David Asper Centre for Constitutional Rights
UNIVERSITY OF TORONTO

Brief on Modernising the *Privacy Act*

Prepared by the David Asper Centre for Constitutional Rights'
Privacy Act *Reform Working Group*

September 25, 2023
Toronto, Canada

Working Group Leaders

Natasha Burman, Sabrina Macklai, Wei Yang

Working Group Contributors

David Côté, Monica Gill, Elliot Jarmain, Dongwoo Kim, Stephen Mapplebeck, Ally Mastantuono, Gordon Milne, Kathryn Mullins, Michael O'Keefe, Yasmin Rezaaifar, Calvin Wang, Hannah West, Alyssa Wong

A special thanks to Executive Director Cheryl Milne, Program Coordinator Tal Schreier, and Professor Lisa Austin for their guidance and constructive feedback throughout the research and writing process.

Table of Contents

About the David Asper Centre for Constitutional Rights

The David Asper Centre for Constitutional Rights (the "Asper Centre") is a centre within the University of Toronto, Faculty of Law devoted to advocacy, research, and education in relation to constitutional rights in Canada. The Asper Centre houses a unique legal clinic that brings together students, faculty, and members of the legal profession to work on significant constitutional cases. Through the establishment of the Asper Centre, the University of Toronto joins a small group of international law schools that play an active role in constitutional debates of the day. It is the only Canadian centre in existence that attempts to bring constitutional law research, policy, advocacy and teaching together under one roof. The Asper Centre aims to play a vital role in articulating Canada's constitutional vision to the broader world. The Asper Centre was established through a generous gift to the law school from University of Toronto law alumnus David Asper (LLM '07).

About the *Privacy Act* Reform Working Group

The *Privacy Act* Reform Working Group (the "Working Group") is led by Natasha Burman (JD 2023), Sabrina Macklai (JD/MI 2023), and Wei Yang (JD 2023) from the University of Toronto Faculty of Law (the "Faculty"). The following students at the Faculty generously contributed to this report as part of the Working Group: David Côté, Monica Gill, Elliot Jarmain, Dongwoo Kim, Stephen Mapplebeck, Ally Mastantuono, Gordon Milne, Kathryn Mullins, Michael O'Keefe, Yasmin Rezaaifar, Calvin Wang, Hannah West, and Alyssa Wong.

The Working Group's objective is to provide recommendations to the House Committee on Access to Information, Privacy and Ethics that ensure future *Privacy Act* reforms and amendments will make the statute fully compliant with the *Canadian Charter of Rights and Freedoms*.

Acknowledgements

We would like to express our greatest appreciation and gratitude to David Asper Centre Executive Director Cheryl Milne, Program Coordinator Tal Schreier, and Faculty Advisor Professor Lisa Austin for their guidance and support. We also would like to extend a special thanks to Gordon Milne and Alyssa Wong, the Working Group members who went above and beyond in helping the Working Group leaders draft this final submission.

PART I: Introduction and Background

Canada's *Privacy Act,* RSC 1985 c P-21[1] (the "*Act*"), which came into force in 1983, regulates the federal government and public-sector institutions' collection, use, disclosure, retention, and disposal of individuals' personal information. In doing so, it governs individuals' privacy rights in their interactions with federal institutions. 40 years later, the *Act* remains substantially unchanged, despite advancements in technology and society at large. Recognizing the need for change, the Department of Justice Canada ("Justice Canada") initiated a commitment to modernise the *Act* starting in 2017.[2] Although Justice Canada has since completed an online public consultation on potential reforms to the *Act*, the legislative amendment process has yet to begin.[3]

The following written submissions by the *Privacy Act* Reform Working Group (the "Working Group") offer 14 recommendations to the House Committee on Access to Information, Privacy and Ethics (the "House Committee") for reforming the *Privacy Act.* They also act as a reminder of the rich sources of information that are already publicly available to inform the House Committee and Parliament of the improvements necessary to better protect and respect the information of fellow Canadians. The following recommendations are divided into three broad categories:

1. Recommendations to make the *Privacy Act Charter*-compliant;
2. Recommendations to bring the *Privacy Act* in line with its international counterparts; and
3. Recommendations based on the 2016 House Committee Report.

The *Act* as it currently stands fails to fully conform and comply with the *Canadian Charter of Rights and Freedoms* (the "*Charter*").[4] Sections of the *Act* contravene the *Charter*'s section 8 guarantee to be free from unreasonable search and seizure. For example, sections 8(2)(e) and (f) of the *Act* allow investigative bodies like law enforcement agencies to obtain personal information held by federal bodies for the purpose of furthering ongoing investigations. Claimants have criticised these provisions

---

[1] *Privacy Act,* RSC 1985 c P-21 [*Privacy Act*].

[2] Department of Justice Canada, "Modernizing Canada's Privacy Act" (September 2021), online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>; The Honourable Jody Wilson-Raybould, *Letter to Blaine Calkins, Chair of the Standing Committee on Access to Information, Privacy, and Ethics*, April 12, 2017, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/GovResponse/RP8892754/421_ETHI_Rpt04_GR/421_ETHI_Rpt04_GR-e.pdf>.

[3] Department of Justice Canada, "Modernizing Canada's Privacy Act – Engaging with Canadians" (March 2022), online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/index.html>.

[4] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

for giving investigative bodies legal shortcuts to seize personal information and conduct warrantless searches, which have raised concerns over using personal information in ways that claimants have not directly consented to.

In addition, the right to privacy, while not explicitly codified in the *Charter*, has been time and time again recognized by the Supreme Court of Canada ("SCC") to underlie the *Charter*'s section 7 right to life, liberty, and security of the person. Former Chief Justice Beverley McLachlin, speaking for the majority in *R v Sharpe* (2001), famously stated that "privacy is at the heart of liberty in a modern state,"[5] citing previous SCC judgments of *R v Dyment* (1988)[6] and *R v Edwards* (1996)[7]*.* The *Act* must be amended to adequately protect the fundamental right of privacy.

Beyond sections 7 and 8 of the *Charter*, under which most privacy-related complaints have arisen, more than 20 years ago, the SCC in *R v Ruby* read down section 51(2)(a) of the *Act* for unjustifiably infringing the *Charter*'s section 2(b) guarantee of freedom of the press.[8] However, this section of the *Act* has yet to be amended despite this decision being released in 2002—stressing the need for Parliament to take not only a more responsive approach to this reform, but also a more proactive one on the issues that exist today and in the future with respect to this *Act*.

The *Privacy Act* has also fallen behind the advancements made in other countries' public-facing privacy legislation, particularly the European Union's ("EU") *General Data Protection Regulation* ("*GDPR*").[9] This legislation provides data subjects with extensive rights that are absent in the *Privacy Act,* such as the right to be informed about one's personal data and the right to erase such dataions with federal bodies compared to Canada.

Given the nature of privacy rights as being fundamental rights, there should be transparency, coordination, and collaboration at all levels of the decision-making process for the reform of the *Act*. The Government of Canada and Parliament have made some moves toward *Privacy Act* reform in the past few years, which should continue to inform the *Act*'s review. Most notably, in 2016, the House of Commons Standing Committee on Access to Information, Privacy, and Ethics released a report with

[5] *R v Sharpe*, 2001 SCC 2 at para 26.
[6] *R v Dyment*, [1988] 2 SCR 417, [1988] SCJ No 82.
[7] *R v Edwards*, [1996] 1 SCR 128, [1996] SCJ No 11 [*Edwards*].
[8] *R v Ruby (Solicitor General)*, 2002 SCC 75 at para 67 [*Ruby*].
[9] EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679> [*GDPR*].

several recommendations related to reforming the *Privacy Act* (the "House Committee Report").[10] In the fall of 2020, Justice Canada launched a public consultation on "modernizing Canada's *Privacy Act*," with a summary of the results being published in a 2021 report (the "Justice Canada Summary").[11] The Justice Canada Summary fails to address some substantive *Charter*-related issues, is conspicuously silent on some recommendations made by the House Committee Report five years prior, and does not adequately consult vulnerable groups such as Indigenous peoples or racialized minorities. In addition, the Working Group found that the Justice Canada Summary placed an alarming emphasis on internal views of government stakeholders over other parties.

