Canadian Privacy Law Review

VOLUME 17, NUMBER 8 Cited as (2020), 17 C.P.L.R. JULY 2020

• HOW TO DEVELOP A PRIVACY-ENRICHED DATA RETENTION POLICY •

Theo C. Ling, Lawyer, Jonathan Tam, Lawyer, Baker & McKenzie LLP

Theo C. Ling

Jonathan Tam

The retention limitation principle under the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) is easy to state: "Personal information that is no longer required to fulfil the identified purposes should be destroyed, erased, or made anonymous."[1] The main thrust of this principle is intuitive: Retaining personal information about an individual for longer than necessary makes it more likely that the information will be subject to unauthorized or accidental access, use or disclosure. It could also violate the terms of the individual's consent and reasonable expectations of privacy.

Many privacy regimes around the world articulate some variation of the retention limitation principle, including the EU *General Data Protection Regulation*,[2] the Australian Privacy Principles,[3] and the Singapore *Personal Data Protection Act 2012*.[4] Some privacy laws and authorities even impose a defined maximum retention period on certain types of personal information. For example, Illinois' *Biometric Information Privacy Act* requires private entities to destroy biometric identifiers and information when the initial purpose for collecting the information has been satisfied, or within 3 years of the individual's last interaction with the entity, whichever occurs first. As another example, France's supervisory authority has issued guidance stating that an employer may generally only keep records of the reasons for employees' absence from the workplace for a maximum of 5 years.[5]

Although the retention limitation principle is easy to state, it is often difficult to comply with in practice. Whether an organization has a legitimate legal or business reason to continue to retain personal information is usually a context-specific inquiry that depends, among other things, on the organization's

• In This Issue •

HOW TO DEVELOP A PRIVACY-ENRICHED DATA RETENTION POLICY
Theo C. Ling and Jonathan Tam 77

PRIVACY IN A PANDEMIC: PRIVACY LAWS MATTER
Wendy J. Wagner, Sarah Boucaud and Romina Hassanzadeh 85

LexisNexis®

CANADIAN PRIVACY LAW REVIEW

Canadian Privacy Law Review is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $355.00 per year (print or PDF)
$545.00 per year (print & PDF)

Please address all editorial inquiries to:

General Editor
Professor Michael A. Geist
Canada Research Chair in Internet and E-Commerce Law
University of Ottawa, Faculty of Law
E-mail: mgeist@uottawa.ca

LexisNexis Canada Inc.
Tel. (905) 479-2665
Fax (905) 479-2826
E-mail: cplr@lexisnexis.ca
Web site: www.lexisnexis.ca

relationship with the individual, privacy notices, scope of intended use of the personal information, and internal operations, and the laws that apply to the organization.

Still, organizations must find a way to adhere to the retention limitation principle. The Office of the Privacy Commissioner (OPC) has taken enforcement action against organizations that kept personal information for too long, including a social networking site that archived users' personal information indefinitely.[6] Outside of Canada, a German authority fined a real estate company €14.5 million in October 2019 for storing personal data about tenants longer than required,[7] and the Danish authority proposed fining a taxi company DKK 1.2 million in March 2019 for failing to delete personal data about customers after it was no longer required.[8]

This article outlines an approach that an organization can take to determine and document how long to retain personal information collected across its operations.

THE END GOAL

It is helpful to consider the desired end goal. PIPEDA requires organizations to *develop guidelines and implement procedures* to govern the destruction of personal information.[9] PIPEDA establishes that an organization's retention guidelines should include minimum and maximum retention periods. In particular, an organization must retain personal information long enough to satisfy legal requirements and allow an individual to access the information if the organization uses it to make a decision about the individual, but the organization must not keep personal information longer than required to fulfil the identified purposes for which it was collected.[10] To address these requirements, a reasonable end goal is for an organization to implement a data retention policy that includes the following core components.

First, the data retention policy would list and describe all of the types of records containing personal information that the organization receives or generates. Organizations typically define such *record types*

based on their function or associated business activity (*e.g.*, customer invoices) rather than their format (*e.g.*, email) because how long a particular record should be retained depends more on its purpose than its format. For each record type listed, the policy would set forth a *retention period* for which a record that falls within that record type is to be retained. The retention period would take into account applicable legal requirements followed by relevant business considerations. If the organization identifies a record type that includes both personal information and non-personal information and wishes to keep the non-personal information in the records for longer than the retention limitation principle allows it to keep the personal information, it might designate a *maximum retention period* that applies specifically to the personal information in the record. For each record type listed, the policy would also set forth a *retention event* that triggers the commencement of the retention period. This information might take the following form:

Record Type	Description	Retention Event	Retention Period
A name for a specific type of record containing personal information.	A description to help the reader understand what the record type includes and perhaps what it does not include.	A description of an event that causes the retention period to begin to run.	The period for which the organization will retain such records (*e.g.*, "X years"). The retention period may also include a maximum retention period that applies to the personal information in the record (*e.g.*, "MAX Y years for personal information").

Second, the data retention policy would guide personnel on when to deviate from the designated retention periods, such as where the organization anticipates that it might enter into a legal dispute with the data subject, receives a warrant or subpoena regarding certain information, or no longer has an individual's consent to continue retaining their personal information.

Third, the organization would have taken steps to implement the data retention policy, including by dedicating resources to its administration and enforcement and providing regular training to all relevant personnel. To operationalize the policy, the organization might also program the data retention policy into its own systems of record,[11] if it has them, so that its computer systems automatically delete records, or remind personnel to delete records, once their corresponding retention period elapses.

To achieve the end goal described above, an organization may consider taking the following steps.

STEP #1: PREPARE A "MAP" OR "INVENTORY" OF PERSONAL INFORMATION COLLECTED

The first step is to understand and document all of the material facts surrounding the organization's collection, use and disclosure of personal information. Privacy professionals often refer to this type of exercise as preparing a "data map" or "data inventory" and it is beneficial to developing not only a compliant records retention policy but also an effective privacy management program as a whole. The key details to record from a retention limitation perspective are:

(1) *What types of personal information does the organization collect?*
(2) *In what context does the organization collect each type of personal information*?
(3) *For what purposes does the organization use each type of personal information?*
(4) *In what applications, systems and locations does the organization store the personal information?*

Regarding question (2) above, there are at least two types of contexts that are useful to take into account. First, the organization may consider whether it uses the personal information for its own purposes, or whether it only uses the personal information on behalf and subject to the instructions of another organization.[12] In general, if an organization determines its own purposes of using personal information, it may retain the personal information for as long as reasonably necessary to fulfil the purposes that the data subject consented to.[13] By contrast, if an organization uses certain

personal information only on behalf and subject to the instructions of another organization, the organization will typically have no legitimate reason to continue retaining that personal information once its relationship with the other organization ends. For example, a company that provides a cloud hosting service to a corporate customer generally has no reason to retain personal information that the customer uploaded to the company's cloud environment after their hosting arrangement ends because the company only needed that personal information to make it available to the customer for the term of the arrangement.

