Modernizing Privacy in Ontario

Comments of

Canadian Wireless Telecommunications Association

September 3, 2021

Introduction

The Canadian Wireless Telecommunications Association (CWTA) appreciates the opportunity to provide its feedback regarding the Ontario government's whitepaper, *Modernizing Privacy in Ontario*, issued on June 17 of this year.

CWTA is the authority on wireless issues, developments and trends in Canada. Its membership is comprised of companies that provide services and products across the wireless industry, including wireless carriers and manufacturers of wireless equipment. The protection of personal information is a key element of our members' business practices and corporate ethos. For that reason, our members invest significant effort and resources to protect the right to privacy of customers and the security of their personal information.

In its whitepaper, the government sets out its vision "to make Ontario the world's most advanced digital jurisdiction". To reach this objective, the government has rightfully identified the need to enhance the public's trust in the use of digital technologies, including the collection and use of personal information. But this is just one of the key elements of any privacy framework.

As the Office of the Information and Privacy Commissioner of Ontario (IPC) stated in its earlier submission to this process (IPC Submission)[1], "businesses and organizations need a regulatory regime for privacy protection that is principles-based, fair and well-balanced, pragmatic, flexible and proportionate." It must also provide flexibility to address privacy risks as they evolve through technological developments and new business models.

Any proposed private sector privacy regulation should have as its purpose what the IPC described as a virtue of the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA); the stated purpose of seeking a balance between protecting privacy and facilitating the legitimate and reasonable use of data and digital technologies.[2] Elevating privacy rights above all other fundamental rights, or legal or societal interests, as some EU countries have done in applying the EU's General Data Protection Regulation (GDPR), risks depriving Ontarians of the benefits of digital innovation and making Ontario a less desirable place for businesses to establish operations. This would make the government's goal of making Ontario "the world's most advanced digital jurisdiction"[3] all but impossible to achieve.

[1] Information and Privacy Commissioner of Ontario, Letter to Minister Thompson re: Ontario Private Sector Privacy Reform Discussion Paper, October 16, 2020 - https://www.ipc.on.ca/wp-content/uploads/2020/10/2020-10-16-ipc-private-sector-consultation-submission.pdf (IPC Submission)
[2] IPC Submission, p. 4
[3] Government of Ontario, *Modernizing Privacy in Ontario,* 2021, p. 1

It is also important that an Ontario private sector privacy framework avoid the creation of overlapping and inconsistent regulations that are not interoperable with those of other jurisdictions in Canada and internationally. This does not mean that Ontario private sector privacy regulations must be identical to privacy regulations across Canada or abroad, but any regulations should avoid introducing measures that create significant inconsistencies and unnecessary barriers to the conduct of business across borders, and that harm the competitiveness of businesses operating in Ontario.

It should also avoid creating confusion as to which law applies; as such confusion harms both businesses and individuals. For this reason, an Ontario privacy sector privacy law should include an exception to the application of such regulations for organizations, such as telecommunication service providers, whose collection, use and disclosure of personal information is already regulated by federal privacy and industry specific legislation.

While CWTA is of the view, as referenced in our first recommendation below, that any proposed Ontario private sector privacy law should not apply to organizations governed by federal legislation, we have also included comments relating to some of the topics raised in the government's white paper. We trust these recommendations will help the government in its deliberations.

Failure to address an item mentioned in the whitepaper should not be construed as agreement with the government proposal. In addition, to the extent that there is any inconsistency between CWTA's submission and that of a CWTA member in this proceeding, in regards to the position of such CWTA member, the member's submission shall prevail.

Comments and Recommendations

1. Ontario private sector privacy regulations should not apply to federal undertakings

Similar to section 3(2)(c) of British Columbia's *Personal Information Protection* Act, any Ontario private sector privacy regulations should expressly state that it does not apply to "the collection, use or disclosure of personal information, if the federal Act applies to the collection, use or disclosure of the personal information." The absence of such a provision would create overlapping privacy regulations for organizations, such as telecommunication service providers (TSPs), already governed by federal privacy laws. This overlap would not only increase the cost and burden of compliance, it will introduce confusion for Ontarians regarding their rights and where to go for resolution of a privacy matter.

Albeit in a different context, the IPC has clearly described the impact of overlapping federal and provincial privacy regulations:

> From the individual complainant's perspective, this regulatory morass tends to create unnecessary confusion as to which law applies and to which oversight body one should complain. For organizations, this can lead to duplicative investigative processes and potentially conflicting outcomes. From the taxpayers' standpoint, this can be perceived as needless bureaucracy and a waste of valuable resources. For policy-makers, it risks impeding innovation and dissuading global investors, setting back the government's economic objectives.[4]

Ontarians' personal information is already well-protected in the context of the telecommunications services that they receive pursuant to multiple federal laws and regulations applicable to federally regulated undertakings generally and to TSPs specifically.

Canada is known for taking a leadership role in the protection of personal information. The collection, use, and disclosure of personal information by TSPs is currently governed by the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA). PIPEDA has long been recognized as a leading piece of privacy regulation globally. With advances in technology and new ways of using personal information, the federal government proposed new legislation, Bill C-11, which sought to preserve the balanced, principles-based approach of PIPEDA, while creating important new individual rights and protections of personal information. Although Bill C-11 was not passed into law before the call of the federal election, it is anticipated that the new federal government will include privacy reform on the parliamentary agenda.

We respectfully disagree with the observation of the Privacy Commissioner of Canada, as echoed in the government's whitepaper, that Bill C-11 "represents a step back overall from our current law." Bill C-11 included additional individual rights, increased the obligations on organizations, gave more powers to the Office of the Privacy Commissioner, and introduced a serious enforcement regime backed by the threat of significant monetary penalties for those who contravene the proposed regulations.

As Bill C-11 sought to replace, and not merely amend, the privacy-related provisions of PIPEDA, it is not surprising that it received significant scrutiny and calls for changes. This is part of the normal legislative process and it was widely expected to be amended during the review process to deal with some of the concerns raised by stakeholders. It is premature for the Ontario government to conclude that updated federal legislation will

[4] IPC Submission, p. 6

be insufficient to protect Ontarians. Instead, the provincial government should proceed cautiously and continue to monitor the federal private sector privacy law reform process.