In addition to the recommendations for reforming the *Act*, the Working Group urges the Government to review their processes and policies with respect to Access to Information requests. As elaborated in Part VI below, during the course of drafting this brief, a Working Group member submitted an Access to Information Request for the public consultation submissions but encountered significant issues and delays in successfully retrieving such data. This speaks to greater problems that rise beyond reforming the *Act*.

[10] House of Commons, *Protecting the Privacy of Canadians: Review of the Privacy Act: Report of the Standing Committee on Access to Information, Privacy and Ethics* (December 2016) (Chair: Blaine Calkins), online: <https://publications.gc.ca/collections/collection_2016/parl/xc73-1/XC73-1-1-421-4-eng.pdf> [House Committee Report].

[11] Department of Justice Canada, *Modernizing Canada's Privacy Act: What We Heard Report: Justice Canada's Online Public Consultation on Privacy Act Modernization*, Catalogue No J2-494/1-2021E-PDF (Ottawa: Department of Justice Canada, 2021), online: <https://justice.canada.ca/eng/csj-sjc/pa-lprp/wwh2-cqnae2/pdf/wwhr_pam_2021_en2.pdf> [Justice Canada Summary].

PART II: Recommendations in Brief

In these submissions, we respectfully provide the following 14 recommendations.

Recommendations to Make the *Privacy Act Charter*-Compliant

Recommendation 1: Amend section 8(2)(f) of the *Privacy Act* to incorporate safeguards that ensure it does not enable investigative bodies to use individuals' personal information without their consent or to conduct warrantless searches.

Recommendation 2: Amend section 8(2)(f) of the *Privacy Act* to require requests for disclosure be in written form.

Recommendation 3: Amend the *Privacy Act* to provide examples of when disclosure under the *Act* engages an individual's reasonable expectation of privacy.

Recommendation 4: Amend the *Privacy Act* to include a preamble that explicitly links the right to privacy to section 7 of the *Charter*, particularly under the "liberty" and "security of the person" interests.

Recommendation 5: Amend the *Privacy Act* to explicitly define "health and biometrics information."

Recommendation 6: Amend section 51(2)(a) of the *Privacy Act* to confirm that the Federal Court retains discretion over whether a proceeding will be held *in camera* when reviewing an application that falls under section 51(1) of the *Act*.

Recommendations to Bring the *Privacy Act* in Line with its International Counterparts

Recommendation 7: Update the *Privacy Act*'s definition of "personal information" by first, removing the requirement that information must be recorded and second, defining identifiability.

Recommendation 8: Amend the *Privacy Act* to clarify when a government institution can collect personal information.

Recommendation 9: Amend the *Privacy Act* to apply the same legal standard to justify the collection, maintenance, use, and disclosure of personal information.

Recommendation 10: Amend the *Privacy Act* to include enhanced requirements for Information Sharing Agreements between state entities.

Recommendation 11: Amend the *Privacy Act* to expand the rights of the data subject by including (1) the right to erase one's personal data; (2) the right to restrict the processing of one's personal data; (3) the right to be informed about one's personal data; (4) the right to data portability; (5) the right to object to the processing of one's personal data; and (6) the right to not be subject to a decision based solely on automated processing.

Recommendation 12: Amend the *Privacy Act* to regulate the transfer of personal data to law enforcement entities consistent with the United Kingdom's ("UK") *Data Protection Act.*

Recommendations Based on the 2016 House Committee Report

Recommendation 13: Amend the *Privacy Act*'s coverage to include all federal government institutions.

Recommendation 14: Following the House Committee Report, the Privacy Commissioner should be provided three new institutional mechanisms to uphold *Privacy Act* requirements: (1) the implementation of "privacy impact assessments;" (2) an ongoing five-year parliamentary review of the *Privacy Act*; and (3) the implementation of Information Sharing Agreements.

PART III: Recommendations to Make the *Privacy Act Charter*-Compliant

This section explores ways to amend the *Privacy Act* so that it is compliant with the *Charter*. Currently, the *Act* is in tension and sometimes even directly conflicts with at least three *Charter* rights: sections 8, 7, and 2(b).

Section 8: The Right to be Secure Against Unreasonable Search or Seizure

The Working Group reviewed *Charter* challenges against section 8 of the *Privacy Act* that allegedly conflict with the *Charter*'s section 8 right to be secure against unreasonable search or seizure.[12] Section 8 of the *Act* permits federal bodies to disclose personal information in its control under certain circumstances.[13] Challenges to this section of the *Act* have concerned permitting infringements of an individual's reasonable expectation of privacy, unjustifiably expanding the scope of searches permitted under the law, and a lack of regulation over disclosing personal information between government agencies. The Working Group recommends that section 8 of the *Act* be amended to include various safeguards that prevent abuse of process and powers.

1. We recommend amending section 8(2)(f) of the *Privacy Act* to incorporate safeguards that ensure it cannot be used by investigative bodies to use individuals' personal information without their consent or to conduct warrantless searches.

The Working Group found that most claimants challenging the constitutionality of the *Act* criticised section 8(2)(f) for giving investigative bodies a legal shortcut to use personal information in ways claimants did not directly consent to nor have a warrant to access. Section 8(2)(f) allows the disclosure of personal information "for the purpose of administering or enforcing any law or carrying out a lawful investigation."[14] Under this section, investigative bodies like law enforcement agencies can acquire personal information by simply making written requests to the federal bodies holding that information. It is up to the discretion of government agencies to decide whether to disclose the requested information. This is in tension with the *Charter*'s section 8 guarantee as it undermines claimants' privacy interests and effectively enables warrantless searches.

For example, in a British Columbia Supreme Court decision where law enforcement officers used section 8(2)(f) of the *Act* to obtain claimants' personal information from a federal body, the claimants took issue with the fact that the police did

[12] *Charter*, *supra* note 4 at s 8. Note: The Working Group conducted a search of every section 8 *Charter* challenge to the *Privacy Ac*t since it came into force. The most relevant challenges were selected to guide these recommendations

[13] *Privacy Act*, *supra* note 1 at s 8.

[14] *Ibid* at s 8(2)(f).

not have a warrant to use their personal information.[15] In particular, the claimants argued that section 8(2)(f) of the *Act* allowed law enforcement to "impermissibly [take] the easy route while ignoring constitutionally compliant ways to obtain the same evidence," and that "the Federal-Provincial agreement … [is] essentially inaccessible to members of the public, and therefore contrary to the rule of law requiring the state to give fair notice to citizens of laws and limitations of their rights through enacted laws."[16] The British Columbia Supreme Court acknowledged the use of section 8(2)(f) as a search and seizure workaround as not only unlawful, but also that any sort of intergovernmental agreement that facilitates such actions cannot be kept hidden away from the public. The Working Group echoes these complaints; in the absence of a warrant, consent, or other compelling legal justification, law enforcement should not be able to access claimants' personal information.

