OBA Submission on
Modernizing Privacy in Ontario

Submitted to: Ministry of Government and Consumer Services - 21-MGCS015

Submitted by: Ontario Bar Association

Date: September 3, 2021

ONTARIO BAR ASSOCIATION
A Branch of the Canadian Bar Association

L'ASSOCIATION DU BARREAU DE L'ONTARIO
Une division de l'Association du Barreau canadien

Table of Contents

I. Introduction

The Ontario Bar Association ("**OBA**") appreciates the opportunity to provide this submission in response to the Ministry of Government and Consumer Services' Public Consultation on Modernizing Privacy in Ontario.

Established in 1907, the OBA is the largest volunteer lawyer association in Ontario, with over 16,000 members who practice on the frontlines of the justice system and who provide services to people and businesses in virtually every area of law in every part of the province.

Each year, through the work of our 40 practice sections, the OBA provides advice to assist legislators and other key decision-makers in the interests of both the profession and the public and delivers over 325 professional development programs to an audience of over 12,000 lawyers, judges, students and professors.

This submission was prepared by members of the OBA Privacy Law and Access to Information Section, which includes lawyers who practice privacy law across a wide range of industries and economic sectors impacted by and subject to privacy legislation.

II. Overview

We commend the government for the important work of addressing the current gap in legislation regulating and protecting personal privacy in Ontario's digital economy.

We have confined our commentary to addressing whether the proposed language and structure of the provisions contemplated in the White Paper, *Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy* (the "White Paper"), align with the legal objectives and issues of concern raised therein. We have also provided commentary on opportunities we see for further development and consultation on the legislation to assist in achieving the identified objectives.

At a high level, the proposed legislation in the White Paper makes significant contributions to enhancing a regulatory approach to privacy in a post-pandemic economy that is defined by digital connection, and data as a central resource in the information economy.

III. Modernizing Privacy Rights in Ontario: *Key Areas of Reform*

For the purposes of the public consultation, this submission focuses on the proposed clauses in the White Paper. Our members believe these amendments will help the government more effectively and efficiently achieve their purpose and the interests of the public and our members.

Based on our members' knowledge of the applicable legal principles and their thorough understanding of this area, we recommend revisions to the following areas:

A. Rights-based approach to privacy;
B. Enhancing consent and other lawful uses of personal information;
C. Data transparency for Ontarians; and
D. A fair, proportionate and supportive regulatory regime.

A. Rights-Based Approach to Privacy

The White Paper identifies a rights-based approach to privacy as a key area of reform. The White Paper says that *"new rules and rights are needed to protect Ontarians from potentially unfair practices and maintain a high level of trust and confidence in the digital economy*." The OBA's suggestions below address how these notions could manifest in the legislation.

a. Preamble

Preambles frame the interpretation of their corresponding statutes. The White Paper's proposed preamble reads as follows:

> *Privacy is a foundational value in society. Every individual is entitled to a fundamental right to privacy and the protection of their personal information.*
>
> *Changes in technology have allowed organizations to easily collect vast amounts of personal information about individuals, often undermining the control that an individual has over their personal information.*
>
> *To establish the trust and confidence of individuals, organizations must be subject to rules, guided by principles of proportionality, fairness and appropriateness with respect to the collection, use or disclosure of personal information.*

Taken together, the preamble emphasizes the importance of a right to privacy in personal information, and the role that modern technology can play in shifting the locus of control over personal information away from the individual.

Appropriateness

While the principles of proportionality and fairness are well developed legal concepts, it is not clear that "appropriateness" is sufficiently well defined in the jurisprudence to add interpretive value. If the intention is to emphasize the importance of "appropriateness of purpose", in the context of what a reasonable person can expect of the processing of their personal information, further clarity on this point would be beneficial.

Transparency

The value of transparency as an underlying principle, necessary to give effect to a meaningful right of privacy, is not articulated in the preamble. In its discussion of the preamble, the White Paper states that "a key factor in establishing public trust and confidence in the right to privacy will be the provision of genuine transparency requirements and strong, independent oversight for Ontarians."

To enshrine transparency as an interpretive principle through which to frame the rights and obligations in the legislative scheme, specific language on transparency in the preamble would be appropriate. The language should recognize the principle of transparency with respect to an individual's right to know the purposes for which their personal information is collected, derived and/or inferred, and then processed, used and/or disclosed to engage with them. The language should also acknowledge the reasonable limits on individuals' right to transparency and access to information, against competing interests of organizations to protect proprietary information to provide innovative digital products and services to individuals.

b. ***Appropriate purposes***

In order to create a fundamental right to privacy, the legislative language should endeavour to create a rebuttable presumption in favour of that right for individuals, over an organization's right to collect, use or disclose their personal information. We recommend a more restrictive construction when setting out when an organization may collect, use or disclose personal information.

