HALCO
HIV & AIDS Legal Clinic Ontario

Response to the Ministry of Government and Consumer Services: White Paper – Modernizing Privacy in Ontario

September 3, 2021

I. INTRODUCTION AND OVERVIEW OF SUBMISSIONS

The HIV & AIDS Legal Clinic Ontario ("HALCO") makes this submission in response to the Ministry of Government and Consumer Services' (the "Ministry") White Paper – Modernizing Privacy in Ontario. As described in HALCO's October 2020 submission to the Ministry on Reforming Privacy in Ontario's Private Sector (attached as Appendix A), HALCO shares the Ministry's view that robust and effective privacy protections for Ontarians are critical to a modern digital and data strategy.

In this submission, HALCO will address three discussion questions raised by the Ministry's White Paper that are most relevant to our client communities. This submission will propose that the draft legislation should include:

1) Data rights to erasure that apply to all information an organisation holds about an individual, and a right to online "source takedown" as a remedy in certain circumstances.
2) Enumeration of categories of information that should be considered "sensitive", including health information.
3) An expansion of powers for Ontario's Information and Privacy Commissioner ("IPC") that includes the ability to award meaningful compensation for privacy breaches.

HALCO, founded in 1995, is a community legal clinic serving the legal needs of low-income people in Ontario who are living with HIV. It is the only such organisation in Canada. Since 2001, HALCO has responded to more than 1,600 enquiries about privacy-related issues and more than 2,900 human rights issues. Privacy and human rights issues permeate all aspects of HALCO's work, whether in relation to direct client services (e.g., privacy complaints and torts, human rights complaints), public legal education or law reform.

HALCO's October 2020 submissions detailed how HIV-related stigma remains shockingly pervasive in Ontario and across Canada. People living with HIV continue to face discrimination, social exclusion, and even violence in all aspects of their lives when their HIV status is disclosed without their consent. For these reasons, it is vital that Ontarians living with HIV can both make use of robust and accessible privacy protections to both prevent breaches in relation to their HIV status and access adequate and responsive remedies when privacy breaches do occur.

HALCO reaffirms all the recommendations in its October 2020 submission.[1] HALCO also welcomes the Ministry's rights-based approach to privacy in its White Paper, and its adoption of a fundamental right to privacy. Such an approach is necessary to protect the dignity and autonomy of Ontarians.

[1] See Appendix A, HALCO, "Submission to the Ministry of Government and Consumer Services: Public Consultation – Reforming Privacy in Ontario's Private Sector" (October 2020).

II. RESPONSE TO DISCUSSION QUESTIONS

1. How far should the data rights of erasure and mobility extend? Should they include all information an organization has about an individual, or only the information the individual provided?

Response

Data rights of erasure, as described in the White Paper, should include all information an organisation has about an individual, and should not be limited to the information the individual provided.

The White Paper's inclusion of a "right to be forgotten" through "de-indexing" provisions is a highly beneficial but incomplete means to close the remedial gap that exists when an individual's privacy is wrongfully breached. The draft legislation should include "source takedown" provisions to fully close that remedial gap.

Right of erasure should include all data an organisation holds about an individual

Data rights of erasure, as described in the White Paper, should include all information an organisation holds about an individual, and should not be limited to the information the individual provided. The right to erasure assigns responsibility to organisations to find solutions for problems that the organisation is responsible for creating or enabling.[2] An interpretation of the right to erasure that is limited to the information that an individual *provides* would leave a remedial gap and does not reflect the reality of modern information sharing and processing.

In an example from HALCO's practice, third party social service organisations often support tenants with disabilities in asking the tenant's landlord for human rights accommodations. In doing so, the third party may provide information about a tenant's disability to the landlord. As the landlord did not receive that information directly from their tenant, they would have no obligation to dispose of that information, even at the request of the individual to whom the information pertains. This leaves the tenant without an effective means of protecting their privacy and maintaining control over their personal information. In other situations, a third party may share disability-related information about an individual with their landlord without the individual's consent. In either situation, an individual should have the right to ask a landlord to dispose of all of their disability-related personal information, subject to exceptions to be outlined in the draft legislation.