Second, the organization may distinguish among the types of individuals about whom it collects personal information for its own purposes. For example, an organization typically uses for its own purposes personal information that it receives from its personnel (*e.g.*, employees, individual contractors, students and interns) and job candidates, the individual representatives of legal entities with whom it has business relationships (*e.g.*, customers and vendors), and any individuals to whom it provides products and services (*e.g.*, consumers). An organization typically uses personal information about these types of data subjects for different purposes, and distinguishing them from one another is useful for step #2 below.

An organization would likely have to involve multiple stakeholders in gathering the information necessary to produce a data map, including human resources representatives, managers, product engineers, and sales and procurement personnel. Anorganization may consider leveraging its systems of record to prepare its data map if it has one. Various businesses offer software tools that assist organizations in generating data maps.

STEP #2: CATALOGUE THE TYPES OF RECORDS CONTAINING PERSONAL INFORMATION THAT THE ORGANIZATION COLLECTS AND GENERATES

The result of Step #1 should yield a data map that identifies each type of personal information that the organization collects in a particular context, the purposes for which the organization uses that personal information, and the locations in which it stores that information. The organization might then consider what record types it collects and generates that match certain groups of personal information that it collects. For example, a federal work analyzing the types of personal information that it uses in the human resources context might find that it uses certain personal information about its employees for tax compliance purposes. The federal work could define a record type for employee tax records and list in the description of the record type examples of relevant tax forms that would fall within it (*e.g.*, TD1s and T2200s).

In defining different record types, an organization may find it helpful to distinguish between "records" and "copies of records". The organization might consider a "record" to be the definitive instantiation of a particular piece of information that the organization holds, and a "copy of a record" to be a transitory reproduction of a record meant for a particular use (*e.g.*, a printout for a meeting) and which should be destroyed once that use is complete. The organization should focus at this stage on identifying the records it creates and generates and grouping them together into record types that serve the same function or relate to the same associated business activity.

Every time the organization identifies and defines a new record type, it should highlight the purpose or purposes in the data map that match that record type, with the goal of highlighting every purpose in the data map by the end of the exercise. To the extent possible, the organization should try to highlight each purpose only once to avoid a particular record falling into multiple record types. But an organization can address the issue of overlapping record types by tweaking their definitions so that they do not overlap, such as by defining one of the record types to expressly exclude records that should fall into the other record type. Some record types may be narrow and some may be broad—there is no one-size-fits-all solution to this step. As long as the organization understands and finds the catalogue and definitions of record types useful, it will have made progress.

STEP #3: ESTABLISH RETENTION EVENTS AND RETENTION PERIODS FOR DIFFERENT TYPES OF RECORDS CONTAINING PERSONAL INFORMATION

Once an organization has compiled and organized a list of all of the record types containing personal information that it collects and generates, and the list reflects all of the purposes for which the organization uses personal information, the organization must determine appropriate retention events and retention periods for each record type. Doing so requires consideration of the following key considerations:

- *What laws apply to the organization's collection, use and disclosure of personal information?* This threshold question underpins many of the considerations further down this list and may depend on the types of services it offers, the locations of data subjects, the locations of data storage and processing, and the degree to which the organization targets its offerings at certain locations.
- *Is the organization legally required to retain a particular type of record containing personal information for a minimum period?* Some laws require organizations to retain certain types of records containing personal information for a prescribed period. For example, the *Breach of Security Safeguards Regulations* under PIPEDA require an organization to maintain a record of every breach of security safeguard for 24 months after the day on which the organization determines that the breach has occurred. Such records must contain any information that enables the Office of the Privacy Commissioner to verify the organization's compliance with the breach reporting requirements under PIPEDA.[14] Since PIPEDA's breach reporting requirements require an organization to notify data subjects of breaches in certain circumstances, these records generally contain some personal information, such as the contents of a breach notice directed at an affected data subject. An organization must ensure that it keeps such records for at least 24 months.
- *Is there a legal obligation to delete certain personal information within a prescribed period?* On rarer occasions, laws and regulatory agencies may impose affirmative obligations on organizations to delete certain information within a prescribed period, such as the requirements mentioned at the beginning of this article. An organization's data retention policy should reflect any such applicable requirements.
- *Is the personal information necessary to defend against possible future legal claims?* If so, an organization could justify setting the applicable minimum retention period so that it aligns with the limitation period past which such a legal claim could no longer arise.
- *How long does the organization need to keep personal information to achieve the legally permissible business purposes for which it collected the information?* An organization should be able to justify why it is legally permitted to use personal information for each of its desired business purposes and how long it needs to keep personal information to achieve those purposes. The organization should consider all relevant legal considerations in answering these questions. For example, PIPEDA generally requires organizations to obtain individuals' informed consent before collecting, using and disclosing their personal information for identified purposes.[15] PIPEDA acknowledges that consent takes many forms, and the individual's reasonable expectations and the sensitivity of the personal information at issue are relevant to the form of consent the organization must obtain.[16] If an individual does not consent or reasonably expect an organization to continue to retain and use their personal information, the organization is likely required to delete the personal information.
- *When should the retention period start to run?* The retention event, or the time when the relevant retention period starts to run, may be set forth in the applicable law imposing the retention requirement. In situations where there is no clear legal guidance, the retention limitation principle

suggests that organizations should implement processes to avoid retaining personal information indefinitely. For example, if an individual has an online account with an organization, the organization could consider defining the retention event as the time at which the individual deactivates their account. But there is the possibility that some individuals do not deactivate their account even though they never plan to use the organization's services again. The organization may therefore wish to consider sending a communication to an accountholder if they have not used their account for a long period without deactivating it, stating that the organization will deactivate their account if they do not respond or resume activity on the account within a reasonable amount of time, and proceeding accordingly.