As drafted, the White Paper's legislative language uses a "may" / "only" formulation, constructed such that organizations may only collect, use and disclose personal information "that a reasonable person would consider fair and appropriate in the circumstances."

In contrast, the construction "shall not" / "unless", emphasizes an obligation on the part of the organization collecting and/or processing the personal information not to do so, as a default course of action.

This distinction, while seemingly trivial, is significant in today's modern digital environments where many organizations gather significant personal information in the form of data exhaust, generated collateral to the primary purpose(s), and for which subsequent utility may be discovered or derived.

The "may"/"only" legislative construction could be interpreted to permit organizations to provide ex-post justifications for why a reasonable person would find the new collection, use or disclosure fair and appropriate. Without an indication to the contrary, this formulation could also shift the onus to the individual to establish that a reasonable person would find the organization's collection, use or disclosure of such personal information unfair or inappropriate.

The alternative construction, 'an organization *shall not* collect, use or disclose personal information *unless*...' avoids these concerns. It would also constrain the interpretive scope of this clause and make clearer the requirement that organizations ensure that a reasonable person would view their activities to be fair and appropriate.

If the government aims to establish a rebuttable presumption in favour of an individual's right to privacy in their personal information, over an organization's right to collect, use and disclose that personal information, then the "shall not"/"unless" construction is more likely to achieve this objective.

c. ***Factors to consider***

Regardless of an individual's consent, every organization must meet the "Appropriate Purpose" test, in limiting what personal information they collect, use and disclose. Organizations are required to consider specific factors, in determining if their collection, use and disclosure is fair and appropriate.

The four factors require organizations to consider: (1) the volume, nature and sensitivity of the personal information; (2) the necessity of processing to achieve "legitimate needs" of the organization; (3) whether there are less intrusive means of achieving the "appropriate purpose" identified as the justification for the collection, use or disclosure of personal information at comparable cost and benefit; and (4) whether the accompanying loss of privacy is proportionate, "in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy..."

Further clarity and flexibility

Given the breadth of personal information the private sector gathers on individuals across all facets of personal, economic and social life, it will be practically impossible for the legislation to anticipate the particular factors that will be relevant in determining if the appropriate purpose for which an organization collects, uses or discloses personal information is fair and appropriate.

Volume, nature, sensitivity, and necessity, the availability of less intrusive means, and the proportionality and availability of measures to mitigate the loss of privacy are all likely to vary from sector to sector, and over time.

While the proposed set of factors is broad, it may be helpful to address the dynamic and contextual nature of privacy across different sectors of the economy, and across time, by making reference to:

- the non-exhaustive nature of the factors;
- industry standards and practices developed in the area to which the personal information relates; and/or
- the promulgation of regulations identifying further factors to consider.

Proportionality

The fourth factor listed in the draft legislative language, requires an organization to consider "whether the individual's loss of privacy is proportionate to the benefits in light of any measurements, technical or otherwise, implemented … to mitigate the impacts of the loss of privacy."

It is appropriate that the draft legislative language requires organizations to consider the measures they will take to mitigate an individual's loss of privacy, as part of the process of factoring the proportionality of the loss/benefit equation, when determining whether the collection, use and disclosure is "fair and appropriate".

We note that the phrase "in light of any measurements, technical or otherwise" does not provide additional clarity for organizations attempting to apply this "proportionality" factor. Whether mitigating measures can change and/or whether the benefit is proportional to the loss of privacy, will emerge from within particular sectors of the data economy, and depend on the type of personal information, the actual risk of a loss of privacy, and the risk of harm from such loss.

We recommend that the legislative language clarify how an organization should "weight" its mitigating measures, when factoring them into the proportionality analysis of the benefits conferred, against the loss of privacy that results from the purpose for which the individual's personal information was collected, used, or disclosed.

The proportionality of the organization's purpose will depend on whether its mitigating measures were proportional to the volume, nature and sensitivity of the personal information, and other contextual factors that may be particular to an industry or sector of the economy.

Adding language in the legislation that references standards of protection and mitigation for personal privacy that exist in the appropriate industry (e.g. health, finance, advertising, etc.), will help organizations to weight their mitigating measures, when conducting the required proportionality assessment of their collection, use and disclosure of personal information.

Individual vs. collective benefits

The fourth factor does not make it explicit that the proportionality factoring must be in relation to the benefits *conferred on the individual* who is exposed to the loss of privacy. The benefits and costs of a proportionality analysis should also take into account the collective benefits and harms that can manifest from aggregated losses of individual privacy.