Further, the purpose of the right to erasure would be undermined if organisations could innovate business models to escape its application—for example, by collecting information indirectly.[3] As the Office of the Privacy Commissioner of Canada ("OPC")

[2] Andrea Slane, "Search Engines and the Right to be Forgotten: Squaring the Remedy with Canadian Values on Personal Information Flow" (2018) 55 Osgoode Hall LJ (QL) at para 38 [Slane].
[3] See *Reference re Subsection 18.3(1) of the Federal Courts Act,* 2021 FC 723 at para 28.

noted, “The business model of data brokers is opaque and creates risks for privacy […] [They] should not be granted greater freedom in the use of data without consent.”[4] In contrast, a right to erasure that includes all the information that an organisation has about an individual, regardless of its source, is forward-looking because it creates incentives for organisations to consider privacy interests in all aspects of their data management.

Source takedown is needed to close the remedial gap in online privacy breaches

As described further below, HALCO recommends the adoption of the mechanisms of “source takedown” and “de-indexing” to implement a right to be forgotten in the online context. The OPC defines these terms as follows:

> De-indexing is the process by which a webpage, image or other online resource is removed from search engine results when an individual’s name is entered as the search term. Source takedown refers to the removal of the content from the internet.[5]

Although HALCO supports the White Paper’s inclusion of a “right to be forgotten” through “de-indexing” provisions, this is an incomplete means to close the remedial gap that exists when an individual’s privacy is wrongfully breached. The draft legislation should include “source takedown” provisions to fully close that remedial gap.

As discussed in HALCO’s October 2020 submission, people living with HIV may face discrimination when their HIV status is disclosed online. Even if a person living with HIV can prove in a human rights application that, for example, their employer discriminated against them after uncovering their HIV status online, the human rights tribunal would have no jurisdiction to order the takedown of materials or de-indexing of search results related to the discrimination.[6]

With the advent of the internet, this leaves these individuals with an incomplete remedy. The risk of harm extends beyond actual future discrimination. For example, the psychological consequence of feeling like ‘everyone knows’ about sensitive personal information is a well-documental barrier to overcoming a traumatic experience.[7] With this in mind, source takedown is the *only* means to eliminate the risk of further discrimination by way of the publically available and wrongfully disclosed information.

Source takedown is a necessary component of a right to erasure as it relates to content the individual has provided to an organisation. PIPEDA provides individuals the right to

---

[4] See Office of the Privacy Commissioner of Canada, *Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020* (2021) [OPC Digital Charter].

[5] Office of the Privacy Commissioner of Canada, *Draft OPC Position on Online Reputation*, (2018) [Online Reputation].

[6] This is particularly important in light of the Federal Court’s observation in *Reference re Subsection 18.3(1) of the Federal Courts Act*, 2021 FC 723 at para 39 that “[privacy legislation] is quasi-constitutional legislation because its focus is on ensuring that individuals can control their person information *which is intimately connected to their individual autonomy, dignity and privacy”* [emphasis added].

[7] See Slane, *supra* note 2 at para 43.

withdraw consent, and requires that personal information that is no longer needed be destroyed, erased or made anonymous. According to the OPC, "Taken together, this implies that individuals should have the ability to remove information that they have posted online."[8]

More broadly, the availability of source takedown and de-indexing should be guided by a number of factors, including:

- Whether the person concerned is a public figure;
- Whether the information is up to date and accurate;
- Whether the information involved is sensitive, as defined by the legislation;
- Whether the data could have a disproportionately negative impact on the person; and
- Whether the data puts the person at risk.

HALCO also recommends that the Ministry set out a clear process for entities to follow in response to source takedown or de-indexing requests, and that an independent review or appeal body, such as the IPC, be available to review denials of such requests.

Finally, if an independent review mechanism is created, the process should also provide for requests that the information at issue be temporarily suspended from public use/access during the review process, where certain factors are met (e.g., where there is a risk of harm in the interim period).

2. How should the concept of personal information, and "sensitive" personal information, be defined in law?

Response

Draft legislation should enumerate categories of sensitive personal information, including health information, rather than relying on contextual variables to evaluate information sensitivity. This approach would better protect against privacy breaches and provide clarity for individuals and organisations.