STEP #4: DEVELOP GUIDANCE THAT INCLUDES NECESSARY EXCEPTIONS TO THE RETENTION REQUIREMENTS

An organization that has completed steps 1-3 will have produced a matrix that includes the information shown in the table in the "End Goal" section above. The organization may find it helpful to include citations to applicable laws that caused the organization to establish the specified retention periods, and any exceptions to the retention periods based on laws in specific jurisdictions. If it wishes, an organization can incorporate these elements in a general policy that applies to all of its records, not just ones that contain personal information. This matrix forms the core of the organization's data retention policy.

An organization could subsequently include guidance in the data retention policy describing its approach to situations where the rules in the table may not apply. In particular, an organization may wish to include guidance relating to the following scenarios:

- *Retaining sensitive personal information:* Whether personal information is sensitive depends on the context,[17] but if the unauthorized access, use or disclosure of certain personal information would likely result in a real risk of significant harm to an individual, the personal information is likely to be more sensitive. There may therefore be increased legal risks associated with retaining the personal information for a long period. An organization that holds sensitive personal information may wish to subject the information to especially short maximum retention periods to address these risks, where feasible.
- *Using personal information to make decisions about individuals:* PIPEDA states that personal information that has been used to make a decision about an individual must be retained long enough to allow the individual access to the information after the decision has been made.[18] An organization can address this requirement by defining the retention events for its record types in a way that reduces the likelihood that it would use such records to make decisions about individuals after the retention event has transpired. Even so, an organization should be aware that it may need to keep records for an additional period to address the above requirement.
- *Responding to legal process:* An organization may need to override its standard personal information retention practices where certain information could be relevant to a legal process, such as an investigation, subpoena, warrant, proceeding or summons. Failing to retain such information could result in risks of claims that the organization destroyed evidence relevant to a legal process. Organizations should therefore implement procedures whereby their legal departments or records managers may issue preservation orders, litigation holds or similar instruments to ensure the continued retention of the records referenced therein.
- *Responding to data subject requests:* An organization may be required to vary from its standard personal information retention practices on receipt of a request from an individual exercising their rights under applicable privacy laws. Under PIPEDA, an organization that collects, uses and discloses an individual's personal information on the basis of their consent

is required to give effect to an individual's withdrawal of consent at any time, subject to legal or contractual restrictions and reasonable notice.[19] In addition, an organization that receives a request from an individual to delete their personal information may be required to interpret the request as a withdrawal of the data subject's consent to continue retaining their personal information.[20] Some laws outside of Canada also give individuals the formal right to request the deletion of their personal information.[21]

- *Relying on statutory exceptions:* Some privacy laws outline exceptions whereby an organization may collect, use and disclose personal information in ways that the laws would otherwise prohibit. For example, PIPEDA permits organizations, in summary, to collect, use and disclose personal information about an individual without their knowledge or consent in situations where the organization reasonably suspects that they contravened or will contravene applicable laws.[22] The retention limitation principle suggests that an organization that relies on an exception to collect, use or disclose personal information about an individual in these types of situations should generally only retain personal information for as long as the relevant exception applies.

STEP #5: IMPLEMENT THE DATA RETENTION POLICY

After an organization has developed its data retention policy, it should take steps to implement and socialize the policy. For example, the organization should put in place procedures that ensure that the organization irreversibly deletes or de-identifies personal information once the applicable maximum retention period elapses.

The organization should also allocate responsibilities to stakeholders who can effectively administer and enforce the policy. Some organizations centralize records management functions within a particular team, while others require virtually all of their personnel to follow the data retention policy for the records that they individually collect and generate. In any case, the organization should ensure that all relevant personnel receive regular training based on their duties under the data retention policy.

An organization may also wish to establish a process to periodically review any records containing personal information that the organization has not clearly accounted for to determine whether it should continue to retain the personal information or can delete it. Implementing such a process decreases the likelihood that personal information gathered by the organization "falls through the cracks" and remains in the organization's systems indefinitely.

[***Theo C. Ling*** *is a lawyer at Baker & McKenzie LLP.*

Jonathan Tam *is a lawyer at Baker & Mckenzie LLP.*]

---

1 Section 4.5.3 of Schedule 1 of the *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5 (PIPEDA).

2 Regulation 2016/679, Article 5(e) ("Personal data shall be […] kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.").

3 *Privacy Act 1988*, No. 119, 1988, Australian Privacy Principle 11 ("If: a. an APP entity holds personal information about an individual; and b. the entity no longer needs the information for any purpose for which the information may be used or disclosed by the entity under this Schedule [and no exceptions apply]; the entity must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.").

4 *Personal Data Protection Act 2012*, No. 25, s. 25 ("An organisation shall cease to retain its documents containing personal data, or remove the means by which the personal data can be associated with particular individuals, as soon as it is reasonable to assume that — (a) the purpose for which that personal data was collected is no longer being served by retention of the personal data; and (b) retention is no longer necessary for legal or business purposes.").

5 Article 4, Deliberation n° 02-001 of January 8 2002 on the automated processing of personal information related to access to premises, schedules and catering,

Commission Nationale de l'Informatique et des Libertés.

6 PIPEDA Case Summary #2012-001, [2012] C.P.C.S.F. No. 1 at para. 61.

7 "Berlin Commissioner for Data Protection Imposes Fine on Real Estate Company", European Data Protection Board, November 5, 2019 news release, available at: https://edpb.europa.eu/news/national-news/2019/berlin-commissioner-data-protection-imposes-fine-real-estate-company_en.

8 The Danish Data Protection Agency proposes a DKK 1,2 million fine for Danish taxi company", European Data Protection Board, March 25, 2019, news release, available at: https://edpb.europa.eu/news/national-news/2019/danish-data-protection-agency-proposes-dkk-12-million-fine-danish-taxi_en.

9 Section 4.5.3 of Schedule 1 of PIPEDA.

10 Sections 4.5.2 and 4.5.3 of Schedule 1 of PIPEDA.

11 A "system of record" is an organization's authoritative listing of each piece of information that it holds or controls.

12 In some jurisdictions, the former situation describes that of a "controller", "business" or "covered entity" and the latter situation describes that of a "processor", "service provider" or "business associate" (*see*, respectively, the EU *General Data Protection Regulation*, the *California Consumer Privacy Act of 2018*, and the *Health Insurance Portability and Accountability Act of 1996*). Since PIPEDA does not make this distinction, this article will not use these terms.