TSPs are also subject to the federal *Telecommunications Act* and the oversight of the Canadian Radio-television and Telecommunications Commission (CRTC). The CRTC's responsibility for privacy in telecommunications is explicitly set out in objective 7(i) of the *Telecommunications Act* (i.e. "to contribute to the protection of the privacy of persons").[5] While the investigation of complaints under PIPEDA is within the jurisdiction of the OPC, the CRTC has the power to create regulations concerning privacy with respect to telecommunications services. This power includes the ability to impose privacy standards that go beyond those found in PIPEDA and that are specific to industry use cases.

Under the powers granted in the *Telecommunications Act*, the CRTC has imposed regulatory measures and other actions to protect confidential customer information and safeguard consumer privacy. These measures include:

a. Prohibiting TSPs from disclosing confidential customer information other than the customer's name, address, and listed telephone number, without express consent of the customer, except in certain specified circumstances;
b. Prohibiting TSPs from using personal information collected for the purpose of traffic management practices for other purposes or disclosing such information;
c. As part of the Wireless Code and the Internet Code, contracts and related documents, including privacy policies, "must be written and communicated in a way that is clear and easy for customer to read and understand." Permanent copies of these documents must be provided to customers after they agree to a contract and TSPs must notify customers of amendments to their privacy policies at least 30 days before the amendments take effect, also in language that is plain, clear and easy to understand;
d. Issuance of an expectation that any TSP that charges for services will obtain express, opt-in consent before using a customer's data for the purposes of targeted advertising. The requests for consent must include a detailed explanation of the actual information that a company might use to target them for advertising purposes; and
e. Requiring TSPs to offer services that protect consumer privacy, such as unlisted number service, call display, call display blocking, prohibiting call return to a blocked number and call trace. The CRTC also established the

[5] *Telecommunications Act* (S.C. 1993, c. 38), ss. 7(i)

National Do Not Call List and the Unsolicited Telecommunication Rules framework.

In addition to the above measures, the CRTC engages in ongoing research that contributes to its understanding of current and emerging privacy issues in the communications market. For example, in 2017, the CRTC published its *Report on the Collection and Use of Canadians' Personal Information by Wireless Service Providers and Third Party Entities.*[6]

TSPs are also subject to Canada's anti-spam legislation, commonly referred to as CASL, which has as one of its purposes the regulation of "commercial conduct that discourages the use of electronic means to carry out commercial activities, because that conduct compromises privacy and the security of confidential information."[7] CASL – enforced by the CRTC, OPC, and Competition Bureau, establishes rules (including consent rules) pertaining to the sending of commercial electronic messages, the alteration of transmission data in electronic messages, and the installation of computer programs on another person's computer system, in the course of commercial activity. The detailed rules set out in CASL, coupled with the onerous penalty provisions under the Act, have ensured that TSPs have developed rigorous compliance programs in connection with the legislation's requirements.

As the above examples illustrate, the CRTC and the OPC have complementary roles in protecting the privacy of TSP customers across Canada, including Ontario. Given the Federal Government's plan to replace PIPEDA with new legislation that addresses new ways in which personal information is collected and processed, while also ensuring Canadian businesses can remain competitive and innovative in the global digital economy, there is nothing to suggest that this privacy framework is insufficient to protect the privacy of Ontarians who use federally-regulated telecommunications services.

Finally, the Government of Ontario has previously recognized that having overlapping provincial and federal regulations regarding the provision of telecommunication services is unnecessary to protect the interests of Ontarians. In December 2018, a bill entitled "Restoring Ontario's Competitiveness Act" was introduced by Ontario's Minister of Economic Development, Job Creation and Trade. The bill amended or repealed certain Acts, including the *Wireless Services Agreement Act, 2013* (WSAA) and two regulations made under it.

In explaining why the WSAA (which provided for certain consumer protections in relation to wireless services contracts) should be repealed, the Government

[6] https://crtc.gc.ca/eng/publications/reports/rp170106/rp170106.htm#4
[7] *CASL* (S.C. 2010, c. 23), s. 3

spokesperson indicated that it "has been superseded by federal regulations which provide nearly identical protections for all Canadians."[8] The spokesperson further stated that, "[b]y repealing it, we are harmonizing with federal regulations, which have made the original Act redundant", and that repealing the WSAA "frees businesses from burdensome duplicate regulations and provides consumers with clarity…"[9] The bill received royal assent and the WSAA was repealed on October 3, 2019.

The same logic applies with respect to protecting the privacy of Ontario users of telecommunication services. As described above, multiple federal regulations and administrative oversight by the OPC and CRTC provide for a robust framework that protects the personal information of telecommunication subscribers. Adding new provincial legislative or regulatory requirements – particularly those which may be inconsistent with federal requirements – would be redundant, create confusion for customers, and impose burdensome regulations on service providers that would impede the competitiveness of important federal undertakings that provide critically important services to Ontarians.

Recommendation: Any proposed provincial privacy legislation should expressly state that it does not apply to the collection, use or disclosure of personal information, if federal legislation applies to same.

2. Provide a transition period to enable organizations to effectively and efficiently implement new requirements

In considering introducing provincial private sector privacy legislation, the government must take into account the work required for organizations to bring their operations and procedures into compliance with any new regulations and provide for a transition period from the date of Royal Assent to the time that the new provisions come into force.

Organizations will need to undertake comprehensive reviews of their data management practices and identify necessary changes. They will have to assess and allocate human and financial resources to implement these changes and develop new policies, practices and procedures. Contracts with service providers and other third parties will have to be reviewed and may need to be renegotiated.

Depending on the changes, it is also likely that software and complex IT systems will have to be updated to account for processes, record keeping, and the administration of requests from data subjects that were not required prior to the enactment of the amendments. These IT changes may be complex, significant and costly. They also will

[8] https://mobilesyrup.com/2018/12/10/experts-split-ontario-bill-66-aim-repeal-wireless-services-agreement-act/
[9] Ibid.

not exist in isolation and will be part of a larger group of information technology projects that have to be budgeted for and prioritized by the organization.