Personal health information should be included in the definition of "sensitive" personal information

Robust protections for individuals' sensitive personal information are well established. All Canadian regimes dealing with information flow—from the *Charter* to PIPEDA to access to information legislation—consider access to personal information, and

[8] *Online Reputation*, *supra* note 5.

especially sensitive personal information, to be justifiably subject to greater limitations than access to other forms of information.[9] The unique character of personal health information is already recognized in Ontario as "one of the most sensitive types of personal information."[10]

Information is generally considered sensitive when there is a high likelihood that its public release would cause harm to the individual to whom it pertains.[11] Information about a person's HIV status, for example, is extremely sensitive because it remains highly stigmatized (see Appendix A for more information regarding stigma related to HIV status).[12] The Supreme Court of Canada has recently recognized that information related to a stigmatized medical condition is an example of sensitive personal information that requires special protection because its disclosure can negatively impact a person's dignity.[13]

Draft legislation should include categories of information that are presumptively "sensitive"

Other privacy regimes have specified that certain categories of personal information, including health information, are particularly sensitive.[14] For example, Article 9 of the General Data Protection Regulation ("GDPR") provides special categories of personal data that attract particular protections, including health data or data concerning a natural person's sex life of sexual orientation.[15]

In determining the categories of information that should be included in the definition of "sensitive" personal information, HALCO recommends that the Ministry consider the grounds protected by the Ontario *Human Rights* Code (the "*Code*").[16] Where a category of information is related to a ground protected under the *Code*, disclosure of that information may be more likely to cause harm to the individual to whom the information pertains. For example, HIV is considered a disability under the *Code* and people living with HIV may experience discrimination on the basis of disability if their HIV status is disclosed. It is appropriate to consider the *Code* and human rights principles given the (i) quasi-constitutional nature (i.e., fundamental and paramount) of human rights legislation; and (ii) importance of privacy as an element of human rights.

---

[9] See Slane, *supra* note 2 at para 49.
[10] Office of the Information and Privacy Commissioner of Ontario, *A Guide to the Personal Health Information Protection Act,* (2004) at 1.
[11] See Slane, *supra* note 2; Paul Ohm, "Sensitive Information" (2015) 88:5 S Cal L Rev 1125 at 1133; See also Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent,* (2018).
[12] See Canadian HIV/AIDS Legal Network, Canadian Public Health Association, *Reducing Stigma and Discrimination Through the Protection of Privacy and Confidentiality,* (2017).
[13] *Sherman Estate v. Donovan*, 2021 SCC 25 at para 77.
[14] See, e.g., *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5, Schedule 1, s 4.3.4.
[15] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.
[16] *Human Rights Code*, RSO 1990, c H.19.

The grounds listed in the *Code* are necessary but insufficient to inform the categories of sensitive information to be included in the draft legislation. The Ministry should broadly consider the likelihood of harm resulting from public release of personal information, definitions from other jurisdictions, and other appropriate factors in determining the list of categories to be enumerated in the draft legislation.

Relying on context to assess sensitivity creates uncertainty

As the OPC observes in the context of PIPEDA, there is no "bright line" separation of what is, and is not, sensitive information. Categories of information such as health or financial information are generally considered sensitive because of specific risks to individuals when said information is collected, used or disclosed.[17] Under a contextual approach, for example, information that is generally considered sensitive may become less so depending on whether other related information is publically available.[18]

This contextual approaches creates indeterminacy for individuals and organisations because the assessment of information's sensitivity is left to the sole discretion of the organisation processing the information.[19] For example, policy may vary from one organisation to the next with respect to the same type of information—resulting in the same information being handled differently. If personal health information becomes publicly available through an initial breach, a contextual analysis may find that information to no longer be sensitive, effectively penalizing individuals for prior data breaches.

3. Would the ability for the IPC to issue orders requiring organizations to offer assistance or compensate individuals be an effective tool to give individuals quicker resolutions to issues?