Whether section 8(2)(f) of the *Act* indeed confers warrantless search powers to law enforcement remains unclear, at least according to the courts. In 2006, the Ontario Superior Court of Justice held that the *Act* "does confer additional warrantless search powers on certain specified investigators ... to obtain an individuals [*sic*] personal information."[17] According to the decision, requiring a warrant under section 8(2)(f) of the *Act* would render unnecessary section 8(2)(c), which permits disclosures pursuant to warrants.[18] In contrast, in the aforementioned 2018 decision of *R v Flintroy*, the British Columbia Supreme Court held that section 8(2)(f) does not authorise warrantless searches. Instead, it merely "allows or permits the keeper of the record … to disclose the document where certain conditions are present," such as when a search is already authorised.[19] The SCC has yet to rule on this specific issue, though it has recognized "some merit" in the argument that section 8 of the *Charter* is engaged insofar as the *Privacy Act*'s disclosure power is an element of the law that authorises a search.[20]

Therefore, the Working Group recommends that section 8(2)(f) of the *Act* be amended to incorporate safeguards that ensure claimants' privacy rights are not undermined through the disclosure of their personal information. This can include incorporating an express consent (or warrant) requirement to obtain personal information under this section. This part of the *Act* should also be amended to incorporate and reflect the legislature's intent, specifically that section 8(2) of the *Act* does *not* grant search

[15] *R v Flintroy,* 2019 BCSC 213 [*Flintroy*, 2019] at paras 69-75.
[16] *Ibid* at paras 78-79. The agreement referenced, according to the court, refers to a memorandum of agreement between Canada and British Columbia relating to the disclosure and sharing of information that includes passport photos, *Flintroy* at para 72.
[17] *R v Stucky*, 2006 CanLII 588 (ONSC), [2006] OJ No 108 at para 22 (on an application to excise an Information to Obtain) [*Stucky*].
[18] *Ibid* at para 21.
[19] *R v Flintroy,* 2018 BCSC 1777 [*Flintroy*, 2018] at para 26.
[20] *Wakeling v United States of America*, 2014 SCC 72 at paras 36-38 [*Wakeling*].

powers. Other constitutionally compliant routes for searches and seizures, such as obtaining warrants, better protect the privacy of individuals through judicial supervision over the obtaining of evidence. At the very least, if the *Act* does confer search powers, Parliament must intervene to clarify the scope of such powers (e.g., through adding an express warrant requirement).

2. We recommend amending section 8(2)(f) of the *Privacy Act* to require requests for disclosure be in written form.

The Working Group found that, in practice, disclosures of personal information under section 8(2)(f) may be in response to oral requests.[21] This is in contrast with the requirement for a *written* request under section 8(2)(e) of the *Privacy Act*, another provision authorising investigative bodies to acquire and disclose personal information. As these provisions are very similar in that they both permit the disclosure of personal information to and from law enforcement agencies, and potentially engage individuals' section 8 *Charter* rights, they should have the same formality requirement for requests.

The requirement for written requests under section 8(2)(e) of the *Act* has unfortunately not been well-enforced by the courts. In *R v Stucky,* the Royal Canadian Mounted Police ("RCMP") in deciding to "share the fruits of [their] investigation," requested permission from Canada Post to disclose the claimant's personal information (that the RCMP originally obtained from Canada Post) to the Competition Bureau (the "Bureau").[22] Notably, this was not prompted by the Bureau's written request to the RCMP, contrary to the letter and spirit of the *Act*.[23] Furthermore, the RCMP only received oral permission from the Canada Post to share that information with the Bureau.[24] Despite the approval not being in written form as required by Canada Post, nothing turned on this finding.[25] This is consistent with later case law: failure to receive written requests and permission is considered a mere minor or technical breach of a limited privacy interest.[26]

With respect, the Working Group disagrees with this analysis. The Working Group recommends that the *Privacy Act* be amended to affirm the importance of the mandated written request, particularly for disclosures made under sections 8(2)(e) and (f). A written requirement not only ensures proper record-keeping for posterity's sake but helps keep government entities accountable when such requests for information are later made and potentially scrutinised.

---

[21] See for example, *Stucky*, *supra* note 17.
[22] *Stucky*, *supra* note 17 at para 5.
[23] *Ibid*.
[24] *Ibid*.
[25] *Ibid*.
[26] *R v Finnegan,* 2014 ONSC 2032 at para 30.

3. We recommend amending the *Privacy Act* to provide examples of when disclosure under the *Act* engages an individual's reasonable expectation of privacy.

The Working Group's survey of the case law revealed that the test for determining whether the *Privacy Act* engages an individual's reasonable expectation of privacy, thereby engaging their section 8 *Charter* rights, is evaluated through a four-part "totality of the circumstances" analysis.[27] This is a heavily contextual analysis, with courts split on what contextual factors are most relevant and to what degree. This has led to courts holding that the same information can attract a reasonable expectation of privacy in one circumstance but not in another. The *Act* should therefore be amended to provide clarity on what contextual factors should guide this analysis.

The SCC has recognized that some contexts preclude the existence of a reasonable expectation of privacy.[28] In the 2012 decision of *R v Cole*, the SCC suggested that the key element in finding a reasonable expectation of privacy is proof that the information at issue was part of the claimants' "biographical core of personal information."[29] However, later decisions by various lower courts apply this reasoning inconsistently. For example, in *Flintroy,* the court was satisfied that the claimants had an objectively reasonable expectation of privacy in the personal information disclosed to law enforcement, despite the defendants accepting the information did not constitute core biographical information.[30] But a different court found that information of the same nature as in *Flintroy* carried no reasonable expectation of privacy.[31] Likewise, in *Stucky*, the reasonable expectation of privacy did not extend to some businesses trying to shield their addresses from government institutions, even though the Court found that there would ordinarily be a reasonable expectation of privacy regarding their addresses with respect to other, non-governmental institutions.[32]

The Working Group found that the current "totality of the circumstances" test used by courts does not provide enough guidance in the *Privacy Act* context as to what circumstances warrant a reasonable expectation of privacy. By amending the *Privacy Act* to include specific examples of where a reasonable expectation of privacy arises,

---

[27] *Edwards*, *supra* note 7 at para 45. See also Government of Canada, "Section 8 – Search and seizure" (June 2022), online: Government of Canada <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html>.
[28] For example, see *Bernard v Canada (Attorney General),* 2014 SCC 13 at para 41.
[29] *R v Cole*, 2012 SCC 53 at paras 45-46, citing *R v Plant*, [1993] 3 SCR 281 at 293, 84 CCC (3d) 203.
[30] *Flintroy*, 2019, *supra* note 15 at paras 80, 99-100.
[31] *R v Baldovi,* 2016 MBQB 221 at para 45.
[32] *Stucky, supra* note 17 at paras 14-15.

Parliament would be sending clearer instructions to the courts regarding what constitutes a reasonable expectation of privacy, and allows the law to be applied consistently and fairly with privacy-protecting principles in mind. The Working Group prefers a robust, privacy-centred definition, informed by the SCC's existing jurisprudence. The SCC has signalled that it will interpret Parliament's reference to "reasonable expectation of privacy" in accordance with the common law.[33] Accordingly, Parliament should keep in mind that the SCC has defined "reasonable expectation of privacy" in some circumstances as a "subjective expectation of privacy that is objectively reasonable in the circumstances."[34] This, therefore, may include records of conversations and biographical information such as birth date, residence, income, etc.

Section 7: The Right to Life, Liberty and Security of the Person

The Working Group identified a trend in the jurisprudence towards recognizing a right to privacy encompassed by the *Charter's* section 7 guarantee to the right to life, liberty and security of the person. Former SCC Justice L'Heureux-Dubé once noted that she had "great sympathy" for this idea, as have other past and current members of the SCC.[35] The *Privacy Act* should be amended to reflect these observations.

4. We recommend that the *Privacy Act* include a Preamble that explicitly links the right to privacy to section 7 of the *Charter*, particularly under the "liberty" and "security of the person" interests.

The Working Group determined that the right to privacy can fall under the *Charter*'s section 7 "liberty" and "security of the person" interests. This is because privacy is heavily tied to an individual's identity and personhood. Explicitly linking the right of privacy under the *Act* to section 7 using a preamble can ensure that individuals' privacy rights are sufficiently respected with a constitutional backing.