As a result, a minimum transition period of 24-months from the date of Royal Assent to the time that any proposed legislation comes into force is needed. Longer transition periods may be required for specific provisions, such as those dealing with data portability.

In addition, any proposed legislation should provide that consents to the collection, use or disclosure of personal information obtained by organizations in compliance with PIPEDA prior to the date in which the provincial legislation comes into force will remain valid. Without such a provision, organizations could be in the position of having to reconfirm consent from Ontarians. This would not only subject Ontarians to a high volume of unwanted communications from organizations but also a loss in services if they fail to reconfirm consent.

Recommendation: Any proposed provincial privacy legislation should include a transition period of no less than 24-months from the date of Royal Assent to the time that the legislation comes into force. In addition, such legislation should state that consents obtained in compliance with PIPEDA should remain valid and not require re-confirmation.

3. Rights based approach to privacy

(a) Privacy as a fundamental right

CWTA agrees that the privacy of Ontarians should be protected and that Ontarians have the right to control the collection, use and disclosure of their personal information. However, protecting privacy rights requires different approaches depending on the context. For example, there are important differences between privacy rights in the context of state surveillance and privacy rights in the context of an individual entering into a commercial transaction with an organization.

In the context of commercial relationships, where businesses must collect personal information in order to provide and bill for goods and services, it is reasonable to expect the organization to use the information for normal business activities to serve their customers better, so long as the personal information entrusted to the organization is kept confidential and secure.

In the commercial context, the desire to protect individual privacy needs to be balanced with the legitimate needs of commercial organizations to collect, use, and disclose personal information. As stated in the IPC submission, this balance is

one of the virtues of federal privacy legislation and it should be the goal of any provincial legislation.

Declaring in the preamble, or elsewhere, that privacy is a "fundamental" right that supersedes all other fundamental rights and legal interests eliminates this balance. Rather than creating legislation that enables responsible businesses to serve customers and allow Ontario to be "the world's most advanced digital jurisdiction", it would regard all collection and use of personal information by organizations as suspect.

Even some supporters of the GDPR now recognize the undesirable distortions created by elevating the right of privacy above all other rights and legal interests. Alex Voss, Member of the European Parliament, and author of the report '*Comprehensive approach on personal data protection in the EU',* which resulted in the subsequent GDPR, now laments the disproportionality between privacy and other fundamental rights in the GDPR and the resulting negative impacts on innovation in the EU.

In his recently published position paper, *Fixing the GDPR: Towards Version 2.0,*[10] Mr. Voss states that this disproportionality is the result of taking data protection laws that were initially designed to protect citizens from the state and applying them to the relationship between citizens and companies:

> The GDPR fails to clarify that data protection is not an absolute fundamental right, but should instead be balanced with other fundamental rights or interests such as the right to life, to liberty and security, the freedom to conduct business or the freedom of the press….Besides that the GDPR does not take into account that the processing of personal data by the controller is, in itself, also protected by fundamental rights (e.g., the freedom of science or the freedom to conduct business).

This has resulted in what Mr. Voss calls the "prohibition principle" where:

> The GDPR sees any processing of personal data as a potential risk and forbids its processing as a principle. Such an anti-processing and anti-sharing approach does not make much sense in our data-driven economy and is contrary to the general objective in Art 1(3) GDPR that promotes the free movement of data."

He adds that the GDPR:

[10] https://www.axel-voss-europa.de/wp-content/uploads/2021/05/GDPR-2.0-ENG.pdf

> …wants to establish the view that processing of personal data is generally regarded as socially undesirable behaviour. This approach is not only latently hostile to progress. The result is that even the processing of personal data that is protected by fundamental rights or that is socially desirable for the protection of public interest comes under constant pressure to justify itself (e.g. sharing the data of potential recipients of vaccines or the delay of COVID-19 tracing apps).

By elevating the right to privacy above all other fundamental rights and legal interests, "the GDPR is seriously hampering the EU's capacity to develop new technology and desperately needed digital solutions, for instance in the realm of e-governance and health."[11]

Both PIPEDA and the proposed federal Bill C-11 illustrate that it is possible to protect the rights of individuals without the need to abandon the appropriate balance between privacy and commerce. Both regulations incorporate the principles of consent and transparency while also recognizing the need for organizations to collect, use and disclose personal information in appropriate circumstances.

Individual rights such as the right to access and correct information are recognized, and Bill C-11 proposed new rights such as the right to request the disposal of information. Organizations are held accountable for their use and security of personal information, and must be transparent with their customers about what information is collected and how it will be used and disclosed. Bill C-11 further restricted the collection, use or disclosure of personal information to purposes "that a reasonable person would consider appropriate in the circumstances."

Recommendation: Any proposed legislation should seek a balance between the protection of privacy and the legitimate need for organizations to collect, use and disclose personal information. As such, privacy should not be referred to as a fundamental right, as doing so could upset this balance by elevating it above other important rights and legal and societal interests. This would have a potentially detrimental impact on Ontario's ability to be a leader in innovation.

(b) Fair and appropriate purposes

In the white paper, the government proposes a general limitation on the collection, use, and disclosure of personal information to those activities that "a reasonable

[11] https://www.politico.eu/article/gdpr-reform-digital-innovation/

person would consider fair and appropriate in the circumstances."[12] Like the reasonableness standard set out in section 12 of the proposed CPPA, such a standard recognizes the need for a balance between individual and organizational interests.

Rather than preserve the flexibility that the reasonableness standard affords, however, the white paper introduces a rigid set of factors that must be considered for the handling of all personal information. Most problematic are undefined notions of whether the collection, use or disclosure "*is necessary to achieve the legitimate needs of the organization", " whether there are less intrusive means of achieving those purposes at a comparable cost and with comparable benefits", and "whether the individual's loss of privacy is proportionate to the benefits in light of any measures [..] to mitigate the impacts of the loss of privacy*."[13]

The vagueness of the listed factors will make them nearly impossible to implement and add no value to the principle that appropriate purposes are those that a reasonable person would consider appropriate in the circumstances. They will open organizations to routine second-guessing regarding the effectiveness and choice of business practices, regardless of the nature of personal information collected, its intended purpose, or the fact that the individual gave his or her consent to the collection, use or disclosure of their personal information for a purpose that a reasonable person would consider appropriate.

