CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission to the Special Committee to Review the *Freedom of Information and Protection of Privacy Act* (British Columbia)

March 31, 2022

Tom Naciuk, JD
Public Interest Articling Fellow

Brenda McPhail, PhD
Director, Privacy, Technology & Surveillance Program

Canadian Civil Liberties Association
400-124 Merton Street
Toronto, ON M4S 2Z2
Phone: 416-363-0321
www.ccla.org

I. Introduction

The Canadian Civil Liberties Association ("CCLA") is an independent, national, nongovernmental organization that was founded in 1964 with a mandate to defend and foster the civil liberties, human rights, and democratic freedoms of all people across Canada. Our work encompasses advocacy, research, and litigation related to the criminal justice system, equality rights, privacy rights, and fundamental constitutional freedoms. Working to achieve government transparency and accountability with strong protections for personal privacy lies at the core of our mandate.

The CCLA believes that a strong access to information regime is crucial to a vibrant democracy. Information about how our government functions assists the populace in making informed choices at the ballot box, participating meaningfully in policy discussions, and is a way to ensure that those in government are held accountable for their decisions. Our Supreme Court has affirmed that Canadians' right to information is derived from freedom of expression protected under the *Canadian Charter of Rights and Freedoms.*[1] This right is engaged when meaningful expression on the functioning of government cannot be undertaken without access to information. The *Charter* also protects privacy, under section 8 (search and seizure) as well as section 7 (legal rights).[2] Section 8 is engaged whenever the state intrudes upon a person's reasonable expectation of privacy without proper legal authority or conducts a search in an unreasonable manner.[3] As for section 7, the right to liberty includes the freedom to make important life choices free from interference by the state, and inherent in this freedom is some measure of personal privacy.[4]

Furthermore, the CCLA believes that a healthy democracy must counterpoise the right of access to information with the privacy rights of individuals, striking a principled balance between the two. Without meaningful access to information, democracy is threatened: access to information under the state's control is necessary to countermand the proliferation of misinformation and disinformation, especially online, and as a pre-condition for informed choice and democratic expression. On the other hand, privacy has inherent value; the human condition flourishes as the fear of state intrusion fades.[5] An unfettered right of access leaves no room for personal privacy, or for any of the other rights and freedoms in a democracy that depend on some measure of informational privacy, including substantive equality and freedom of thought. In the opposite extreme, an unfettered right to informational privacy poses an entirely different risk to democracy, e.g., when information is kept secret owing to personal information that would otherwise be in the public interest to disclose, democratic expression is limited when the state relies on this information to make an important decision. A healthy democracy must find a stable balance that values access to information and informational privacy equally: the point of equilibrium where democratic society thrives, sustained by the freedoms afforded by individual privacy.

---

[1] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23 at paras 36-40.
[2] *Canadian Charter of Rights and Freedoms*, ss 7-8, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11.
[3] *R v Caslake*, [1998] 1 SCR 51 at paras 10-11.
[4] *Association of Justice Counsel v Canada (Attorney General)*, 2017 SCC 55 at para 49.
[5] *R v Ahmad*, 2020 SCC 11 at para 38.

British Columbia's *Freedom of Information and Protection of Personal Privacy Act* has strayed from this equilibrium. FIPPA is being quickly side-lined as changes in technology outpace developments in the law, threatening to make it and other privacy and access to information statutes in Canada obsolete. Social media platforms have become gold mines of personal information, prized not only by the private sector, but also by the state. Advances in technology have made the large-scale collection of personal information easier than ever, and readily adaptable to evolving forms of data. In today's data-driven world, for almost any person, the state can conceivably access some combination of facial images, personal or familial DNA, fingerprints, financial and employment information, health and driving information, biometric data, location, criminal record, vital statistics, known associates (social network), and subscriber-device pairings, often with corresponding metadata or linked to other data points. The Internet has expanded the state's reach enormously and provides a wealth of information, openly accessible to the government, or available for purchase, e.g., social media, genealogy websites, web crawling and data scraping. Of course, this is in addition to the government's own records and databases. The commodification of data and public-private surveillance partnerships today have exceeded the upper limits of FIPPA's legislative design.