13 *See* Section 4.2 of Schedule 1 of PIPEDA, which requires organizations to identify the purposes of collecting personal information at or before the time the information is collected and Section 4.3 of Schedule 1 of PIPEDA, which requires organizations generally to obtain individuals' informed consent before collecting, using and disclosing their personal information. Sections 4.5.3 and 4.5.4 of Schedule 1 of PIPEDA expressly tie the retention limitation principle to Sections 4.2 and 4.3 of Schedule 1 of PIPEDA.

14 *Breach of Security Safeguards Regulations*, SOR/2018-64, section 6.

15 *Ibid*.

16 *See* Sections 4.3.4 to 4.3.7 of Schedule 1 of PIPEDA. *See also Royal Bank of Canada v Tang*, 2016 SCC 50 and "Guidelines for obtaining meaningful consent", Office of the Privacy Commissioner of Canada, Office of the Information and Privacy Commissioner of Alberta, and Office of the Information and Commissioner for British Columbia, issued May 2018, available at: https://www.priv.gc.ca/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/.

17 Section 4.3.4 of Schedule 1 of PIPEDA.

18 Section 4.5.2 of Schedule 1 of PIPEDA.

19 Section 4.3.8 of Schedule 1 of PIPEDA.

20 PIPEDA Case Summary No. 2017-005, [2017] C.P.C.S.F. No. 4.

21 *See, e.g.*, Article 17 of the GDPR and Cal. Civ. Code § 1798.105(a).

22 Sections 7(1)(b) and (2)(a) of PIPEDA.

• PRIVACY IN A PANDEMIC: PRIVACY LAWS MATTER •

Wendy J. Wagner, Partner, Sarah Boucaud, Associate, Romina Hassanzadeh, Articling Student, Gowling WLG

Wendy J. Wagner

Sarah Boucaud

Romina Hassanzadeh

The COVID-19 pandemic has led to unprecedented social and economic responses across Canada and globally. Such responses implicate, but do not override, Canadian privacy laws. In fact, attention to privacy laws may be more important than ever in light of businesses shifting to online and remote delivery models and questions around public surveillance in light of this global occurrence.

Generally, Canadian privacy regulators are announcing that during a public health crisis, privacy laws continue to apply but should not present a barrier to appropriate information sharing due to available exemptions under those laws.[1] Where there is a declaration of public emergency, powers to collect, use, and disclose personal information may be expanded, within the bounds of the specific law in question. Privacy Commissioners across Canada have highlighted that the principles of necessity and proportionality should inform decisions made to address the current crisis.[2] Moreover, in these exceptional times, in which remote working has become the norm, organizations must be aware of their obligations to ensure that their employees use safe and secure remote access procedures and that the new working environment does not jeopardize the privacy and the security of personal information.

In this article, we will provide a summary of general trends across the guidance documents, notices and statements issued by Canadian Privacy and/or Access to Information Commissioners (**section A.**). This will be followed by an overview of the specific guidance issued by each of the federal, provincial, and territorial authorities overseeing privacy legislation in their respective jurisdictions (**section B.**). Not all Privacy Commissioners have addressed the same concerns. Some Privacy Commissioners have chosen to focus their comments on "access" provisions under access to information and privacy laws, including whether an extension of time to respond to an access to information request may be warranted. Others have also addressed privacy provisions within these laws and the specific disclosure exceptions that may be applicable in a public health crisis.

To date, the following Privacy and/or Access to Information Commissioners have made statements that relate to their operations, the protection of privacy, and/or the application of privacy and access to information laws in light of COVID-19:

1. **Canada**
2. **Alberta**
3. **British Columbia**
4. **Manitoba**
5. **New Brunswick**
6. **Newfoundland and Labrador**
7. **Northwest Territories**
8. **Nova Scotia**
9. **Nunavut**

10. Ontario
11. Québec
12. Saskatchewan
13. Yukon

We were unable to locate similar guidance applicable to organizations in Prince Edward Island.

Additionally, we have highlighted and consolidated the "tips", where offered by Privacy Commissioners, for persons engaged in remote work (see **Section C.**).

We also invite you to review articles prepared by our Birmingham Office in order to understand responses to "privacy in a pandemic" in other jurisdictions:

- COVID-19: Time to be even more cyber aware
- Processing Personal Data for COVID-19 Purposes

DISCLAIMER: We expect that there will consistently be new information available as the situation evolves. Please check the websites of Canada's Privacy Commissioners for the most updated information. This information does not include updates following the date of publication, unless otherwise advised.

A. GENERAL TRENDS

At a high level, businesses can expect that "privacy in a pandemic" may:

1. Require A Careful Analysis of the Various Laws in Play and what is Available Under Each:

Several layers of public and private sector privacy legislation at the federal, provincial and territorial levels may concurrently play a role during the management of a public health crisis, which involves close coordination between different levels of government.[3] As such, businesses must still be aware of the different privacy laws that apply to them and the ways in which such laws intersect. It is recommended that the specific laws that are applicable and any issued guidance and announcements from relevant privacy regulators be reviewed closely.

2. Engage the Use of Specific Legislative Authorizations for the Collection, Use and Disclosure of Personal Information without Consent:

Of the Privacy Commissioners that have issued COVID-19 related guidance materials or announcements, many have expressly indicated that existing privacy law frameworks already provide for legislative authorizations that allow organizations to respond to a public health crisis. These include the ability to disclose personal information without consent in specific, exceptional circumstances. Examples are outlined in greater detail below.

3. Require Justification and a Proportionate Response:

We note that the legislative authorizations referenced above do not apply to "regular" business operations, simply because a public health crisis exists. While businesses are faced with a variety of challenges in light of the pandemic, as well as shifting business practices as they move to an online delivery model, compliant privacy practices must remain a focus. As such, businesses should be wary of applying legislative authorizations that provide exemptions to the requirement to obtain consent for the collection, use and disclosure of personal information. Organizations relying on legislative authorizations or other exemptions to privacy laws must be able to communicate and justify the basis for doing so, and the specific authority that is being relied on in each case.[4]

4. Require Extensions of Time:

Privacy Commissioners have indicated that response times to privacy complaints and access to information requests may be affected by the pandemic. Organizations engaged in these processes may have to anticipate delays in receiving responses from institutions, but also may be able to benefit from extensions in circumstances where they are required to respond to privacy/access related requests. Further information is provided below.