It is clear that the list of proposed factors is based on section 12(2) of the proposed CPPA. It is our understanding that subsection 12(2) is intended to codify the test referenced in *Turner v Telus Communications Inc.*, 2005 FC 1601, as presented in the Office of the Privacy Commissioner's (OPC) Guidance on inappropriate data practices: Interpretation and application of subsection 5(3) [of PIPEDA].[14] However, the OPC misconstrued the effect of *Turner* when creating the OPC guidelines.

The test that the OPC presents as the Federal Court's test for appropriateness is actually its own test. This test was previously applied by the OPC in its own investigation, but the Court refused to adopt it, despite the OPC urging it to do so.[15]

[12] Supra note 3, *Modernizing Privacy in Ontario,* p. 5
[13] Ibid.
[14] https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gd_53_201805/
[15] Ibid, para 67, "Put another way, and more briefly, it is not for the Commissioner, however knowledgeable and informed she or he might be with respect to the issues here coming before the Court, to set the agenda of this Court where hearings such as this are in the nature of *de novo* proceedings."

In fact, the kind of factors listed in subsection 12(2) have been applied by the courts only with respect to particularly sensitive personal information, such as sensitive medical information, biometric data and video surveillance of employees.

Codifying these factors and applying them to the collection, use and disclosure of all forms of personal information would remove judicial discretion and render the provincial privacy regulation an inflexible and prescriptive set of rules that must be applied regardless of the context. It would require organizations to undertake analysis and keep detailed documentation for all activities involving personal information, even those that should not be controversial, in case they were called upon to establish that all the listed factors had been considered.

The most appropriate way to address the concerns listed above is to not include a list of factors but instead rely on the flexible, context-driven reasonableness standard. If that is not acceptable to the government, the list of factors should only apply to the collection, use and disclosure of sensitive personal information. This change would ensure that the scope of the list of factors is not extended beyond current jurisprudence on the appropriateness of the collection, use and disclosure of personal information.

Recommendation: To preserve the flexibility that the reasonableness standard affords, any proposed legislation should not include the rigid set of factors to be considered for the handling of personal information as set out in the white paper. The vagueness of the listed factors would make them nearly impossible to implement and add no value to the principle that appropriate purposes are those that a reasonable person would consider appropriate in the circumstances.

(c) Fairness standard

The white paper proposes that appropriate purposes for the collection, use and disclosure of person information be limited to what “a reasonable person would consider fair and appropriate in the circumstances.” This is departure from PIPEDA, Bill C-11 and existing provincial privacy legislation, which do not include the consideration of fairness when considering what an appropriate purpose is. The whitepaper states that the inclusion of the fairness requirement will strengthen the appropriate purposes component of Ontario’s privacy framework. We respectfully disagree.

While it is relatively easy to contemplate what a reasonable person would consider to be an appropriate purpose for the collection, use or disclosure of personal information in a commercial context, the same cannot be said with respect to fairness. While the concept of fairness is used within the context of natural justice

and administrative law, it is not clear what it means for a purpose to be fair. In this latter context, fairness would seem to be in the eye of the beholder and not an objective standard. Requiring organizations to consider the fairness of a purpose will create uncertainty and confusion for both organizations and individuals.

Recommendation: Any proposed Ontario privacy framework should align itself with the legislation of other common law provinces and federal privacy law and not include fairness as a factor to be considered when assessing the purpose of an organization's processing of personal information.

(d) Disposal by service provider

The white paper proposes an individual right to request that an organization dispose of personal information that it has collected from the individual. The proposed language is similar to the language of section 55 of the proposed CPPA.

While we do not oppose a right to request the disposal of personal information, we have concerns with the way that CPPA proposed to do so. These concerns are equally relevant to any proposed Ontario privacy framework.

Section 53 of the proposed CPPA recognizes that organizations should be able to retain such information as long as is necessary to fulfil the purpose of the collection and to comply with CPPA and other legal obligations. However, this recognition is undermined by section 55, as the exceptions listed in that section do not cover all of the circumstances under which an organization may need to retain such information despite a disposal request.

While the list of exceptions proposed in the whitepaper is slightly broader than section 55 of CPPA, the exceptions to such a right must be still broader. For example, Article 17 of the GDPR, which provides the GDPR's version of the right to request disposal, does not apply if the organization needs to process personal information to exercise the right of freedom of expression and information, to comply with a legal obligation, or for reasons of public health, archiving in the public interest, or the establishment, exercise or defense of legal claims as the organization may choose to exercise.

Recommendation: Any proposed right to request disposal must include a broader list of exceptions that take into account legitimate reasons why an organization should be able, or may be required, to retain such information.

(e) Data portability

While we recognize that the concept of data portability is useful in the context of voluntary participation in data trusts and other data management schemes, CWTA

has concerns with introducing a portability right within an Ontario privacy framework and applying the corresponding obligations to all industry sectors.

First, while the inability to easily transfer personal information to an alternate service, such as some social media platforms or online data storage services, may present a barrier to switching service providers, such is not the case with every industry, including mobile wireless services. Wireless subscribers can easily switch to another wireless service provider, including being able to use the same phone number with the new service provider. This process is overseen by the CRTC which, given its expertise, is best-placed to determine whether there are any barriers to switching providers, and if so, how to address them.

Requiring the mobile wireless industry, and similarly situated sectors, to engineer technical solutions and procedures to enable personal data transfers that will provide little, if any, benefit to consumers is an unnecessary burden that will only make the provision of services more costly. It also gives rise to potential security risks as fraudsters could attempt to impersonate consumers and use the portability right to illegally obtain consumers' personal information.[16] In fact, it may require organizations to collect even more personal information from individuals for the sole purpose of being able to authenticate the individual in case a data transfer request is made.

Secondly, it is unclear how data portability enhances the privacy of Ontarians. If the concern is that the inability to easily transfer personal information presents a potential barrier to competition in some sectors, the matter is better dealt with under competition law.

The federal government is appropriately taking a cautious approach to introducing data portability rights. While section 72 of the draft CPPA included such a right, it is qualified by the requirement that both organizations must be subject to a data portability framework that is to be provided under future regulations.