Much of the innovation in modern data processing of personal information offers diffuse benefits to individuals, and acute benefits to organizations. Harms are often experienced on a group basis, and while potentially *de minimis* at an individual level, are disproportionate to the benefit derived by the organization. This fourth "proportionality" factor should incorporate language that emphasizes the contextual nature of the relationship between the benefits and harms at scale.

d. ***Purposes***

The proposed purpose clause requires that at or before the time of collection of any personal information, the purpose for which the information is to be collected, used or disclosed "shall" be recorded.

Notwithstanding our comments above, with respect to establishing rebuttable presumption to privacy, we also acknowledge that in practice, organizations may find a new purpose for the information post-collection or pre-deletion.

To address this common situation, we propose that language be added that obliges an organization to identify the new purpose, and where required, promptly disclose the new purpose to the individual and obtain the individual's consent.

e. ***Legitimate needs***

The language of this proposed section aims to limit activities that an organization may claim are "necessary" in the pursuit of its "legitimate needs", by proscribing what constitutes a legitimate need. Our comments are focused on two aspects; influencing individuals under 16 and legitimate actions that cause harm.

Influencing individuals under 16

Proposed subsection (a) prohibits monitoring or profiling of individuals under the age of 16, *"for the purposes of influencing the individual's behaviour or decisions"*. The OBA supports the intent of this provision. However, the government should consider including exceptions for categories of socially beneficial influencing activities by organizations.

For example, the Government may decide it wishes to exclude, from this prohibition, activities that benefit the mental or physical health of individuals under the age of 16, where appropriate consent has been obtained

Legitimate actions that cause harm

Subsection 4(b) proposes to prohibit an organization from claiming that the purpose of its collection, use or disclosure of personal information is fair and reasonable, because it serves a legitimate need of the organization, if those purposes are known or are likely to cause, significant harm to the individual, or group of individuals.

The clause as it is drafted, does not take into account scenarios where significant harm can be legitimately caused to an individual or group of individuals. Examples include the enforcement of contractual rights (such as the collection of a debt), and the prevention and reporting of illegal activity.

We therefore recommend inclusion of the phrase 'without juristic reason', or some similar language, to allow for purposes that may legitimately cause significant harm to an individual, require the collection and processing of personal information to do so, and are nevertheless permitted at law.

Recommended change:

(4)(b) purposes that are known to cause, or are likely to cause, significant harm to the individual or groups of individuals ***without juristic reason;***

f. *Limiting collection, use and disclosure*

The government should ensure that the language in these provisions allow for personal information to be collected, used and disclosed provided certain requirements (such as obtaining knowledge and consent where appropriate) are met. Such language recognizes the dynamic and evolving nature of personal information in relation to an organization's activities, purposes and relationship to the individual.

Further, requiring that the personal information an organization collects, uses or discloses be "necessary" for the purposes identified, narrowly constricts the obligation imposed on the organization. This proposed clause would benefit from additional clarification of the term "necessary" to prevent litigation and/or privacy complaints in the difference between an organization's interpretation of necessity and an individual's interpretation.

Recommendation:

The personal information is ***reasonably*** *necessary for the purposes determined and recorded under [subsection]; and*

g. *Disposal at individual's request & by service provider*

Our comments regarding disposal at an individual's request and by service provider are focused on three aspects; to prevent spoilation, confirmation of spoilation and clear recourse.

Prevent spoliation

As currently drafted, the requirement to dispose of an individual's personal information could be interpreted as a statutory justification for spoliation. We recommend that the language in this provision is modified to ensure that information that may be required for use in a legal proceeding is not disposed of as follows:

Recommended change

(1)(c) the personal information has been disclosed in the course of a legal proceeding, ***it is reasonably foreseeable that the personal information will be relevant to a legal proceeding,*** *or the personal information is otherwise available to a party of a legal proceeding; or*

Confirmation of disposal

Unless particular requirements are prescribed in the regulations, the proposed provision does not impose an obligation upon the organization receiving a given disposal request to provide confirmation to the individual upon disposal. As the White Paper suggests, we agree that the legislation should address in more detail a requirement for an organization to provide confirmation of the disposal to the individual. If the organization is required to provide confirmation of disposal by its service providers, this should be clearly stipulated in the legislation.

In imposing such an obligation on organizations and their service providers, the obligation should be sensitive and proportionate to such factors as the nature and sensitivity of the personal information, the capacity of the organization to comply, and the risk of harm to the individual where the organization fails to, or imperfectly complies with its obligation under this provision.

Clear recourse

The legislation should also include clear information on the recourse available to challenge an organization's denial of a disposal request.

h. ***Right to be Forgotten***

The White Paper raises the possibility of enshrining a "right to be forgotten" by requiring organizations to de-index search results containing personal information about an individual, posted by others. We recognize that enshrining such a right will necessarily need to be balanced against other fundamental rights, including rights to freedom of expression and access to information, and the need to preserve evidence. Our comments are focused on specificity of application and a robust dispute resolution process.