5. Impact Privacy Practices Related to Employees:

Please see section C. for more information on best practices for employers.

B. GUIDANCE ISSUED BY CANADIAN PRIVACY COMMISSIONERS IN LIGHT OF COVID-19

The Office of the Privacy Commissioner of Canada ("OPC") and several provincial and territorial authorities that oversee compliance with privacy and access legislation in their respective jurisdictions have published their own statements in response to the pandemic. These statements emphasize that privacy laws continue to apply but should not be a barrier to appropriate information sharing within the bounds of the law, and in the case of access requests, may extend timelines for response.

1. Canada

a. Joint statement

On May 7, 2020, federal, provincial and territorial Privacy Commissioners issued a joint statement, outlining principles and inviting respective governments to use them to the extent they intend to use contract-tracing applications.

b. Office of the Privacy Commissioner of Canada

March 20, 2020 the OPC issued guidance to help organizations subject to federal privacy laws understand their privacy-related obligations during the COVID-19 pandemic. The OPC has urged that while privacy laws still apply, they are not necessarily a barrier to appropriate information sharing.

OPC is responsible for overseeing compliance with Canada's federal privacy legislation:

(1) *Personal Information Protection and Electronic Documents Act* ("PIPEDA"); and
(2) *Privacy Act*.

The OPC published a framework on April 17, 2020 to assess privacy-impactful initiatives in response to COVID-19. Its intention is to support government institutions faced with response efforts. It supports a flexible and contextual application of privacy laws and represents a more targeted approach to the OPC's expectations. The OPC has also announced "Tips for Canadians to consider when using videoconferencing services".

PIPEDA and the *Privacy Act* each contain provisions that allow for personal information to be used or disclosed for specific reasons that may be relevant in the time of a public health crisis. The following is an overview of relevant provisions from each statute.

i. PIPEDA

PIPEDA applies to private sector organizations that collect, use or disclose personal information in the course of commercial activities unless their activities are wholly within a province with substantially similar privacy laws (i.e. Alberta, British Columbia and Québec). PIPEDA also applies to the collection, use and disclosure of personal information in connection with the operations of a federal work, undertaking or business ("FWUBs") and for these organizations only, it also applies to employee personal information. FWUBs includes airlines, telecommunications providers and other federally regulated entities. It should be noted that organizations may be subject to both PIPEDA as well as other provincial privacy laws, depending on their specific operations (e.g. provincial private sector privacy laws and health sector privacy laws). These laws may further restrict or prohibit the disclosure of personal information/ personal health information without consent.

Pursuant to Principle 3 of PIPEDA, organizations are required to obtain meaningful consent prior to the collection, use or disclosure of an individual's personal information. There are exceptions, which may allow for the collection, use and disclosure of personal information without consent:

- **Timely Consent:** If the collection is clearly in the interests of the individual and the consent cannot be obtained in a timely way [paragraph 7(1)(a)].

- **Required by Law:** If the collection and use is for the purpose of making a disclosure required by law [paragraphs 7(1)(e), 7(2)(d) and 7(3)(i)].
- **Administrative Request:** If the disclosure is requested by a government institution under a lawful authority to obtain the information and the disclosure is for the purpose of enforcing or administering any law of Canada or a province [paragraphs 7(3)(c.1)(ii)-(iii)].
- **Lawful Authority to Prevent Contravention of Canadian or Foreign Laws:** If the disclosure is made on the initiative of the organization to a government institution, which has reasonable grounds to believe that the information relates to a contravention of the laws of Canada, a province, or a foreign jurisdiction that has been, is being, or is about to be committed [paragraph 7(3)(d)(i)].
- **Emergency Situation:** If the disclosure is for the purpose of acting in respect of an emergency that threatens the life, health or security of an individual [paragraphs 7(2)(b) and 7(3)(e)].

ii. *Privacy Act*

The *Privacy Act* governs the personal information handling practices of federal government departments and agencies. Information may only be disclosed without an individual's consent in a limited set of circumstances. These include:

- **Use Consistent with Original Consent:** For the purpose for which the information was obtained or compiled, or for a use consistent with that purpose, i.e. "if employers wish to use their employee's phone number to provide updates about a pandemic" [paragraph 8(2)(a)].
- **Authorized by Legislation:** Where authorized by any other Act of Parliament or any regulation made thereunder that authorizes its disclosure [paragraph 8(2)(b)].
- **Information Sharing Agreement:** Under an information sharing agreement between federal government institutions and the government of a province, foreign estate, some First Nations councils, or international organization, for the purpose of enforcing any law or carrying out a lawful investigation [paragraph 8(2)(f)].
- **Public Interest Disclosure:** Where, in the opinion of the head of the institution, the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure; or where the disclosure would clearly benefit the individual to whom the information relates [paragraph 8(2)(m)].

The OPC has further provided that, "[w]hile privacy laws include several provisions that authorize the collection, use and disclosure of personal information in the context of a public health crisis, if you rely on them, you should be able to communicate to the persons involved the specific legislative authority under which this is done". As such, it is important to consult the text of these specific exemptions prior to taking action that implicates the privacy of an individual.

Given the Minister of Health's announcement of an Emergency Order under the Quarantine Act on March 25, 2020, it is possible that the above listed provisions may be relied upon to justify the disclosure of personal information without consent.

2. Alberta

In a recent advisory, "Privacy in a Pandemic", the Office of the Information and Privacy Commissioner of Alberta ("OIPC AB') has noted that in the case where a public or general emergency is declared, the powers to collect, use and disclose personal information or personal health information to protect the public may be very broad.

Alberta has three privacy laws, which govern the collection, use, and disclosure of personal or personal health information, the:

(1) *Freedom of Information and Protection of Privacy Act* for the public sector;
(2) *Health Information Act* for the health sector; and
(3) *Personal Information Protection Act* for the private sector.

Each legislation contains provisions to allow for the sharing of personal or personal health information in

the event of an emergency, without consent. However, this authority must be exercised proportionately and limited to information that is needed to achieve the purpose of collection, use or disclosure, and within the scope of the authorization provided by the specific exemption. Organizations must consult the text of the applicable privacy law for the wording of the specific disclosure exemption.