CWTA recommends that the Ontario government not include a data portability right in any proposed legislation and instead continue to monitor developments regarding data portability in federal legislation.

If, notwithstanding the foregoing, data portability requirements are introduced, they should not be applicable to industries such as telecommunications, which are already subject to industry-specific regulatory oversight that can better assess the merits of applying such obligations to that industry.

[16] See https://www.theregister.co.uk/2019/08/09/gdpr_identity_thief/ for examples of how fraudsters have used new individual rights under the GDPR to illegally obtain information.

If such a right is implemented, in addition to them being subject to an applicable data portability framework that provides for standard processes and safeguards, impacted organizations must be provided sufficient time to implement such frameworks. The wireless industry's experience with designing and implementing a mobile number portability framework shows that operationalizing data portability is a time-consuming and often difficult task. As we have recommended to the federal government with respect to the proposed data portability provisions in CPPA, the entry into force of data mobility provisions should be delayed to three years after the applicable data portability regulations are enacted.

Finally, organizations should only be required to transfer information provided by the data subject, and should not be required to transfer information created by the service provider, including inferred data and derived data. Exceptions where compliance would reveal a trade secret or otherwise provide the new service provider a competitive advantage should also be included.

Recommendation: Data portability is a matter of competition law and not privacy regulation and should not be included in any proposed provincial privacy legislation. If it is included in proposed privacy legislation, it should not apply to industries such as telecommunications, which are already subject to industry-specific regulatory oversight that can better assess the merits of applying such obligations to that industry.

4. Safe use of automated decision-making

The whitepaper proposes that an Ontario private sector privacy framework address the use of automated decision-making systems (ADS). While CWTA does not oppose the regulation of ADS, it is questionable whether privacy legislation is the appropriate place to deal with this issue.

As leading technology law expert Barry Sookman has noted:

> The automated decision systems provisions of [Quebec] Bill 64 and the *CPPA*, like the comparable provisions in the GDPR, are not, however, truly directed at privacy-related mischief. They regulate the use of particular technologies more than the use of information – though, due to the nature of the technologies in question, the line is admittedly difficult to draw. Further, the goals are not the protection of reasonable expectations of privacy – which is what privacy laws

> advance – but to avoid other harms such as ensuring that decisions are not biased or inaccurate.[17]

These potential harms, Mr. Sookman argues, are already addressed under other regulatory frameworks such as competition laws, consumer protection laws, and human rights legislation:

> The regulation of automated decision making under privacy law will likely result in privacy commissioners such as the OPC, with limited or no expertise in the other regulatory areas, becoming mixed up in areas that are better handled by the existing regulatory regimes already in place.[18]

To the extent that existing regulations do not address all of the issues arising from the use of ADS, stand-alone legislation or best practices are more appropriate than trying to deal with the complex issue under privacy laws.

Notwithstanding the above, if the government decides to address the use of ADS, the provisions proposed in the whitepaper require some amendments.

The proposed definition of "automated decision system" references "technology that assists or replaces the judgement of human decision-makers…."[19] This definition is too broad. Not all systems are the same, and the degree to which they aid human decision-making will vary. The focus on any regulation of ADS should be limited to those systems that could materially impact human decision-making. As such, the word "materially" should be inserted before "assists".

Similarly, the obligation to provide an explanation to an individual of any prediction, recommendation or decision made using ADS should be limited to circumstances in which the use of ADS could have a significant impact on the individual.

Other than the right to request an explanation, and a general right to request the correction of personal information that is not specific to the use of ADS, we do not agree with the other prohibitions and safeguards proposed in the whitepaper regarding the use of ADS.

The proposed prohibitions are redundant as the general purpose threshold for the collection, use and disclosure of personal information, together with the transparency

[17] https://www.barrysookman.com/2021/04/30/using-privacy-laws-to-regulate-automated-decision-making/
[18] Ibid
[19] Supra note 3, *Modernizing Privacy in Ontario,* p. 12

and consent requirements, offer sufficient protections to individuals. Adding overlapping qualifiers invites uncertainty rather than clarity for both organizations and individuals.

We also agree with the approach taken in the proposed CPPA that requires, upon request, an explanation of a use of ADS, but does not give the individual the right to challenge the decision. As referenced above, privacy legislation is not the appropriate vehicle for addressing all potential harms arising from the use of ADS.

Recommendation: The regulation of ADS should not be dealt with under privacy legislation and is best left to stand-alone legislation or best practices. If the government elects to address ADS in proposed privacy legislation, it should be limited as described above.

5. Enhancing consent and other lawful uses of personal information

CWTA supports the government's goal of improving the meaningfulness of consent and providing alternative authorities for collecting and using personal information to reduce consent fatigue.

(a) Implied consent

In the white paper, the Ontario government indicates that it is considering allowing organizations to rely on implied consent, "taking into account the sensitivity of the personal information involved and the reasonable expectations of the individual".[20] CWTA strongly supports the inclusion of implied consent. It is a concept that works well under existing Canadian privacy laws, helps achieve the desired balance of protecting the privacy of individuals and facilitating the legitimate and responsible use of data by organizations, and would reduce "consent fatigue" for Ontarians.

(b) Alternatives or exceptions to consent

Consent fatigue is a real problem for organizations and individual Canadians. If individuals are asked to provide express consent for nearly all collections and uses of personal information, rather than just for activities they would not expect under the circumstances or for activities that require the collection and use of sensitive information, the act of seeking express consent will lose its meaning and individuals will not take consent requests seriously. We have seen this phenomenon occur with website cookie notices.

[20] Supra note 3, *Modernizing Privacy in Ontario,* p. 17

The white paper proposes several grounds for collecting, using and disclosing personal information without requiring consent. The first ground is entitled "business activities".

(i) Business activities

The white paper proposes that express consent not be required for the collection or use of personal information for what it terms "business activities".[21] The draft provisions are largely based on section 18 of the proposed CPPA, which provides an exception to the requirement for express consent if the collection or use of personal information is made for a business activity that "a reasonable person would expect" and that is "not collected or used for the purpose of influencing the individual's behaviour or decisions".