The SCC has suggested on numerous occasions that this expansive interpretation of privacy rights is protected under section 7 of the *Charter*. For instance, Wilson J.'s concurrence in *R v Morgentaler* points to the broader potential of privacy rights under section 7: "[T]he right to liberty contained in section 7 guarantees to every individual a degree of personal autonomy over important decisions intimately affecting their private lives."[36] Similarly, in *M. (A.) v Ryan*, L'Heureux-Dubé J. in dissent held that privacy is

[33] *R v JJ*, 2022 SCC 28 at para 46.
[34] *Ibid* at para 47, citing *Edwards*, *supra* note 7 at para 45.
[35] *M. (A.) v Ryan*, [1997] 1 SCR 157 at para 80, 143 DLR (4th) [*Ryan*] 1; See also *R v Beare*; *R v Higgins*, [1988] 2 SCR 387 at para 413, 55 DLR (4th) 481 [*Beare*]. See also *R v Morgentaler,* 1988 CanLII 90 (SCC), [1988] 1 SCR 30 [*Morgentaler*] and *Wakeling*, *supra* note 19.
[36] *Morgentaler, supra* note 35 at 171.

essential to human dignity, linking the physical and psychological interests protected under section 7 to the right to privacy.[37] Likewise, in *Edmonton Journal v Alberta (Attorney General)*, La Forest J. recognized in his dissent the close link between section 7 and the right to privacy, stating that, "in some contexts at least, privacy interests may well be invoked as an aspect of the liberty and security of the person guaranteed by s. 7 of the *Charter.*"[38] Finally, in *Ruby v Canada,* Mr. Ruby challenged section 51 of the *Privacy Act* on the grounds that it violated his sections 2(b), 7, and 8 *Charter* rights.[39] The SCC found that Mr. Ruby's section 8 *Charter* arguments were "entirely subsumed under section 7" and were thus not addressed independently.[40] This again shows the relevance of section 7 in determining if an individual's right to privacy is implicated.

While section 7 of the *Charter* does not explicitly reference a right to privacy, the Working Group recommends that explicitly referencing this section in the preamble of the *Privacy Act* will reinforce the importance of privacy as a quasi-constitutional or unenumerated constitutional right. It is important that the *Act* reflects privacy's potential to implicate individuals' liberty and security of the person interests, as recognized by the SCC. Moreover, Parliament will be able to better address the threat of privacy breaches by explicitly acknowledging the importance of privacy protection for achieving the full exercise of section 7 rights. This acknowledgment could empower the judiciary in dealing with these emerging challenges.

5. We recommend that the *Privacy Act* explicitly defines "health and biometrics information."

The Working Group found that the *Privacy Act* currently does not provide any helpful guidance on what qualifies as "health and biometrics information," or how this information is to be shared in a safe manner. The *Act* must be amended to explicitly define health and biometrics information and provide more specific guidelines around the use of this information, in order to better protect highly sensitive health and biometrics data when information sharing is required. Other jurisdictions already have such definitions in their privacy legislation; for example, the EU's GDPR defines biometric data as "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data."[41]

---

[37] *Ryan*, *supra* note 35 at para 80.
[38] *Edmonton Journal v Alberta (Attorney General)*, [1989] 2 SCR 1326 at 1377 [*Edmonton*], citing *Beare*, *supra* note 35.
[39] *Ruby*, *supra* note 8 at paras 2, 16, 24-26, 30.
[40] *Ibid* at para 30.
[41] *GDPR, supra* note 9 at Art 4(14).

Section 7 rights are increasingly being raised in cases involving health and biometrics information, like in *Cheskes v Ontario (Attorney General)* and *R v Gowdy*.[42] This trend will likely continue considering the increased interest in sharing medical data for health care services. For example, medical data may be shared to enable the use of emerging, data-driven technologies like precision medicine tools.[43] Further, in light of the COVID-19 pandemic, there have been calls for provinces and the federal government to work together more effectively, which may require sharing medical data.[44]

Section 2(b): Freedom of Expression and the Press

6. We recommend that section 51(2)(a) of the *Privacy Act* be amended to confirm that the Federal Court retains discretion over whether a proceeding will be held *in camera* when reviewing an application that falls under section 51(1) of the *Act*.

The Working Group found that the *Act* currently contains a provision that the SCC already declared unconstitutional for infringing the *Charter*'s section 2(b) guarantee to freedom of expression and the press. Section 51 of the *Privacy Act* sets out rules for hearings to review applications made to the Federal Court where access to personal information held by a government institution was refused by the head of the government institution. Section 51(2)(a) of the *Act* stipulates that *in camera* hearings are required for any applications that fall under section 51(1) of the *Act*.[45] This means they must be heard in private, or away from the public. This requirement was declared unconstitutional by the SCC and should be repealed.

In *Ruby*, the SCC held that section 51(2)(a) infringes section 2(b) of the *Charter* for being overly broad.[46] Specifically, the *in camera* requirement constituted a blanket ban on press coverings of these proceedings, infringing freedom of expression in a way that could not be saved under section 1 of the *Charter*. The SCC read the provision down so only *ex parte* submissions (i.e., where only one side of the legal proceeding is present) would be required to be held *in camera.*[47]

---

[42] *Cheskes v Ontario (Attorney General)*, 2007 CanLII 38387 (ONSC), 288 DLR (4th) 449; *R v Gowdy*, 2016 ONCA 989.
[43] Alessandro Blasimme et al., "Data Sharing For Precision Medicine: Policy Lessons And Future Directions" (2018) 37:5 Health Affairs 702 at 702.
[44] Andrea Riccardo Migone, "Trust, but Customize: Federalism's Impact on the Canadian COVID-19 Response" (2020) 39:3 Policy and Society 382 at 395.
[45] *Privacy Act*, *supra* note 1, s 51(2)(a).
[46] *Ruby*, *supra* note 8 at para 67.
[47] *Ruby*, *supra* note 8 at para 3.

The Working Group found that despite the decision being released over 20 years ago, the *Act* has yet to be updated to reflect the current state of the law. This is yet another example demonstrating the *Act*'s failure to comply with the *Charter.*

PART IV: Recommendations to Bring the *Privacy Act* in Line with its International Counterparts

This section considers ways that the *Privacy Act* may be updated to align with its international counterparts. Canadian courts have openly considered international contexts to complement and enhance their own decision-making.[48] In light of this reality, it should be noted that the *Privacy Act* has fallen behind advancements made in the public-facing privacy legislation of other countries, most notably the EU's *General Data Protection Regulation* ("*GDPR*").[49]

The Working Group surveyed equivalent legislative counterparts to the *Privacy Act* from Australia, Brazil, Chile, China, the EU, India, Japan, New Zealand, Singapore, South Korea, South Africa, Thailand, the United States, and the United Kingdom ("UK"). Following this comprehensive comparative analysis, it is evident that Canadians' personal information can be more robustly protected than what the *Act* currently provides. It should be noted that many of the listed countries have recently amended their respective legislation to bring it closer in line with the *GDPR*; hence, these submissions focus mainly on the EU legislation.[50]

Canada must follow suit in order to adequately protect the rights of data subjects (i.e., individuals whose personal information is collected, stored, and processed). In addition to the previous recommendations to make the *Act Charter*-compliant, the Working Group poses the following recommendations based on these international counterparts to the *Privacy Act* so that Canada may catch up to the rest of the world.

Recommendations Based on the *GDPR*

The *GDPR* is considered by some to be the strictest privacy and security legislation that exists today, with a very strong compliance standard that is even followed by entities outside the EU.[51] Our recommendations here for updating the *Privacy Act* pertain

---

[48] For example, see *Chaoulli v Quebec (Attorney General)*, 2005 SCC 35 at paras 80, 98 re: health legislation.

[49] *GDPR, supra* note 9.

[50] These include the *Brazilian General Data Protection Law* (passed in 2020), Chile's 2018 constitutional guarantee to privacy (yet, this may change as Chile is drafting a new constitution), China's *Personal Information Protection Law of the P.R.C* (passed in 2021), Japan's 2020 amendments to the *Protection of Personal Information Act*, New Zealand's *Privacy Act 2020*, South Korea's 2020 amendments to their *Personal Information Protection Act*, South Africa's *Protection of Personal Information Act, 2013* (passed in 2020) and the United Kingdom's *Data Protection Act* (passed in 2018, a law in identical form to the *GDPR*).

[51] Ben Wolford, "What is GDPR, the EU's new data protection law?" *GPDR.eu*, online: <https://gdpr.eu/what-is-gdpr/>; also see an example of Canadian recognition of the *GDPR*: *Department of Health and Wellness (Re)*, 2018 NSOIPC 12 (CanLII).

specifically to the standards of the *GDPR*: definition of personal information; requirements for the collection, maintenance, and use of data; direction on Information Sharing Agreements; and protection of data subjects' rights.