On the access to information front, the OIPC AB has issued a separate notice regarding "Requests for Time Extensions During an Emergency". The OIPC AB is currently not considering any time extensions for responding to access requests beyond the circumstances outlined in section 14(1) of the *Freedom of Information and Protection of Privacy Act*. "A public body does have authority to grant itself a 30-day extension under section 14(1) if unable to access or process records due to a disaster or pandemic. Furthermore, the Commissioner has no ability to grant an extension in such circumstances." If requests cannot be addressed in a timely fashion, the Commissioner advises public bodies to inform applicants about their right to seek a review pursuant to section 65(1).

The OIPC AB has also specified that the AB Information and Privacy Commissioner has no authority under *Health Information Act* to disregard a health custodian's section 64 obligations to prepare a privacy impact assessment during a public health emergency. On April 14, 2020, the AB Information and Privacy Commissioner advocated for a flexible approach, while reinforcing the importance of the right to access information.

3. British Columbia

The Office of the Information and Privacy Commissioner for British Columbia (OIPC BC) has issued a statement on COVID-19, indicating that British Columbia's privacy laws are designed to ensure appropriate information sharing that protects the health and safety of British Columbians. The Provincial Health Officer has broad authority to collect and use personal information in the public interest. While no reference is made to the interpretation afforded to British Columbia's privacy laws in light of COVID-19, we expect that certain exemptions therein may also be applicable in some circumstances during this emergency.

The OIPC BC is responsible for overseeing and enforcing the:

(1) *Freedom of Information and Protection of Privacy Act*; and
(2) *Personal Information Protection Act*.

For example, section 33.1 of the *Freedom of Information and Protection of Privacy Act* outlines circumstances in which a public body may disclose personal information, with or without consent. The text of these particular disclosure exceptions should be reviewed to assess their application in a particular situation.

As it relates to access requests under British Columbia's privacy laws, British Columbia's Privacy Commissioner has issue a "Decision" stating that it is fair and reasonable to grant the head of each public body in British Columbia permission to extend the time to respond to a request for access to records under the *Freedom of Information and Protection of Privacy Act* (FIPPA).

This permission applied to requests for access to records that a public body receives between March 1, 2020 and April 30, 2020. It was extended on April 22, 2020, to apply to requests received between May 1 and May 15, 2020. These extensions are granted in addition to any extension of time that a public body is authorized to make. A public body that extends time pursuant to this Decision is expected to provide the Commissioner's Office with a document listing every request for access in respect of which it has extended the time for responding by July 15, 2020. Moreover, pursuant to subsection 10(3) of FIPPA, public bodies are reminded to notify each applicant of any extension of time.

As a result of the COVID-19 pandemic, the Minister of Citizens' Services in British Columbia has enacted Ministerial Order No. M085, directly dealing with the province's public sector privacy law. In an effort to

strengthen the province's public health response, this Order provides public bodies with explicit authority to disclose personal information within and outside Canada pursuant to the *Freedom of Information and Protection of Privacy Act* until June 30, 2020. The disclosure must be necessary:

- For the purposes of communicating with individuals respecting COVID-19,
- For the purposes of supporting a public health response to the COVID-19 pandemic, or
- For the purposes of coordinating care during the COVID-19 pandemic.

The Order also provides for disclosures of personal information inside or outside Canada, using third party tools and applications, in prescribed circumstances. This carves out new exceptions from British Columbia's privacy and data-residency laws which require personal information about citizens to be stored in and only accessed within Canada. This Order aims to temporarily permit health care bodies, such as the Ministry of Health, the Ministry of Mental Health and Addictions, and other health authorities to use communication and collaboration software that may host information outside of Canada to better respond to the pandemic.

4. Manitoba

The Office of the Ombudsman in Manitoba has oversight over the following provincial access and privacy laws:

(1) *Freedom of Information and Protection of Privacy Act*; and
(2) *Personal Health Information Act.*

Manitoba has not commented on any specific interpretations that apply to these privacy laws in light of a public health emergency. We recommend that the text of the laws themselves be reviewed to discern whether particular exemptions may apply in light of current events. For example, section 44(1) of the *Freedom of Information and Protection of Privacy Act* outlines instances in which a public body may disclose personal information. Consent of the individual is not required under certain exceptions.

The Office of the Ombudsman has issued advisories for public bodies (in relation to its public sector privacy law) and trustees (in relation to its health sector privacy law). Manitoba is taking the impact of COVID-19 into consideration as an exceptional circumstance that may impact a public body's ability to respond to access requests within the 30 day time limit mandated by the province's *Freedom of Information and Protection of Privacy Act*. The Manitoba Ombudsman has also issued a specific advisory for trustees about responding to access requests under the *Personal Health Information Act*.

5. New Brunswick

In New Brunswick, the Office of the Ombud for New Brunswick ("Office of the Ombud"), Access to Information and Privacy Division, oversees and enforces the:

(1) *Right to Information and Protection of Privacy Act*; and
(2) *Personal Health Information Privacy and Access Act*.

On March 27, 2020, the Office of the Ombud issued guidance on privacy and the COVID-19 outbreak. This guidance highlights the provisions, under both legal frameworks, in which public bodies (under the public sector privacy law) and custodians (under the health sector privacy law) may disclose personal information or personal health information without consent in specific circumstances. The provided guidance also emphasizes that: "Both Acts require that any collection, use or disclosure of personal information or personal health information be limited to that which is needed to achieve the responsible purpose of the collection, use or disclosure". Please visit the guidance document and text of the applicable legislative provisions for more information.

The Office of the Ombud has also issued a notice on its operations and impacts to access requests related to its public sector privacy law. The Access and Privacy Division of the Office of the Ombud has closed its offices and suspended active complaint investigations. However, it will continue to respond

to urgent matters, such as time extension applications and requests to disregard access requests (sections 11 and 15 of the *Right to Information and Protection of Privacy Act*).

More recently, on April 14, 2020, a memorandum was issued regarding privacy breaches. Specifically, this served as a reminder to public bodies and health care custodians of mandatory breach reporting requirements, in light of the declared state of emergency on March 19, 2020.

6. Newfoundland and Labrador

Newfoundland & Labrador's privacy laws are the:

(1) *Access to Information and Protection of Privacy Act*, 2015; and
(2) *Personal Health Information Act*.