However, subsection (2) of the proposed provision further limits what is considered a business activity to five sets of circumstances. Given the reasonableness standard in subsection (1), subsection (2) stands out as entirely redundant and out of line with the standards applied by Canada's trading partners.

By contrast, California's CCPA considers the pace of data-driven business models of the digital economy. It allows organizations to collect, use and even sell personal information without having to obtain consent (except in the case of minors), provided they must give individuals the right to opt-out of having their personal information sold.

For its part, the GDPR also takes a much more flexible approach to consent, fully recognizing the contextual nature of the requirement for express or implied consent by allowing processing without express consent where "*processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*"[22]

As drafted in the white paper, the proposed business activities provisions makes, with few exceptions, express consent the default basis for the collection and use of personal information. This would not only put Canada out of step with its trading partners, it would abandon both the flexible approach of PIPEDA that has served Canada so well and the rational approach that grounds implied consent in the circumstances that surround it.

[21] Ibid.
[22] GDPR, Article 6(1)(f)

The white paper's proposal for business activities could disadvantage Ontario organizations by imposing a narrow, rules-based approach to consent. In contrast to the realistic approach adopted in the GDPR and the CCPA, the approach proposed in the white paper would require organizations operating in Ontario to disproportionately rely on express consent, with no gain for the individual's privacy. This onerous approach to consent means organizations operating in Ontario will face the cost and administrative burden of managing a distinct consent regime that is likely to put them at a competitive disadvantage.

Recommendations: The government should continue to monitor the progress of consent-related provisions in federal privacy reform.

With respect to the provisions proposed in the white paper, to ensure that any proposed legislation provides a rational, principled and technology-neutral approach that has been the strength of privacy regimes in Canada, subsection (2) should be discarded. This would allow the contextual criteria of subsection (1) to determine whether express consent is required. The collection and use of such information also remains subject to the "fair and appropriate" standard discussed above.

To address consent fatigue, keep express consent meaningful, and ensure that individuals are informed about the collection, use and disclosure of their personal information on complex technological platforms, the activities currently listed in subsection (2) should be left to the obligation to disclose them in privacy policies.

In the alternative, if the government is intent on limiting business activities to a prescribed set of circumstances, the activities listed in the proposed subsection (2) must be expanded. At a minimum the following two additional business activities should be added, each of which would remain subject to the reasonableness standard and the restriction on influencing behaviour or decisions set forth in subsection (1):

- an activity that is carried out to understand and analyze the interests, needs, and preferences of customers and users;

- an activity that is carried out to assess, develop, enhance or provide products and services;

With respect to paragraph (2)5 – "Any other prescribed activity", if, notwithstanding our recommendation above, a list of business activities remains part of any proposed legislation, paragraph (2)5 should remain. As noted above, the prescribed list of activities in paragraphs 1-4 is extremely restrictive and virtually guarantees that it will require updating to reflect changes in technology and

business models where it is generally agreed that express consent for the collection or use of personal information should not be required.

If proposed legislation is to include a list of qualifying business activities, it must allow for the list to be updated in an efficient manner. Requiring a statutory amendment to add a prescribed activity does not allow for government to respond quickly and make necessary changes. This could place organizations doing business in Ontario at a disadvantage compared to organizations operating elsewhere.

(ii) Prospective business transactions

The white paper proposes an exception to consent for prospective business transactions and proposes provisions similar to those found in section 22 of the proposed CPPA.

Like the CPPA, the white paper proposes a condition that personal information must be de-identified before it is used or disclosed in the context of a business transaction (as defined) and remains so until the transaction is completed. This requirement does not reflect the reality of business transactions.

As part of the due diligence process, it is common that a prospective purchaser of assets of the company needs to review information pertaining to key employees, as well as client lists. This information is required for the acquiring party to assess the level of risk and the value of the transaction.

Current PIPEDA provisions in this regard properly reflect the reality of exchanges of information that is necessary to determine whether to proceed with a transaction and, if so, under what terms. Privacy is protected through the requirement for an agreement that governs the exchange of personal information, limiting it to what is necessary and specifying that it can only be used for the purposes related to the transaction. Appropriate security safeguards must be applied and the receiving organization must be obligated to return this information should the transaction not proceed.

There is no indication that the above-mentioned provisions of PIPEDA are not working, and the proposed provisions in the white paper contain similar safeguards. It is not clear what problem the additional requirement to de-identify information prior to disclosure is trying to solve. Rather, it is an unnecessary requirement and makes the proper exercise of due diligence impossible.

Recommendation: Subsection (1)(a) of the proposed “Prospective business transaction” provision should be deleted.

6. Data transparency for Ontarians

(a) Privacy by design and privacy impact assessments

The white paper poses the question of whether there should be a mandatory requirement for “Privacy by Design” principles or “privacy impact assessments”.

Privacy by design principles provide that organizations should consider the protection of privacy throughout the design and development of products and services, and not as an afterthought. While these principles offer helpful guidance to organizations on how to protect the privacy of individuals and to fulfill their legal obligations, we have concerns with requiring organizations to follow these principles.

Every product or service is different and requiring organizations to follow strict standards regardless of the context risks creating unnecessary obstacles to, and increases the costs for, the development of innovative products and services. In addition, some of the principles, such as requiring that products be designed to offer the highest level of privacy as the default setting could also create a bad user experience for Ontarians, requiring them to reprogram products to function as expected.

Rather than making privacy by design a part of any proposed privacy legislation, we recommend that the promotion of privacy by design principles be part of the IPC’s mandate to educate and promote best practices.

If, notwithstanding the above, the government decides to include privacy by design principles as part of proposed legislation, any requirement to follow such principles should be qualified to take reasonable commercial considerations into account. This includes consideration of the cost of implementation and the degree of risk to privacy involved. Similarly, the “highest level of privacy” should depend on the context and take into account technical and interoperable standards used in other jurisdictions. Requiring products and services to comply with different settings or standards than other jurisdictions could negatively impact the availability of such products or services to Ontarians.