7. We recommend that the *Privacy Act* update its definition of "personal information" by first, removing the requirement that information must be recorded and second, defining identifiability.[52]

Currently, the *Act* defines personal information as "information about an identifiable individual that is recorded in any form," which is followed by a non-exhaustive list of examples, such as information relating to race, education, blood type, etc.[53]

In contrast, the *GDPR* defines personal information under Article 4 as any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."[54]

The Working Group found two main differences between the Canadian and EU definitions of personal information. First, the Canadian definition requires that the information be recorded. Second, the aspect of "identifiability" is defined in the *GDPR* but not in the *Act*.

Removing the requirement that the information be recorded to be considered personal information is beneficial for two reasons. First, it "reflects the realities of the digital age" where information is often not formally recorded (i.e., if information is viewed but not recorded). Second, privacy concerns are often context-sensitive and should not depend on whether they are recorded.[55]

There are also two reasons in favour of defining "identifiability" like the *GDPR* provides: first, it enables the legislature to provide greater context, and second, it allows the legislature to either make the definition consistent with the jurisprudence or to change it.[56]

---

[52] See also Justice Canada Summary, *supra* note 11 at 7-11.
[53] *Privacy Act*, *supra* note 1 at s 3.
[54] *GDPR, supra* note 9 at Art 4(1).
[55] Justice Canada Summary, *supra* note 11 at 8, citing the Office of the Privacy Commissioner.
[56] *Ibid* at 8.

8. We recommend that the *Privacy Act* be amended to clarify when a government institution can collect personal information.

Section 4 of the *Act* allows the collection of personal information by a government institution only where "it relates directly to an operating program or activity of the institution."[57] This provision is extremely broad. Under Article 6 of the *GDPR*, processing (including collection) of personal data is lawful only if one of six enumerated conditions are met.[58] Some of these grounds include the provision of consent by the data subject, and necessity based on compliance requirements.[59] The Working Group recommends adopting a similar model, whereby the collection of personal information can only be done where it is *necessary* to further an explicit legislative objective. Unnecessary overcollection of personal information is not only redundant and a waste of effort and resources, but also increases risks associated with the potential misuse or misappropriation of such information.

9. We recommend that the *Privacy Act* be reformed to apply the same legal standard to justify the collection, maintenance, use, and disclosure of personal information.

The *Act* currently sets out different criteria to determine when a government institution may collect, use, or disclose personal information.[60] As a result, this creates a confusing patchwork of inconsistent standards. The *GDPR* does not establish different sets of criteria depending on whether collection, use, or disclosure are implicated. Instead, the *GDPR* consolidates these actions under an umbrella term of "processing," defined as including not only acts of collection, use, and disclosure, but also "storage … alteration, retrieval, consultation … [and] erasure," among others.[61] The Working Group recommends adopting a similar umbrella term. The consistent use of one defined term not only streamlines the complexity of the *Act*, but strengthens privacy protections by ensuring the same level of protection applies uniformly.[62]

10. We recommend that the *Privacy Act* be reformed to include enhanced requirements for Information Sharing Agreements between state entities.[63]

---

[57] *Privacy Act*, *supra* note 1 at s 4.
[58] *GDPR, supra* note 9 at Art 6(1)(a)-(f).
[59] *Ibid* at Art 6(1)(a),(c).
[60] *Privacy Act*, *supra* note 1 at ss 4-8.
[61] *GDPR, supra* note 9 at Art 4(2).
[62] *Ibid* at Art 6(1).
[63] See also Justice Canada Summary, *supra* note 11 at 20.

Information Sharing Agreements, which document the terms and conditions of an exchange of personal information between government parties,[64] are not currently regulated by the *Privacy Act*. This needs to change. The transfer of information between state entities must be regulated in order to better protect the fundamental rights of Canadians, ensure broad and consistent protection of private information across entities, and to hold government agencies accountable in this endeavour.[65]

For example, state entities should consider whether the recipient state entity will manage personal information consistent with the principles of (what is currently) the Code of Fair Information Practices (i.e., the *Privacy Act*, sections 4-8), which governs the collection, accuracy, use, disclosure, retention, and disposition of personal information.[66] These principles are based on the internationally accepted "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," which were adopted by the Organisation for Economic Co-operation and Development ("OECD") and accepted by Canada in 1984.[67] The Working Group found that there are currently no specific requirements that a state entity follow these guidelines upon receiving personal data.

In comparison, Articles 44-50 of the *GDPR* extensively cover the transfer of personal information to a third country or international organisation.

Note that this recommendation was previously proposed by the House Committee in 2016, which is further explored in Part V of these submissions.

11. We recommend that the *Privacy Act* be reformed to expand the rights of the data subject by including: (1) the right to erase one's personal data; (2) the right to restrict the processing of one's personal data; (3) the right to be informed about one's personal data; (4) the right to data portability; (5) the right to object to the processing of one's personal data; and (6) the right to not be subject to a decision based solely on automated processing.

---

[64] Treasury Board of Canada Secretariat, "Guidance on Preparing Information Sharing Agreements Involving Personal Information" (July 2010), online: <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html>, s 1.2.

[65] House Committee Report, *supra* note 10 at 11

[66] Treasury Board of Canada Secretariat, *supra* note 64 at s 2.6.

[67] Government of Canada, "Archived - Privacy and Data Protection Guidelines - Roles and Responsibilities" (December 1993), online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=25492&section=html>.

The data subject is the individual whose personal information is collected, stored, and processed.[68] The *Act* fails to include a clearly defined term for such individuals and thus fails to substantively address the rights of the data subject.

Section 12 of the *Privacy Act* accords the right to access one's personal information to Canadian citizens and permanent residents. This right extends to any personal information contained in an information bank or under the control of a government institution "with respect to which the individual is able to provide sufficiently specific information on the location of the information as to render it reasonably retrievable by the government institution."[69] Furthermore, section 12 grants individuals a right to correct an error or omission, requires that a notation be attached to the information reflecting corrections that were requested but not made, and requires that persons or bodies to whom the information is disclosed be notified of the correction or notation.[70]

The Working Group found that these rights are rather minimal and should be expanded, so that individuals can have more control over their personal information. In contrast to the *Act*, the *GDPR* dedicates an entire chapter to data subject rights. Articles 15-22 enumerate eight fundamental rights that data subjects can exercise. These rights without an equivalent in the *Privacy Act* are: (1) the right to erase one's personal data; (2) the right to restrict the processing of one's personal data; (3) the right to be informed about one's personal data; (4) the right to data portability; (5) the right to object to the processing of one's personal data; and (6) the right to not be subject to a decision based solely on automated processing.[71]

Rights of the data subject should be adequately protected and enshrined in an amended *Act,* following the *GDPR* as an example. The rights of the data subject notably will empower individuals with control over their personal data.

Recommendations Based on the UK's *Data Protection Act*

When comparing the UK's *Data Protection Act* to Canada's *Privacy Act,* the Working Group found a large gap in Canada's protection of individuals' personal information within law enforcement settings.

---

[68] See *GDPR, supra* note 9 at Art 4(1).

[69] *Privacy Act*, *supra* note 1 at s 12(1)(b). Note that foreign nationals, and not only Canadian citizens and permanent residents, now have a right to access personal information under the *Privacy Act*: Office of the Privacy Commissioner, "Foreign nationals now have right to access personal information under *Privacy Act*" (July 2022), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/an_220713/>.

[70] *Privacy Act, supra* note 1 at s 12(2)(a)-(c).

[71] *GDPR, supra* note 9 at Arts 17-22.

12. We recommend that the *Privacy Act* be reformed to regulate the transfer of personal data to law enforcement entities consistent with the UK's *Data Protection Act*.

Part 3 of the UK's *Data Protection Act* is entirely devoted to the processing of personal information in law enforcement settings.[72] This UK legislation sets out different principles governing the usage of personal data by law enforcement, which are more stringent when compared to non-law enforcement related uses. In contrast, the Working Group found that Canada's *Privacy Act* contains few references to how personal information may be used specifically by law enforcement.

