demonstrable Accountability for the Development and Implementation of AI Processing

Can-Tech WG is very concerned that the OPC lacks the highly specialized expertise and resources to effectively regulate some of the suggestions in its proposal, such as undertaking new types of proactive inspections.

We are supportive of the OPC offering incentives for organizations adopting demonstrable accountability measures, such as giving consideration to these measures as mitigating factors during an investigation. Currently there are very few accredited standards for measuring accountability in AI processing. In the absence of such standards there is a dearth of professionally regulated auditors that can perform such audits. Rather than require audits by law, we instead suggest that the OPC encourage the development and adoption of national and international standards for AI processing. The OPC could consult with the CIO Strategy Council, for example, which is accredited by the Standards Council of Canada and made up of public, private and non-profit stakeholders. The organization has already developed a standard for the Ethical Design and Use of Automated Decision Making Systems.[28]

We do not support mandating that each AI use in the privacy sphere require third party audit or verification throughout the lifecycle of the system. Other controls can be employed to foster accountability, such as:

- ensuring that the operators can verify that the automated decision-making systems act in accordance with their intentions;
- promoting desirable or beneficial outcomes and monitors; and
- identifying and rectifying harmful outcomes with respect to privacy.[29]

Notwithstanding the above, Can-Tech WG also encourages the OPC to consult international guidance documents, such as the EU Report from the Expert Group on Liability and New Technologies.[30]

Proposal 11: Empowering the OPC to issue binding orders and to impose financial penalties on organizations that do not comply with the law

Can-Tech WG believes that discussion on the OPC's increasing powers is better served as part of a larger discussion on PIPEDA modernization. AI should not be more substantially regulated or penalized than collection, use and disclosure of personal information using alternate mechanisms. If enacted, enforcement of certain technical areas of PIPEDA related to certification, for example, should not be within the OPC's purview.

Conclusion

Once again, the members of Can-Tech WG appreciate this opportunity to provide feedback on the OPC's proposals for the modernization of PIPEDA and we look forward to the opportunity to continue a

[28] CIO Strategy Council, *National Standard of Canada for Automated Decision Systems* (2 October 2019), online: <https://ciostrategycouncil.com/standards/implement-standards/>.

[29] Please see Watney, *supra* note 13 and Faber, *supra* note 15 for recommended resources and technical suggestions for regulators on how to implement balanced measures and foster algorithmic accountability.

[30] EC, Commission, *Report by the Expert Group on Liability and New Technologies on Liability for Artificial Intelligence and Other Emerging Digital Technologies* (2019), online: <https://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeetingDoc&docid=36608>.

discussion on the issues described above. Please feel free to contact Elena Iosef, Co-Chair of Can-Tech's Artificial Intelligence Working Group, for further information.

Contributors to this submission are:

Elena Iosef – Legal Counsel, Tata Consultancy Services Canada Inc.
Nancy Cleman – Partner, Lapointe Rosenstein Marchand Melançon LLP
Lisa R. Lifshitz – Partner, Torkin Manes LLP
Jesse-Ross Cohen – Associate, Goodmans LLP
Chiedza Museredza – Associate, McMillan LLP
Imran Ahmad – Partner, Blake, Cassels & Graydon LLP
Alec McIlwraith-Black – JD Student, University of Alberta Faculty of Law