The Office of the Information and Privacy Commissioner for Newfoundland and Labrador ("OIPC NL") is the body responsible for overseeing and enforcing these laws. It has issued COVID-19 privacy guidance in the form of a slide deck, "Don't Blame Privacy – What To Do and How To Communicated in an Emergency". The position of the OIPC NL is that emergencies impact, but do not supplant the need for privacy. While privacy considerations should not put anyone's health at risk, privacy interests should still be protected where possible:[5] "This slide deck is intended to shine some light on where the communication line is when privacy and urgent circumstance collide. The goal is to demonstrate how to not unnecessarily violate privacy, while also preventing unwarranted concerns from slowing response times."

The materials highlight circumstances under each Newfoundland and Labrador privacy law whereby the indirect collection of personal information and personal health information is appropriate. While obtaining consent for the disclosure of personal information is the general rule, these statutes are not barriers to the appropriate sharing of information in an emergency where consent cannot be obtained. "Both acts (ATIPPA and PHIA) have provisions that allow for disclosure in emergencies or when the public interest trumps the protection of privacy."[6] The slide deck also discusses issues around the repercussions of release. Specifically, the application of certain "shields" for public bodies and custodians when they act in good faith under the provincial privacy laws. However, it is important to note that regardless of the situation, privacy principles continue to apply and parties are reminded to collect, use, and disclose the minimum information that is necessary.

On March 18, the Office of the Information and Privacy Commissioner announced that it is preparing an application to the Supreme Court to extend the 65 business day time limit for the issuance of Commissioner's reports. A further notice will be issued when the Court decides on this application.

In its quarterly newsletter, "Above Board", issued in April of 2020 (vol. 12, issue 2), the OIPC NL addressed several topics in relation to the pandemic, including: processing access requests during the COVID-19 pandemic; time extensions; what to do and how to communicate in an emergency; and privacy impact assessments.

OIPC NL has also adopted a framework for the provincial government to assess privacy-impactful initiatives in response to COVID-19.

7. Northwest Territories

The Northwest Territories has two privacy laws, which fall under the purview of the Information and Privacy Commissioner of the Northwest Territories:

(1) *Access to Information and Protection of Privacy Act*;
(2) *Health Information Act*.

The Information and Privacy Commissioner of the Northwest Territories has issued/promoted several resources in response to these extraordinary circumstances: (1) Privacy in a Pandemic; (2) Privacy and Working from Home; and (3) Access to Information in Extraordinary Times (a message from Canada's Information Commissioner that applies to NT as well).

The "Privacy in a Pandemic" resource highlights specific legislative provisions, pursuant to each privacy law, that permits disclosure of personal information and personal health information, with or without consent of the individual. These may be engaged as necessary and applicable in the public interest in the event of an emergency. Any collection, use, or disclosure of personal information or personal health information must be limited to that which is needed to achieve the reasonable purpose of that collection, use, or disclosure.

This particular resource also highlights that the Chief Public Health Officer has broad powers to collect, use and disclose personal health information to protect public health, whether or not a formal health emergency is declared. Moreover, Orders issued under public health legislation could require the collection, use, and disclosure of certain personal information relating to employees, patients and customers.

8. Nova Scotia

The Information and Privacy Commissioner of Nova Scotia oversees and is responsible for the:

(1) *Freedom of Information and Protection of Privacy Act*; and
(2) *Personal Health Information Act*.

On March 24, Nova Scotia's Office of the Information and Privacy Commissioner ("OIPC NS") released a statement emphasizing that the Provincial Health Officer has broad authority to collect and use personal information in the public interest during these times. It encourages public bodies to contact the OIPC NS if they are unclear of their responsibilities to collect and use personal information.

The OIPC NS has directed those with questions about the pandemic to refer to guidance issued by the Privacy Commissioner of Canada and the Information and Privacy Commissioner for Newfoundland & Labrador, offering a link to the slide deck referenced above. As it relates to disclosure exceptions, please review the text of the applicable statute in light of the particular circumstances. While such exceptions were not referenced specifically by the OIPC NS, the current privacy laws still apply and disclosure exceptions could be leveraged by public bodies and health information custodians, as applicable and required.

As it relates to access rights under Nova Scotia's privacy laws, the OIPC NS will be able to review and approve or decline time extension requests from public bodies and municipalities.[7]

9. Nunavut

The Office of the Information and Privacy Commissioner of Nunavut has posted a message from Canada's Information Commissioner on its website regarding "Access to Information in extraordinary times". It indicates this also applies to the Government of Nunavut. The message emphasizes transparency and appropriate documentation practices in order to uphold the right of access.

A message was also issued on protecting privacy while working from home.

10. Ontario

The Information and Privacy Commissioner of Ontario ("IPC") has not yet released specific guidance on how to interpret the province's privacy legislation during a public health emergency, such as COVID-19. However, its news release on the Impact of COVID-19 offers insight into its operations, including what essential services will be provided by the IPC during this time, and "tips" for those working from home.

While the IPC news release was not explicit in describing the application of privacy laws during a public health crisis, exceptions to disclosure may still be applicable in the circumstances. For example, section 42 of Ontario's *Freedom of Information and Protection of Privacy Ac*t outlines permitted disclosures, not unlike those found in other privacy laws.

The IPC oversees the application of several privacy laws in Ontario, meaning that its news release is applicable for relevant organizations in the public, health and child and youth sectors across Ontario. These laws include:

(1) *Freedom of Information and Protection of Privacy Act*;
(2) Part X of the *Child, Youth and Family Services Act*;
(3) *Municipal Freedom of Information and Protection of Privacy Act*; and
(4) *Personal Health Information Protection Act*.

IPC has stated that the expectation to comply with Ontario's access laws remains in effect. However, the current circumstances will be taken into account when evaluating appeals relating to deemed refusals should there be an impact on an organization's ability to respond within prescribed time limits

11. Québec

On March 25, 2020, the Québec Commission d'accès à l'information ("COI") commented on the impact of COVID-19 on the protection of personal information. The Québec government declared a state of health emergency on March 13, 2020. Pursuant to the *Public Health Act* (c. S-2.2), such a declaration allows health authorities to gain access to personal or confidential information in order to protect the health of the population [section 123].

In Québec, two main laws outline the protection of personal information:

(1) *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (c. A-2.1) for the public sector; and
(2) *Loi sur la protection des renseignements personnels dans le secteur privé* (c. P-39.1) for the private sector.

Pursuant to both, consent is a necessary element to communicating personal information, unless there is an exception provided by law. These exceptions can allow for the disclosure of personal information without consent if such disclosure is:

(a) necessary for the application of a law in Quebec;
(b) made to a person having the power to compel the disclosure of personal information and who requires it in the exercise of their functions;
(c) made due to an emergency situation that endangers the life, health or safety of the person concerned; and
(d) necessary for the exercise of a mandate or the execution of a service or business contract.