Similarly, while privacy impact assessments (PIAs) are good practice, requiring PIAs in all circumstances will create unnecessary burdens on organizations. If, as recommended in the “Administrative Monetary Penalties” section, any proposed legislation includes due diligence as a mitigating factor to the imposition of monetary penalties, organizations will already have sufficient motivation to employ

PIAs where appropriate. For this reason, we do not think that it is necessary to require PIAs.

If, notwithstanding the foregoing, the government decides to include a PIA requirement in any proposed legislation, such requirement should be qualified so that organizations are not required to engage in formal analysis of all processing activities, regardless of the context. For example, under the GDPR, organizations are only required to conduct PIAs when the processing activity presents a "high risk" to the data subject, taking into account the nature, scope, context and purpose of processing.

Recommendation: Following privacy by design principles, or undertaking privacy impact assessments, should be encouraged by not made mandatory. Every good and service is different, and imposing strict standards regardless of the context or risk to privacy could create unnecessary obstacles to, and increase the costs for, the development of innovative products and services.

(b) Validity of Consent

The white paper proposes that, for consent to be valid, it must be "reasonable to expect that the individual understands the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting".[23] It further sets out in the proposed subsection (3)2 a prescribed list of information that must be provided to the individual.

The proposed subsection (3)2 does not reflect the need identified by the IPC for a principles-based privacy regime. Instead, it imposes highly prescriptive rules regarding the kind of information that must be provided to the individual, at or before the time that consent is sought. Not only does this rigid approach foreclose other reasonable methods for obtaining informed consent, it throws into doubt the validity of consents already obtained by organizations that did not follow these prescriptive requirements.

The unintended consequence is that Ontarians could be inundated with requests to re-confirm consent for previous collections and processing of personal information. This would not only impose undue burdens on organizations, it would also result in a confusing and unwelcome inconvenience for individual Ontarians, especially where the provision of services that utilize such information are interrupted as a result of the omission by the individual to re-confirm consent.

[23] White paper, page 28 – "Information for consent to be valid"

Recommendation: Subsection (3) of the proposed provisions dealing with validity of consent should be amended to remove paragraph 2. If paragraph 2 remains as part of any proposed legislation, it should be recast as an exemplary list of possible, but not the only, ways by which an organization can satisfy the requirement for valid consent. In addition, it should be expressly stated that any consent obtained in compliance with PIPEDA prior to the coming into force of provincial legislation remains valid.

7. A fair, proportionate and supportive regulatory regime

In the white paper, the government suggests that to provide regulatory oversight it could make the IPC responsible for oversight and compliance with a new private sector privacy regime, which would include stronger enforcement powers, as well as require the IPC to provide support and guidance to organizations.

(a) Role of the privacy commissioner

The main goal of any private sector privacy regime should be to help organizations comply with the law. This is best achieved when the regulator is able to work cooperatively with organizations to provide guidance and consultation on how organizations can achieve their business objectives while respecting the privacy rights of individuals. While some of this collaboration results from inquiries made by organizations, providing the regulator with the power to investigate, audit, and attempt to resolve and mediate complaints also lends itself to the collaborative approach, as the vast majority of organizations want to comply with the law.

This approach has been successful at both the federal level and in provinces that have their own private sector privacy laws, with most valid complaints being resolved voluntarily. If, as proposed in the white paper, the regulator is made both the enforcer and the advisor, much of the benefit of the collaborative approach risks being lost. Many organizations would hesitate to consult with the IPC knowing it has the power to directly impose significant monetary penalties on them. At the same time, the IPC may find that it no longer has the resources to engage constructively with organizations, as it devotes the bulk of its resources to enforcement actions. Both of these outcomes would harm the government’s goal of fostering economic growth through the responsible use of data and digital technology.

For the above reasons, to the extent that any proposed privacy legislation includes administrative monetary penalties or fines, the power to levy such penalties or fines should not rest with the IPC. As set out in the proposed CPPA, the IPC should be limited to making recommendations regarding penalties or fines. The

decision to seek such a penalty or fine should rest with the attorney general and be adjudicated by the provincial courts.

Recommendation: The primary role of the privacy commissioner should be to help organizations comply with the law. Giving the commissioner the power to levy fines or penalties would hinder such collaborative approach. As such, the authority to levy fines or penalties should not reside with the privacy commissioner.

(b) Administrative monetary penalties

As observed above, in other Canadian jurisdictions, the vast majority of valid privacy complaints are voluntarily resolved without the threat of the kind of penalties or fines proposed in the white paper. In addition, while penalties may be necessary to deal with organizations that willfully ignore their privacy obligations, most organizations, including CWTA members, regard the protection of their customers' privacy as a serious responsibility. It is within this context that any discussion of penalties or fines must take place. As the IPC (British Columbia) stated in its submission to British Columbia's ongoing consultation on privacy reform, "monetary penalties would be reserved for the most serious violations of the law, for the worst offenders and the worst offences."[24]

In the white paper, the government seeks to protect fairness in the imposition of a penalty with a list of factors that "may" be considered. This would mean that the decision maker has no obligation to consider any factors in assessing a penalty. Rather than reserving monetary penalties for the most egregious offenders, even organizations that had tried their best to comply could be exposed to significant monetary penalties. This would have a chilling effect on innovation in Ontario, as there would no mitigating factors that must be considered when assessing penalties. Contrast this to section 93(2) of the proposed CPPA, which requires the Commissioner to consider a number of factors before recommending a penalty to the tribunal.

In addition to requiring the decision maker to consider a list of factors before assessing a penalty, the factors that must be considered should be expanded to include the novelty of the facts or findings in the case, as well as the organization's due diligence and good faith in attempting to comply with the legislation. For example, cyberattacks are a constant and evolving threat. Even the most highly-protected institutions, including the military, suffer breaches of security. Fairness dictates that the application of penalties must be limited to organizations that have not met their obligations. In the case of security obligations, the test is not whether

[24] https://www.IPC.bc.ca/special-reports/3465 p. 20

there has been a breach, but rather whether the organization has met its due diligence obligations in implementing security safeguards.

Recommendation: Monetary penalties should be reserved for the most serious violations by actors who flagrantly ignore the law. They should not be used to punish organizations who have tried to comply. In addition, the decision maker should be required to consider a list of mitigating factors, as described above, before imposing a monetary penalty.