Like other access to information laws in Canada, under FIPPA, there is a drastic imbalance in the enormous availability of personal information to the state, compared to the information available to its residents on the particulars of its collection, use, and disclosure of personal information. When used to train artificial intelligence systems for algorithmic profiling or automated decision-making, these vulnerabilities pose even greater risks to rights and freedoms.[6] The social and historical context of systemic discrimination influences the reliability of any AI system that uses law enforcement data sets (arrests and criminal records) for training purposes.[7] Predictive policing or automated decision-making relying on this information is therefore likely to exhibit the same biases, jeopardizing equality rights and transparency.[8] Similarly, privacy rights and freedom of expression are jeopardized by algorithmic surveillance in public places or online, and the chilling effect of limiting opportunities for anonymous expression. These burdens are experienced disproportionately by marginalized communities. Nevertheless, access to information on how this data is being used and collected by the state, including for algorithmic policing, is severely limited.[9] In short, FIPPA must be part of the solution, not the problem.

Privacy law and access laws in Canada, including British Columbia, are quickly being left behind as other jurisdictions modernize their laws to keep pace with technological developments. In 2018, the European Union's *General Data Protection Regulation* (GDPR) came into force, setting a new gold standard for privacy law and data security around the world. In December 2021, the Special Committee of the Legislative Assembly of British Columbia to Review the *Personal Information Protection Act*, in its report, "stressed the importance of alignment and harmonization with the changing federal, provincial and international privacy landscape, including the European Union's [GDPR]."[10] Previously, in July 2021, on behalf of the CCLA, Dr. Brenda McPhail

[6] Citizen Lab, *To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto: University of Toronto, 2020), online: <citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.
[7] *Ibid* at 3.
[8] *Ibid*.
[9] *Ibid* at 2.
[10] British Columbia, Special Committee to the Review the Personal Information Protection Act, *Modernizing British Columbia's Private Sector Law* (December 2021) (Chair: Mable Elmore) at 6.

appeared before the Special Committee to make recommendations for the reform of PIPA, FIPPA's private sector equivalent in BC.[11] This included support for many of features of the GDPR.[12] The present review of FIPPA is an opportunity to introduce similar advancements in BC's public sector law, and to modernize even further.

A coordinated approach is key to re-imagining privacy and access to information laws in Canada to meet the demands of the globalized, data-driven word of today. The patchwork of privacy and access to information laws in Canada – public and private sector legislation, enacted in both the provincial and federal spheres – are only as strong as the weakest link. The federal government and several other provinces have, to varying extents, taken steps to modernize their own laws, for both the public and private sectors. For instance, in 2021, the federal government undertook a review of the *Privacy Act*, which regulates how federal public sector institutions collect, use, disclose, retain, and dispose of the personal information of individuals.[13] In an apparent response to the GDPR, and to continue meeting European standards for data exchange, the federal government also tabled Bill C-11 in November 2020, which proposed replacing PIPEDA with a new *Consumer Privacy Protection Act*.[14] Although the bill died on the order paper with the prorogation of the 43rd Parliament, it is widely anticipated that the federal government will re-introduce the bill. In Quebec, significant progress has been made with the passage of Bill 64 in September 2021, making a host of changes to Quebec privacy law coming into force in 2023, including a requirement to appoint a Privacy Officer and a new breach notification requirement.[15] In 2024, further amendments will take effect in Quebec, including a data portability right.[16] Public sector legislation, such as FIPPA, must be at least as strong – and consistent with – private sector legislation, and ensure privacy standards are maintained across jurisdictional and regulatory lines. The present review is an opportunity to consider FIPPA's place in a broader system of interlocking privacy and access to information laws.

The CCLA also recognizes the progress that has been made since the last review of FIPPA in May 2016. On November 25, 2021, Bill 22 received Royal Assent, making numerous amendments to FIPPA.[17] For instance, the CCLA welcomes the addition of a mandatory breach notification and reporting framework to FIPPA, as well as the requirement that public bodies must have a privacy management program.[18] The CCLA similarly recognizes long-standing innovative features of BC access to information and privacy law, including a public interest override for disclosure.[19] These are important steps towards modernization but are far from sufficient.