The COI has also addressed the topics of technology, transparency, and respecting the rights of tenants in its various communications.

12. Saskatchewan

The Information and Privacy Commissioner of Saskatchewan ("IPC SK") has oversight over the:

(1) *Freedom of Information and Protection of Privacy Act*;
(2) *Local Authority Freedom of Information and Protection of Privacy Act*; and
(3) *Health Information Protection Act*.

The IPC SK has issued several statements, which can be accessed here at the bottom of the page, under the heading, "What's New?".

The statement on COVID-19 supports that privacy laws should not be a barrier to appropriate information sharing. Provisions under each act will allow for the sharing of personal information or personal health information by public bodies and trustees in the event of an emergency, within the bounds of the particular exception. The collection, use, or disclosure of personal information or personal health information must be limited to that needed to achieve the purpose for which these actions were taken (i.e. "data minimization principle").The statement on access to information during a pandemic clarifies that citizens of Saskatchewan still have the right to request information or records and public bodies are still required to accept and process access requests. "Public bodies when faced with a heavier that normal workload on access requests, can consider an extension but no public body should just refuse to process the request."

The IPC SK has notably issued a "Pandemic Binder" on May 1, 2020, in an attempt to consolidate its blogs, statements and advisories, as well as those of other Commissioners. It has since continued to release advisories on specific, targeted issues.

13. Yukon

The Yukon Information and Privacy Commissioner has oversight authority to monitor compliance with Yukon's two privacy laws, the:

(1) *Access to Information and Protection of Privacy Act* ("ATIPP"); and
(2) *Health Information Privacy and Management Act* ("HIPMA").

The Ombudsman and Information and Privacy Commissioner of the Yukon has oversight of these laws. The Yukon Information and Privacy Commissioner has issued guidance on Disclosure of Personal Information during an Emergency in Yukon. This guidance maintains that Canadian privacy laws all contain provisions that allow for the disclosure of personal information or personal health information in the event of an emergency. The documents proceed to outline provisions that authorize public bodies to disclose personal information without an individual's consent. The same exercise is undertaken for HIPMA and the comparable authorizations for custodians.

Section 36(b) of ATIPP authorizes a public body to disclose personal information about an individual with their consent. However, section 28 and section 36(d), (f), (n), (o) authorize public bodies to disclose personal information without an individual's consent including in the case of emergency. Similarly, HIPMA contains several provisions that authorize a custodian to disclose personal health information without consent. Some of these provisions provide specific authority for custodians to disclose personal health information in the case of an emergency. Regardless, information custodians must apply the limitation principles to disclosure.

Guidance has also been issued on access to information and possible delays during the COVID-19 pandemic.

C. BEST PRACTICES FOR EMPLOYERS

Several provincial privacy authorities have urged employers to deploy secure remote access measures for employees. Relevant guidance can currently be found for the following jurisdictions:

Alberta
British Columbia
New Brunswick
Northwest Territories
Nunavut
Ontario
Québec
Saskatchewan
Yukon

Ontario and Yukon have both released helpful guidance for employees dealing with personal information when working from home. These can be summarized as follows:

- Password protect all mobile devices and lock your device when not in use;
- Ensure portable storage devices, such as USBs, are encrypted and password protected;
- Keep your software up-to-date;
- Do not use personal email accounts to handle personal data;
- Only remove personal information from the office if it is necessary to carry out your job duties; and
- Electronic devices and paper records should not be left unattended in vehicles or public spaces.

In Québec, public bodies and businesses have the obligation to put in place security measures to ensure the protection of personal information. The COI has also warned employers to be aware and equipped to deal with cyberfraud and phishing attempts by phone, email or text message.

Alberta's Information and Privacy Commissioner has asked health custodians considering new administrative practices or information systems with implications for individuals' privacy to combat the pandemic to notify the Commissioner about such new measures. These health custodians are also required to submit privacy impact assessments pursuant to section 64 of the *Health Information Act*.

***

We will continue to provide you with important updates as new developments continue to happen. Please reach out to the COVID-19 dedicated team at Gowling WLG for support and questions.

***

NOT LEGAL ADVICE. Information made available on this website in any form is for information purposes only. It is not, and should not be taken as, legal advice. You should not rely on, or take or fail to take any action based upon this information. Never disregard professional legal advice or delay in seeking legal advice because of something you have read on this website. Gowling WLG professionals will be pleased to discuss resolutions to specific legal concerns you may have.

[***Wendy J. Wagner*** *is a partner in Gowling WLG's Ottawa office and leader of the firm's Privacy & Data Protection Group. Her practice focuses on international trade, privacy, access to information and defamation law. Wendy's expertise is recognized by Chamber Global, The Legal 500, Lexpert, Expert Guides and Best Lawyers.*

Sarah Boucaud *is an associate lawyer in Gowling WLG's Ottawa office. Her practice focuses on international trade and privacy law. Sarah is on the board of the Organization of Women in International Trade, Ottawa chapter (OWIT-Ottawa).*

Romina Hassanzadeh *is an articling student in Gowling WLG's Ottawa office. Romina completed her JD degree at the University of Ottawa. During her studies, she has remained active in the community, volunteering as an intern at Pro Bono Ontario.*]

---

1 Office of the Privacy Commissioner of Canada ("OPC"), "Announcement: Commissioner issues guidance on privacy and the COIVD-19 outbreak" (March 20, 2020), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200320/> ["Announcement"].

2 Announcement, *ibid*.

3 OPC, "Privacy and the COVID-19 outbreak" (March 2020), online: https://www.priv.gc.ca/en/privacy-topics/health-genetic-and-other-body-information/health-emergencies/gd_covid_202003/ ["OPC-COVID-19 outbreak"].

4 OPC-COVID-19 outbreak, *ibid*.

5 Office of the Information and Privacy Commissioner for Newfoundland and Labrador, "Don't Blame Privacy – What To Do and How to Communicate in an Emergency" at slide 2, online: <https://www.oipc.nl.ca/pdfs/EmergenciesPrivacy.pdf>.

6 *Ibid* at slide 6.

7 Office of the Information & Privacy Commissioner of Nova Scotia, "What's New", online: <https://oipc.novascotia.ca/>.