For example, Chapter 2 of Part 3 of the *Data Protection Act* lays out six data protection principles that are unique to law enforcement settings, summarised in the statute as follows:

> "(a) section 35(1) sets out the first data protection principle (requirement that processing be lawful and fair);
>
> (b) section 36(1) sets out the second data protection principle (requirement that purposes of processing be specified, explicit and legitimate);
>
> (c) section 37 sets out the third data protection principle (requirement that personal data be adequate, relevant and not excessive);
>
> (d) section 38(1) sets out the fourth data protection principle (requirement that personal data be accurate and kept up to date);
>
> (e) section 39(1) sets out the fifth data protection principle (requirement that personal data be kept for no longer than is necessary);
>
> (f) section 40 sets out the sixth data protection principle (requirement that personal data be processed in a secure manner)."[73]

The Working Group strongly recommends that the *Act* be amended to better regulate the transfer of personal data to law enforcement agencies so that it is consistent with the UK's stringent and robust *Data Protection Act*.

[72] *Data Protection Act 2018* (UK), Part 3.
[73] *Ibid* at s 34(1).

PART V: Recommendations Based on the 2016 House Committee Report

This section provides recommendations based on information already available to the House Committee. While Canadian case law and international instruments are helpful to guide potential amendments, they are not the only sources of information available. The Government has considered reforming the *Privacy Act* in the past, going beyond Justice Canada's most recent public consultation from 2020 to 2021.[74] Specifically, in 2016, the House Committee released *Protecting the Privacy of Canadians: Report of the Standing Committee on Access to Information, Privacy and Ethics* (the "House Committee Report"). This report contained recommendations on reforming the *Privacy Act* based on consultations with experts and other stakeholders.[75]

The Working Group urges the House Committee to review the House Committee Report and consider its recommendations in light of the upcoming reform. Several recommendations from the House Committee Report re-emerged in part or in whole in Justice Canada's 2021 *What We Heard Report: Justice Canada's Online Public Consultation on Privacy Act Modernization* (the "Justice Canada Summary"). This includes recommendations related to the transparency of Information Sharing Agreements and new punitive mechanisms for failures to protect personal information.[76] The Working Group further urges the Government to consider recommendations from the House Committee Report that are absent from the Justice Canada Summary, lest they be overlooked in the upcoming reforms.

13. We recommend the *Privacy Act* cover all federal government institutions.

In order for the *Privacy Act* to sufficiently protect Canadians' personal information, the Working Group urges that the *Act* must apply to all federal government institutions. The House Committee had previously recommended exploring the extension of the *Privacy Act*'s coverage to include all federal government institutions.[77] This would include ministers' offices and the Prime Minister's Office, which currently fall outside the *Act*'s purview.[78] These executive branch offices not only exercise significant authority, but also collect personal information similar in nature to what government bureaucracies collect.

---

[74] Department of Justice Canada, "Modernizing Canada's Privacy Act – Engaging with Canadians", *supra* note 3.
[75] House Committee Report, *supra* note 10.
[76] *Ibid* at 16, 10-13; Justice Canada Summary, *supra* note 11 at 12, 16-17.
[77] House Committee Report, *supra* note 10 at 60.
[78] *Ibid* at 58-60.

The collection of Canadians' personal information by the executive branch deserves greater care and scrutiny given its proximity to the decision-making apparatus.[79] For example, while most government departments are required to comply with the *Privacy Act* when handling personal information (which would ideally better protect *Charter* rights after a reform), the Prime Minister's Office is currently under no obligation to comply with the safeguards of the *Act*. It thus could implement policies for handling personal information in ways that may infringe Canadians' *Charter* rights.[80] There is no principled basis to have different privacy protections based only on which office or department is handling the personal information.[81]

14. Following the House Committee Report, the Privacy Commissioner should be provided three new institutional mechanisms to uphold *Privacy Act* requirements: (1) the implementation of "privacy impact assessments;" (2) an ongoing five-year parliamentary review of the *Privacy Act*; and (3) the implementation of Information Sharing Agreements.

Another key set of recommendations from the House Committee Report involves new institutional mechanisms through which the Privacy Commissioner could enforce *Privacy Act* requirements. The House Committee Report called for: (1) "privacy impact assessments" on new federal initiatives; (2) an ongoing five-year parliamentary review of the *Act*; and (3) the implementation of Information Sharing Agreements.[82] The Working Group found that these recommendations were not substantially referenced in the Justice Canada Summary, apart from passing remarks with respect to (1) and (3). The Working Group urges that all three recommendations be followed.

Each of these three new requirements would allow the Privacy Commissioner to advise government stakeholders on how changes to the *Act* may impact the collection, retention, and deletion of personal information.

First, by implementing privacy impact assessments ("PIAs"), potentially adverse privacy impacts could be pre-emptively flagged so that appropriate measures could be taken to avoid unintended adverse consequences.[83] Under a PIA requirement, government institutions subject to the *Privacy Act* that are considering an initiative that will impact privacy would be required to identify the privacy risks associated with the initiative and set out plans for mitigating those risks. One useful example of a PIA

[79] House Committee Report, *supra* note 10 at 59, citing Professor Michael Geist of the University of Ottawa.
[80] *Ibid* at 58-60.
[81] *Ibid*.
[82] *Ibid* at 10-14, 39-42, 48-49.
[83] *Ibid* at 39-42.

requirement can be found in the Treasury Board's Directive on Privacy Impact Assessment (the "Directive"). Under the Directive, government institutions that plan to use personal information in a project must submit a PIA to the Office of the Privacy Commissioner ("OPC").[84] Government institutions face a similar requirement to submit a new PIA when considering substantial modifications to such projects.[85] The Directive further specifies various risk factors that the PIA must analyse, like the number of people impacted and the type of personal information at issue.[86] This analysis of risk factors must be made available to the public.[87] The PIA must further identify the specific ways in which the institution will ensure compliance with obligations under the *Privacy Act*.[88]

While the Directive is a useful model for structuring a PIA and helps improve government accountability for conducting privacy assessments, more work is required. The Directive provides limited recourse for non-compliance,[89] and the implementation of PIAs was described in the House Committee Report as "uneven."[90] Further, the Privacy Commissioner has urged that creating a legal requirement to implement PIAs under the *Privacy Act* would promote more timely and higher-quality PIAs than those prepared under the Directive.[91]

Second, the House Committee Report recommended the *Privacy Act* be amended to require an ongoing five-year parliamentary review.[92] The House Committee Report determined that an ongoing review was required to ensure that the *Act* is consistently updated to respond to technological developments.[93] The need for periodic review is evidenced by the current state of the *Privacy Act*, which fails to account for nearly 40 years of technological and constitutional advances, especially with respect to the internet and social media. Implementing a process which ensures regular review of the *Privacy Act* would help prevent its provisions from becoming antiquated in the future and is a suggestion endorsed by the Working Group.

---

[84] House Committee Report, *supra* note 10 at 39-40.
[85] See the Treasury Board of Canada Secretariat: *Directive on Privacy Impact Assessment* (Ottawa, 2010) online: *Treasury Board Secretariat* <www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308&section=html> at Appendix C, s II [Treasury Board Directive on PIA].
[86] *Ibid*.
[87] *Ibid* at s 6.3.16.
[88] *Ibid* at Appendix C, Section V.
[89] Treasury Board of Canada Secretariat, *Policy on Privacy Protection* (Ottawa, 2022), online: *Treasury Board Secretariat* <www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12510> at s 7.
[90] *House Committee Report*, *supra* note 10 at 40, citing the Privacy Commissioner's evidence.
[91] *Ibid*.
[92] *Ibid* at 60.
[93] *Ibid*.

Further, mandating parliamentary review periods would help increase the likelihood of the *Act's* ongoing *Charter* compliance, relieving some pressure off Canada's courts. The legislature can play a role with respect to the constant evolution of Canadian society and the judiciary's interpretation of the *Charter* given Canada's "living tree" Constitution: the core of the "living tree" doctrine is the courts' recognition that the Constitution and its interpretation "[accommodate] and [address] the realities of modern life."[94] Modern life now includes the proliferation of personal information handled, retained, and processed by government entities, and the privacy interests that these activities implicate.