---

[11] *Ibid* at 51.
[12] Legislative Assembly of British Columbia, Special Committee to Review the Personal Information Protection Act, *Evidence*, 42-2, No. 9 (7 July 2021) at 9:05am (Dr. Brenda McPhail).
[13] Government of Canada, "Modernizing Canada's *Privacy Act* – Online Public Consultation" (last modified 1 September 2021), online: <justice.gc.ca/eng/csj-sjc/pa-lprp/opc-cpl.html>.
[14] Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading in the House of Commons on 17 November 2020, died on the order paper after prorogation).
[15] Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2020 (Royal Assent granted 22 September 2021), SQ 2021, c 25.
[16] *Ibid*.
[17] Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021*, 2nd Sess, 42nd Parl, British Columbia (Royal Assent granted 25 November 2021), SBC 2021, c 39.
[18] *Ibid*, s 25, inserting Division 4 to Part 3 of *FIPPA*.
[19] *FIPPA*, s 25.

While there is a long list of reforms that can and should be made to our system, the CCLA has focused in this brief on five main issues:

1) The need for a statutory duty to document;
2) The need to expand the scope of the Act;
3) The need to ensure equitable access and to address the unreasonable delays associated with the access regime
4) The need for modernization to respond to emerging technologies and the commodification of data:
    a. the collection, use, and disclosure of biometric information
    b. the use of artificial intelligence technologies by public bodies
    c. the collection, use, and disclosure of de-identified information
5) The need to strengthen data residency requirements

The CCLA makes the following eleven recommendations:

Recommendation 1: The Government should adopt legislation requiring public servants, government officials and other entities subject to FIPPA to document and retain records relating to their deliberations, actions, and decisions and adopt appropriate oversight and enforcement mechanisms.

Recommendation 2: The Government should adopt legislation that prescribes record management systems be designed to facilitate the right of access.

Recommendation 3: Reformulate the definition of "public body" using a criteria-based definition rather than allowing the government to designate specific agencies, boards, commissions, and corporations by regulation.

Recommendation 4: Amend Section 13 of FIPPA to narrow the scope of the policy "advice" and "recommendations" discretionary exemption.

Recommendation 5: Amend Section 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timeline for responding to access requests.

Recommendation 6: Amend Section 75 to make fee waivers available as a matter of course, without the applicant having to make a specific request, when there is significant public interest in disclosure.

Recommendation 7: Amend FIPPA to explicitly recognize privacy as a human right in its statement of purpose.

Recommendation 8: Amend FIPPA to codify a presumption that biometric data is quintessentially private data. It would be beneficial for the Committee to engage in a specific analysis of the privacy risks of biometric identifiers to identify additional principled and proactive protections that may be required and could be addressed by FIPPA amendments.

Recommendation 9: Amend FIPPA to contain a right of individuals to be informed about the use of automated decision-making processes they are subject to, a right to object to automated decision-making, and a right to correct personal information used to make decisions about them.

Recommendation 10: Amend FIPPA to cover all "de-identified data," as well as introduce appropriate definitions, enforcement, and accountability mechanisms.

Recommendation 11: Amend FIPPA to include minimum requirements for the storage of personal information outside Canada by public bodies, such as by permitting data storage or disclosure outside of Canada only in jurisdictions with substantially similar privacy laws.

II. A duty to document

Recommendation 1: The Government should adopt legislation requiring public servants, government officials and other entities subject to FIPPA to document and retain records relating to their deliberations, actions, and decisions and adopt appropriate oversight and enforcement mechanisms

A meaningful right of access to information is dependent on the existence of adequate documentation of government actions and decisions and the retention of these records.[20] When actions and decisions are not documented properly, or at all, there are no records to provide a requester with concerning a specific government action or decision.