(c) Procedural fairness and right of appeal

A principles-based and balanced privacy regime requires that the exercise of any powers granted to the IPC be subject to procedural fairness.

(i) Compliance Orders

The white paper proposes that the IPC could have order making powers, including "the ability to order an organization to take measures to comply with the law, stop doing something that is in contravention of the law, make public any measures it has taken to fulfill its obligations under the law, and destroy any personal information collected unlawfully."[25] It further suggests that any such order could be appealed to the Divisional Court "on a question of law".[26]

The Privacy Commissioner, however well-intentioned, is a single decision maker, fallible as any other. The Commissioner may also not have the necessary business experience to properly assess the balance between the individual's right to privacy and the legitimate need of organizations to collect and process personal information. Decisions will have a long-lasting, formative influence on interpretations of privacy regulations, as well as direct impacts on organizations. For these reasons, organizations should not have to wait until after an order is made to seek remediation of an erroneous position of the Commissioner in a timely manner.

A recent and compelling illustration of the need for such preliminary recourse arose in 2019 when the federal OPC erroneously interpreted PIPEDA to require consent for cross-border transfers of personal information. Such an interpretation would have had significant detrimental impacts on the global competitiveness of Canadian organizations, making routine data transfers that are essential to their operations impractical, and in many cases operationally impossible to implement.

[25] Supra note 3, *Modernizing Privacy in Ontario,* p. 34
[26] Ibid, p. 37

The OPC's new requirements also risked contravening Canada's commitments under several international trade and other agreements, and would have made Canada an outlier when compared to its trading partners around the world. Fortunately, the OPC reversed its position after launching a public consultation that overwhelmingly demonstrated its legal mistake. However, public consultations are infrequent processes and would not address all potential errors.

The incident underscores the need for a preliminary recourse to the courts where a respondent organization can properly defend its good faith interpretation of the law in a timely fashion, and before the Commissioner issues a finding. In the federal case cited above, had such a right been provided in PIPEDA, the affected organization could have turned to the Federal Court as the investigation was ongoing to seek clarification regarding the legality of the position taken by the OPC.

In addition, as referenced above, because the Commissioner is a single decision maker whose decisions can have long-lasting and serious impacts, it is important that the decisions of the Commissioner be subject to rigorous review. Limiting review on appeal to questions of law is not sufficient. The standard of review must also include the reasonableness of any questions of fact or question of mixed law and fact.

Recommendation: As a matter of procedural fairness, organizations should be provided with recourse to the courts to seek an interpretation of law before the Commissioner issues a finding. In addition, any decision by the Commissioner should be subject to appeal not only on questions of law, but also on the reasonableness of any questions of fact or question of mixed law and fact.

(ii) Assistance or compensation orders

CWTA strongly opposes the government's suggestion that the IPC could be given the power to order organizations "to assist or compensate individuals for losses, financial or otherwise in the event of a failure of security safeguards involving personal information."[27] As mentioned above, cyber-attacks are a constant and evolving threat. Even the strongest security measures can be vulnerable to attack. Making organizations responsible for any failure of such safeguards would, in effect, make data breaches a strict liability offence. Rather than making Ontario "the world's most advanced digital jurisdiction," such a measure could serve as a significant deterrent to organizations making their

[27] Supra note 3, *Modernizing Privacy in Ontario,* p. 38

products and services available in Ontario, and deprive Ontarians of the benefits of digital innovation.

Moreover, the assessment of individual losses is an issue that falls outside the expertise of the IPC. To the extent that an individual suffers harm from a failure of security safeguards, they already have remedies through privacy claims in tort and contract law, where the courts are best placed to assess an organization's responsibilities and the appropriate remedy.

Recommendation: The IPC should not be given the power to order organizations to assist or compensate individuals.

8. Supporting Ontario innovators

The white paper includes a discussion of de-identified information and anonymized information. CWTA agrees that any proposed legislation should clearly and practically define these two concepts. One of the major problems with Bill C-11 is that it defined the term "de-identify" in a way that appears to encompass what most would consider anonymous information. The resulting use of the term in Bill C-11 renders some provisions impractical and/or creates unintended circumstances.

(a) De-identified information

CWTA agrees that de-identified information, as defined in the white paper, should be considered personal information because it is reasonably foreseeable that such information would be used in conjunction with other information to identify the data subject. Notwithstanding the foregoing, we also agree with the government's proposal that certain provisions of the proposed privacy legislation, such as an individual's right to request access, append, port or delete such information, should not apply to de-identified information.

(b) Anonymous information

CWTA agrees that any proposed legislation should expressly state that it does not apply to anonymous information, and that doing so may encourage organizations to anonymize information when possible. However, we do not agree with the proposed definition of anonymous information, which states that information must be "altered irreversibly…in such a way that no individual could be identified…"[28]

[28] Supra note 3, *Modernizing Privacy in Ontario,* p. 41

We understand that there may be concern about the risk of re-identification, given the amount of personal data on the internet and unprecedented data mining capacity. The right to privacy and the differentiation between personal and non-personal information has never required the complete absence of any risk of re-identification.

In the Supreme Court of Canada decision, *R. v. Duarte*, [1990] 1 SCR 30, the Court defines the right to privacy as "*the right of the individual to determine when, how, and to what extent he or she will release personal information*" (our emphasis). The Federal Court of Canada in *Gordon v. Canada (Health), 2008 FC 258* states that information is "*personal*" where it creates "*a serious possibility that an individual could be identified through the use of that information, alone or in combination with other available information".* It is therefore established in Canadian law that, where there in not "*a serious possibility that an individual be identified*", there is no personal information.

It should follow then that any definition of anonymous, or non-personal information, in the proposed privacy legislation should employ the "serious possibility" or "reasonably foreseeable" standard.

Recommendation: We agree with the government's proposal that certain provisions of any proposed privacy legislation should not apply to de-identified information. However, we are concerned with the proposed definition of "anonymous information" and recommend that it be amended to include a "serious possibility" or "reasonably foreseeable" standard.

For questions or comments regarding this submission, please contact:

Robert Ghiz
President & CEO
rghiz@cwta.ca

Eric Smith
Senior Vice President
esmith@cwta.ca