Third, regarding Information Sharing Agreements, information-sharing poses particular risks, especially since information passed to law enforcement agencies in Canada and abroad could engage sections 7 and 8 of the *Charter*, as discussed in part III of these submissions. The current absence of information-sharing documentation—that would explain what information is shared, with whom it is shared, and how it is transmitted—hinders the Privacy Commissioner's ability to hold government agencies accountable for non-compliance with the *Privacy Act*.[95] Moreover, any potential *Charter* challenges would face significant evidence-gathering issues without comprehensive and substantive documentation and record management policies, as already alluded to in Part III of these submissions. As previously mentioned in Part IV of these submissions, the *GDPR* has more robust provisions regarding Information Sharing Agreements. Along with the aforementioned case law in Part III of these submissions, we have recently witnessed further consequences of the absence of an overarching and robust codification of Information Sharing Agreements and policies: potato farmers in Prince Edward Island have alleged in a lawsuit against the federal government filed in late 2022 that the Canada Revenue Agency illegally shared the plaintiffs' tax information with Environment and Climate Change Canada.[96]

The Working Group urges that the House Committee Report and the Justice Canada Summary be read in complement with each other. The Justice Canada Summary expands on some of the topics from the earlier House Committee Report, most notably by incorporating consultations with Indigenous communities likely to be impacted by changes to the *Privacy Act*. However, it is also missing much of the nuance from the House Committee Report that ought to be carefully considered.[97]

---

[94] *Reference re Same-Sex Marriage*, 2004 SCC 79 at para 22, citing *Edwards v Canada*, [1930] 1 DLR 98 at 107, [1929] All ER Rep 571 [*Edwards, 1930*]; see also *Edwards, 1930* at 106.
[95] House Committee Report, *supra* note 10 at 10-13.
[96] CBC News, "P.E.I. Potato Farmers Sue Federal Government Over Release of Tax Information", *CBC News* (9 December 2022), <https://www.cbc.ca/news/canada/prince-edward-island/pei-tax-farm-docherty-skye-view-lawsuit-1.6680758>.
[97] Justice Canada Summary, *supra* note 11 at 19-21.

An Alarming Overemphasis on Internal Views

In lieu of some of the missing valuable recommendations made in the House Committee Report, and by other individual contributors to the public consultation, the Justice Canada Summary instead paid disproportionate attention to submissions by affiliated institutions like the OPC.

Throughout both the Justice Canada Summary and the House Committee Report, submissions from the OPC played an outsized role in their analysis. In the Justice Canada Summary, nearly every topic addressed included a review of the OPC's perspective, and the recommendations generally conformed to the OPC's input.[98] The Working Group recognizes and appreciates the key role that the OPC plays in public policy with respect to privacy law and its unique perspective on the powers that would help it effectively protect Canadians' information. We are not suggesting that the OPC's recommendations be downplayed or downgraded. Instead, the Working Group stresses that the perspectives of advocates, academics, and other stakeholders must be carefully considered alongside the OPC's submissions, especially when considering what powers the OPC should be granted.

This imbalance in views was made clearer after Justice Canada released the individual written submissions made by members of the public who consented to their release.[99] The Justice Canada Summary often refers to the OPC, Office of the Information Commissioner of Canada, and Canadian Bar Association by name when referring to those groups' submissions, but refers to most other parties as "other stakeholders."[100] Other than some stakeholders who wished to anonymize their submissions, references to some groups by name and other non-anonymous contributors simply as "others" creates an appearance of deprioritizing input from the "other" groups.

In particular, the Working Group would like to highlight the submission of Professor Lisa Austin of the University of Toronto Faculty of Law and Professor Andrea Slane of Ontario Tech University.[101] Among many other important thoughts, Professors Austin and

[98] See for example, Justice Canada Summary, *supra* note 11 at 7, 11, 15.
[99] Department of Justice Canada, "Public Consultation on the *Privacy Act* - Submissions" (last modified 30 November 2021), online: *Department of Justice Canada* <https://justice.canada.ca/eng/csj-sjc/pa-lprp/sub-sou/index.html>.
[100] For example, see Justice Canada Summary, *supra* note 11 at 13 ("Charting a Path Forward"), 16 ("Clarifying the Role of the Privacy Commissioner"), 18 ("Applying all the Privacy Act's Rules to 'Publicly Available' Personal Information").
[101] Lisa M Austin and Andrea Slane, February 14, 2021, submission reproduced in Department of Justice Canada, "Public Consultation on the *Privacy Act* - Submission - Lisa M. Austin and Andrea Slane" (last modified 30 November 2021), online: *Department of Justice Canada* <https://justice.canada.ca/eng/csj-sjc/pa-lprp/sub-sou/austinslane.html>. Note that Professor Lisa Austin is also the Working Group's Faculty Advisor.

Slane recommended omitting any law enforcement and national security exemptions to several provisions of the *Act*, especially as they relate to transparency and accountability requirements. Exempting law enforcement from requirements that promote accountability and transparency goes against the public interest in maintaining proper civilian oversight of law enforcement activities, a principle which was recognized by the SCC in *R v Mentuck* (2001).[102] The Justice Canada Summary almost entirely omits this view. In fact, the opposing view *supporting* exceptions for law enforcement exception is mentioned at least three times in relation to publicly available information,[103] personal information principles,[104] and transparency.[105] Professors Austin and Slane's input is relegated to one sentence alluding to "concerns" by some stakeholders over this exception.[106]

Moreover, while the Justice Canada Summary purports to incorporate public consultation, the data reveal that 40 per cent of the online survey respondents worked with the *Privacy Act* in a professional capacity.[107] Such a disproportionate share of feedback suggests that the survey results are potentially biased toward the views of privacy professionals in the government and supporting industries, which may not correspond with broader public sentiment. The Working Group understands that those who work closely with the *Act* likely have a level of expertise and perspective that make their input uniquely relevant and valuable for the purpose of the reform, and acknowledges that issues like *Privacy Act* reform do not typically attract popular public attention. That said, there must be a greater effort made to include broader public input, and more thoughtful analysis on how the *Act* and potential reform can impact the majority of individual Canadians who opted not to contribute.

The Justice Canada Summary suggests that the government may not be taking full stock of the situation, which raises genuine questions as to whether the *Privacy Act* reform can live up to its constitutional and privacy-protecting obligations.

[102] *Ibid* at Heading 7, citing *R v Mentuck*, 2001 SCC 76.
[103] Justice Canada Summary, *supra* note 11 at 9-10.
[104] *Ibid* at 10.
[105] *Ibid* at 15.
[106] *Ibid* at 18.
[107] *Ibid* at 25.

PART VI: A Note on the Working Group's Experience with Access to Information

Finally, the Working Group would like to bring to the House Committee's attention some of the issues that arose during the preparation of these submissions. For Canadians and other stakeholders to hold policymakers accountable, there must be relative ease in obtaining, accessing, and reviewing information held by the Government in an efficient and transparent manner.

During the research period for our submissions, a member of the Working Group, with the assistance of the David Asper Centre for Constitutional Rights, submitted an Access to Information Request for the particulars of the public consultation by Justice Canada. Specifically, the Working Group requested the survey data and the individual written submissions solicited by Justice Canada during the consultation period.

Although we initially received a prompt response from officials, the Working Group ultimately obtained only a portion of the requested materials due to what appeared to be an unfortunate miscommunication related to a prior Access to Information request submitted by a third-party with respect to the same or similar information. Although Justice Canada provided the Working Group with the information on the survey results, it never provided the individual written submissions, nor did it explain their absence. Regrettably, the Working Group was unable to reach a resolution directly with the Access to Information officials, despite several attempts over email. Ultimately, the Working Group submitted a formal complaint for the failure to respond to the full request, but the complaint was rejected due to the statutory limitations period.