Specificity of application

The fundamentally networked nature of the internet and personal information in a data driven economy makes it challenging to define the organizations that are engaged in an activity that should bring them within the obligations imposed by a right to be forgotten.

Legislation should use a narrow and specific definition of the organizations captured by an obligation to respond to a de-indexing request. A precise definition of the nature of the activity that covered organizations are engaged in will allow them to anticipate the legal obligations of such enterprise.

Robust dispute resolution

Without speaking to the legislative language specifically, it is important to emphasize that a robust mechanism for resolution of disputes is essential to the meaningful realization of this right. There is potential that such requests will be highly contentious given the nature of such a request and the collision of a right to be forgotten with other competing rights. The mechanism for making and disputing de-indexing requests should be specific and provide the parties with certainty to the extent possible.

For example, if organizations captured by the obligations imposed by a right to be forgotten will be responsible for determining such competing interests in the first instance, it will be essential for the legislative scheme to establish a robust mechanism for appealing such decisions.

Such a process for challenging the competing rights engaged by a right to be forgotten will require an efficient adjudicative process for resolving such disputes, that is economical for both the individual and organizations obliged to respond.

B. Enhancing Consent and Other Lawful Uses of Personal Information

The White Paper proposes to address consent fatigue for users of products and services in the digital economy by not relying on consent in certain circumstances. Our comments are focused on the language of 'business activities'.

Business activities

The proposed legislative language permits the collection, use and disclosure of personal information for described business activities where:

- a reasonable person expects such collection or use for the business activity, and
- the information is not collected or used for the purpose of influencing the individual's behaviour.

The language describing the business activities in the subsequent subsections as drafted does not appear to limit the scope of "business activities" to commercial enterprises in the pursuit of profit. It would be helpful to clarify the intent of the language, with respect to whether the broad scope of the described business activities would extend to cover the activities of non-profit and political organizations.

C. Data Transparency for Ontarians

As we have emphasized above, and as the White Paper acknowledges, transparency about data practices is of central importance to enabling Ontarians to exercise meaningful consent over the collection, use and disclosure of their personal information.

We agree that the requirement for organizations to implement a privacy management program should be balanced by taking into account to the size of the organization, the sensitivity of the personal information, and the organization's purposes.

D. Fair, Proportionate and Supportive Regulatory Regime

The White Paper suggests providing the Ontario IPC the powers to issue binding orders if the IPC determines the organization is found to be in non-compliance with the law (including the power to compel an organization to take any positive action, or refrain from an action) and to apply administrative monetary penalties. These enforcement powers are extensive and can have significant ramifications for any organization subject to them.

These extensive enforcement powers should be met with sufficient safeguards to ensure fairness in both procedure and result.

Procedure

With respect to procedure, it is recommended that Ontario apply procedural fairness best practices, including as described in administrative law jurisprudence. Adjudicative and prosecutorial streams within the IPC should be kept separate.

Result

With respect to ensuring fair results, organizations should not be subject to a narrowed right of appeal. Organizations should have the right to appeal questions of fact, law and mixed fact and law. The appellate standard of review (correctness for questions of law, palpable and overriding error for questions of fact and mixed fact and law) should be applied to this right of appeal. This approach ensures a twofold result. First, IPC decisions receive deference. Second, organizations are granted a greater scope of appealing decisions if a determination of fact or mixed fact and law made in an abbreviated fact-finding process has unfairly impacted their matter.

Given that privacy law remains a dynamic and under-developed area of law, the OBA recommends against insulating questions of mixed fact and law from judicial scrutiny and jurisprudential development. The following modification to the right of appeal is therefore recommended:

> *Recommended change:*
>
> *(1) A complainant or organization that is affected by a Compliance order may appeal it to the Divisional Court on question**s** of **fact,** law **or mixed fact and law** in accordance with the rules of court by filing a notice of appeal within 30 days after the complainant or organization receives the order. **The standard of review for an appeal is correctness for questions of law and palpable and overriding error for questions of fact or questions of mixed fact and law.***

While the second sentence maybe redundant in light of recent jurisprudence, specifying the applicable standard of review assists practitioners and complainants by adding clarity and certainty to the appeal process.

IV. Conclusion

In closing, we believe that our members' knowledge of the applicable legal principles and their thorough understanding of this area will help improve the approach to Modernizing Privacy in Ontario through amendments to the rights-based approach to privacy, enhancing consent and other lawful uses of information, data transparency for Ontarians, and a fair, proportionate and supportive regulatory framework.

Thank you for taking the time to review the submission. We hope you find the feedback from the Ontario Bar Association helpful and informative in drafting legislation to enhance privacy in the province, and we invite the Government to engage in further direct dialogue with our Privacy & Access to Information section executive, as you move forward with drafting legislation to modernize privacy law for Ontarians.