Response

Yes, an expansion of the IPC's powers to include the ability to order assistance or compensation would improve access to justice by streamlining the enforcement and compensation mechanisms for breaches of privacy. Legislators should avoid a two-stage compensatory framework because it will likely exacerbate access to justice challenges in Ontario.

[17] See Office of the Privacy Commissioner of Canada, *Guidelines for obtaining meaningful consent,* (2018) [Meaningful Consent]; See also *Royal Bank of Canada v Trang*, 2016 SCC 50 at para 36.
[18] See Meaningful Consent, *ibid*.
[19] See *Reference re Subsection 18.3(1) of the Federal Courts Act,* 2021 FC 723 at para 59 where the Federal Court took note of the fact that Google had no commercial motivation to de-index or de-list information from its search engine. Likewise, organisations may have no commercial interest in developing robust policies to protect sensitive personal information in light of any ambiguity.

HALCO agrees with the Ministry that an independent oversight body is needed to promote good privacy practices and to enforce the law, when necessary. The new legislation should expand the IPC's powers to allow it to fill this role.

To ensure all Ontarians can access fair compensation for breaches of their privacy, legislators should consider giving the IPC the power to make meaningful compensatory orders. Although administrative penalties and statutory offences are important tools to enforce privacy legislation, they provide no remedy to individuals who have suffered a breach of their privacy.

While PIPEDA and substantially similar privacy regimes allow for parties to apply to civil court for enforcement and compensation following a proven privacy breach,[20] court proceedings can be prohibitively lengthy, overly formal and costly. This type of two-stage compensation scheme is likely to create barriers to access to justice, which the Supreme Court of Canada has described as "the greatest challenge to the rule of law in Canada today."[21]

Legal actions involving breaches of privacy can be particularly complex. As an example, where a civil privacy breach claim requires the complainant to reveal highly sensitive information—as is nearly always the case for HALCO's clients when a privacy breach involved disclosure of their HIV status—the complainant may require a confidentiality order from the court to protect their identity. As a result, even where the IPC has found a breach of privacy, Ontarians who do not have the resources or expertise to navigate the complex confidentiality order process or cannot otherwise participate in court proceedings may be unable or unwilling to access fair compensation.

Where the IPC has investigated and found a breach of privacy, it would be expedient and efficient for the IPC to order compensation. This provision could take a similar form as recommendation 34 of the Submission of the OPC of Canada on Bill C-11, which would permit the IPC to order an organisation to "take measures which allow individuals to be compensated for damages suffered, financial or otherwise, stemming from a breach or violation of security safeguards required by law."[22]

HALCO recommends that individuals need not be required to prove financial damages in order to be granted compensation. The damage associated with a privacy breach can be difficult to quantify. Ontario courts have decided that it is unnecessary to prove pecuniary loss in order to receive an award of damages for a breach of privacy at common law.[23] Similar principles should apply to statutory compensation for breach of privacy. Damages should be material to have a meaningful deterrent effect on privacy breaches, and not merely create a license fee for organisations that misuse individuals' private information.

---

[20] *Personal Information Protection and Electronic Documents Act*, SC 2000, c. 5; *Personal Information Protection Act*, SA 2003, c P-6.5; *Personal Information Protection Act*, SBC 2003, c 63; *An Act respecting the protection of personal information in the private sector*, CQLR, c P-39.1; *Personal Health Information Protection Act*, SO 2004, c 3.

[21] *Hryniak v. Mauldin*, 2014 SCC 7 at para 1.

[22] OPC Digital Charter, *supra* note 4.

[23] *Jones v. Tsige*, 2012 ONCA 32 at para 74.

III. NEXT STEPS

HALCO is keen to continue this dialogue and to support the development of leading, strong, and effective privacy and data protection that protects the dignity and autonomy of Ontarians living with HIV. To talk further about how a modern privacy law could be designed to meaningfully protect Ontarians' sensitive personal information, please contact HALCO.

Ryan Peck
Executive Director
HIV & AIDS Legal Clinic Ontario
peckr@lao.on.ca

Robin Nobleman
Staff Lawyer
HIV & AIDS Legal Clinic Ontario
noblemar@lao.on.ca

Adam Kouri
Donner Fellow/Law Student
HIV & AIDS Legal Clinic Ontario