It was only by chance that the Working Group eventually discovered that an assortment of the requested written submissions had been made publicly available by Justice Canada.[108] The Working Group was never advised by Justice Canada of their release (or their impending release, if that was the case depending on timing) at any time before or after the original Access to Information request, despite having originally requested these specific materials.

Therefore, **the Working Group additionally recommends that the Government review their processes and policies with respect to their communications and services related to Access to Information requests**, such that these requests are dealt with more expediently and transparently. This ensures Canadians can continue to not only hold the government accountable, but that individuals, institutions, and stakeholders can provide relevant and substantive feedback to policymakers, especially when constitutional rights are implicated.

[108] Department of Justice Canada, *supra* note 99.

PART VII: Conclusion

Canada's *Privacy Act* first came into force in 1983. After 40 years, much has changed while the *Act* remains substantially the same. The world has shifted into a predominantly digital realm, and government agencies can more easily collect, store, and share Canadians' personal information. In light of these changing realities, the *Act* must be reformed to continue to adequately protect and respect the privacy rights of Canadians.

The right to privacy has been recognized by the highest court in the nation as essential to human dignity and at the heart of liberty in a modern liberal state. Despite this, the *Act* as it stands fails to comply with or reflect the spirit of constitutionally protected *Charter* rights. Canadians should not have to wait for the courts to protect their privacy rights and correct legislative oversights.

Further, other states have moved ahead with their public-facing privacy legislation, better protecting the privacy rights of individuals compared to Canada. The House Committee must act swiftly to ensure Canada catches up to the rest of the world in better protecting privacy rights and giving our courts more robust legislation to work with.

The Working Group has presented 14 recommendations for the reform of the *Act,* highlighting the key provisions and areas where attention is needed most. Given the nature of privacy rights as being fundamental rights, there must be transparency at all levels of the decision-making process for the reform of the *Act.* Notably, minority groups in Canada must be consulted.

Respectfully, we urge the House of Commons Standing Committee on Access to Information, Privacy and Ethics, the Office of the Privacy Commissioner of Canada, and the Office of the Information Commissioner of Canada to heed the Working Group's recommendations as they work towards modernising the *Privacy Act*.

Bibliography

LEGISLATION: CANADA

Canadian Charter of Rights and Freedoms, Part I of the *Constitution Act, 1982,* being Schedule B to the *Canada Act 1982* (UK)*,* 1982, c 11.

Privacy Act, RSC 1985 c P-21.

LEGISLATION: FOREIGN

Data Protection Act 2018 (UK).

EC, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), [2016] OJ, L 119/1, online: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>.

JURISPRUDENCE

Bernard v Canada (Attorney General), 2014 SCC 13.

Chaoulli v Quebec (Attorney General), 2005 SCC 35.

Cheskes v Ontario (Attorney General), 2007 CanLII 38387 (ONSC), 288 DLR (4th) 449.

Department of Health and Wellness (Re), 2018 NSOIPC 12 (CanLII).

Edmonton Journal v Alberta (Attorney General), [1989] 2 SCR 1326.

Edwards v Canada, [1930] 1 DLR 98 at 107, [1929] All ER Rep 571.

M. (A.) v Ryan, [1997] 1 SCR 157, 143 DLR (4th)

R v Baldovi, 2016 MBQB 221.

R v Beare; *R v Higgins*, [1988] 2 SCR 387, 55 DLR (4th) 481.

R v Cole, 2012 SCC 53.

R v Dyment, [1988] 2 SCR 417, [1988] SCJ No 82.

R v Edwards, [1996] 1 SCR 128, [1996] SCJ No 1.

R v Finnegan, 2014 ONSC 2032.

R v Flintroy, 2018 BCSC 1777.

R v Flintroy, 2019 BCSC 213.

R v Gowdy, 2016 ONCA 989.

R v JJ, 2022 SCC 28.

R v Mentuck, 2001 SCC 76.

R v Morgentaler, 1988 CanLII 90 (SCC), [1988] 1 SCR 30.

R v Plant, [1993] 3 SCR 281, 84 CCC (3d) 203.

R v Sharpe, 2001 SCC 2.

R v Stucky, 2006 CanLII 588 (ONSC), [2006] OJ No 108.

Reference re Same-Sex Marriage, 2004 SCC 79

Ruby v Canada (Solicitor General), 2002 SCC 75.

Wakeling v United States of America, 2014 SCC 72.

SECONDARY MATERIALS

Alessandro Blasimme et al., “Data Sharing For Precision Medicine: Policy Lessons And Future Directions” (2018) 37:5 Health Affairs 702.

Andrea Riccardo Migone, “Trust, but Customize: Federalism’s Impact on the Canadian COVID-19 Response” (2020) 39:3 Policy and Society 382.

Ben Wolford, “What is GDPR, the EU’s new data protection law?” *GPDR.eu*, online: <https://gdpr.eu/what-is-gdpr/>.

CBC News, “P.E.I. Potato Farmers Sue Federal Government Over Release of Tax Information” *CBC News* (9 December 2022), <https://www.cbc.ca/news/canada/prince-edward-island/pei-tax-farm-docherty-skye-view-lawsuit-1.6680758>.

Department of Justice Canada, “Modernizing Canada’s Privacy Act – Engaging with Canadians” (March 2022), online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/index.html>.

Department of Justice Canada, “Modernizing Canada’s Privacy Act” (September 2021), online: <https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/modern.html>.

Department of Justice Canada, “Public Consultation on the *Privacy Act* - Submissions” (last modified 30 November 2021), online: *Department of Justice Canada* <https://justice.canada.ca/eng/csj-sjc/pa-lprp/sub-sou/index.html>.

Department of Justice Canada, “Public Consultation on the *Privacy Act* - Submission - Lisa M. Austin and Andrea Slane” (last modified 30 November 2021), online: *Department of Justice Canada* <https://justice.canada.ca/eng/csj-sjc/pa-lprp/sub-sou/austinslane.html>.

Department of Justice Canada, *Modernizing Canada’s Privacy Act: What We Heard Report: Justice Canada’s Online Public Consultation on Privacy Act Modernization*, Catalogue No J2-494/1-2021E-PDF (Ottawa: Department of Justice Canada, 2021), online: <https://justice.canada.ca/eng/csj-sjc/pa-lprp/wwh2-cqnae2/pdf/wwhr_pam_2021_en2.pdf>.

Government of Canada, “Archived - Privacy and Data Protection Guidelines - Roles and Responsibilities” (December 1993), online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=25492&section=html>.

Government of Canada, “Section 8 – Search and seizure” (June 2022), online: Government of Canada <https://www.justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art8.html>.

House of Commons, *Protecting the Privacy of Canadians: Review of the Privacy Act: Report of the Standing Committee on Access to Information, Privacy and Ethics* (December 2016) (Chair: Blaine Calkins), online: <https://publications.gc.ca/collections/collection_2016/parl/xc73-1/XC73-1-1-421-4-eng.pdf>.

Office of the Privacy Commissioner, “Foreign nationals now have right to access personal information under *Privacy Act*” (July 2022), online: <https://www.priv.gc.ca/en/opc-news/news-and-announcements/2022/an_220713/>.

The Honourable Jody Wilson-Raybould, *Letter to Blaine Calkins, Chair of the Standing Committee on Access to Information, Privacy, and Ethics*, April 12, 2017, online: <https://www.ourcommons.ca/Content/Committee/421/ETHI/GovResponse/RP8892754/421_ETHI_Rpt04_GR/421_ETHI_Rpt04_GR-e.pdf>.

Treasury Board of Canada Secretariat, “Guidance on Preparing Information Sharing Agreements Involving Personal Information” (July 2010), online: <https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/privacy/guidance-preparing-information-sharing-agreements-involving-personal-information.html>.

Treasury Board of Canada Secretariat, *Directive on Privacy Impact Assessment* (Ottawa, 2010) online: *Treasury Board Secretariat* <www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=18308&section=html>.

Treasury Board of Canada Secretariat, *Policy on Privacy Protection* (Ottawa, 2022), online: *Treasury Board Secretariat* <www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=12510>.