According to the federal Office of the Information Commissioner, the absence of records can be attributed to two main factors. First, the use of new communication technologies has added a layer of complexity to information management.[21] The use of multiple systems has created duplicate records, and copies and versions of the same record may be stored on multiple platforms, making retrieval more difficult.[22] Second, a lack of stringency in the documenting of actions and decisions by institutions has exacerbated this issue.[23]

British Columbia should adopt stand-alone legislation, or amend FIPPA, to create a statutory duty for public servants, government officials and other entities subject to FIPPA to document and retain records relating to their deliberations, actions, and decisions.[24] For example, in New Zealand, the *Public Records Act 2005* requires every public office and local authority to "create and maintain full and accurate records of its affairs, in accordance with normal, prudent

[20] British Columbia, Office of the Information and Privacy Commissioner, *Submissions to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (Victoria: OIPC, 2015) at 5.
[21] Canada, *Observations and Recommendations from the Information Commissioner on the Government of Canada's Review of the Access to Information Regime* (Gatineau: Office of the Information Commissioner, January 2021) at 8.
[22] *Ibid*.
[23] *Ibid* at 7.
[24] British Columbia, Office of the Information and Privacy Commissioner, *Submissions to the Special Committee to Review the Freedom of Information and Protection of Privacy Act* (Victoria: OIPC, 2015) at 5.

business practice, including the records of any matter that is contracted out to an independent contractor."[25]

To be effective, this statutory duty must be accompanied by independent oversight and enforcement measures. The OIPC's jurisdiction should be expanded to include overseeing the record keeping practices of institutions subject to FIPPA, including auditing powers. As for ensuring compliance, the Government should enact a new offence for intentionally failing to create and retain adequate records in contravention of the Act.

Recommendation 2: The Government should adopt legislation that prescribes record management systems be designed to facilitate the right of access

Government records are primarily indexed for the government's convenience, rather than in a manner facilitating the right of access to information.[26] Requesters often know what kind of information they are searching for, but not necessarily where the information is to be found or the structure of the records to be searched.[27] The only provincial freedom of information law that prescribes records be classified and indexed to facilitate this right is that of Quebec.[28] Following the example of Quebec, BC should amend FIPPA to require that "[a] public body must classify its documents in such a manner as to allow their retrieval."[29]

III. Expanding the scope of the Act and narrowing the scope of some exceptions

Recommendation 3: Reformulate the definition of "public body" using a criteria-based definition rather than by allowing the government to designate specific agencies, boards, commissions, and corporations by regulation

The CCLA believes that FIPPA should apply broadly to all public bodies by default. A purposive expansion of access rights—the purpose being of course a robust democratic infrastructure with respect to information— would require access to information laws to apply to any entity that is controlled in whole or in part by the government, receives public funding, or performs a public function.[30] Undoubtedly, this should include corporate entities that are nominally designated as "private." The rationale behind this purposive expansion has to do with the rapid increase in public-private partnerships, and the consequent outsourcing of many tasks traditionally performed by the government to private institutions. Without subjecting such institutions to FIPPA, the requisite degree of transparency for a healthy democracy is not achieved—and accountability becomes increasingly evasive.

---

[25] *Public Records Act 2005* (NZ), 2005/40, s 17(1).
[26] Stanley L Tromp, *It's Time for Change! 206 Recommendations for Reforms to Canada's Access to Information Act* (Toronto: Centre for Free Expression at Ryerson University, August 2021) at 39.
[27] House of Commons, Standing Committee on Access to Information, Privacy and Ethics, *Evidence*, 42-1, No 72 (23 October 2017) at 1535 (Cara Zwibel).
[28] Stanley L Tromp, *It's Time for Change! 206 Recommendations for Reforms to Canada's Access to Information Act* (Toronto: Centre for Free Expression at Ryerson University, August 2021) at 39.
[29] *An Act respecting access to document held by public bodies and the protection of personal information*, CQLR c A-2.1, s 16.
[30] World Press Freedom, *(ATIA)* (16 June 2021), online: <worldpressfreedomcanada.ca/submission-from-world-press-freedom-canada-wpfc-to-treasury-boards-review-of-the-access-to-information-act-atia/>.

At present, Part 2 (Freedom of Information) of FIPPA applies "to all records in the custody or under the control of a public body."[31] In turn, a "public body" includes:[32]

- every ministry of the government of British Columbia, including, for certainty, the Office of the Premier;
- the agencies, boards, commissions, or other bodies listed in Schedule 2, which may be added to by Order in Council; and
- any local public body, defined as:[33]
    - local government bodies
    - health care bodies
    - social services bodies
    - educational bodies
    - governing bodies of professions or occupations listed in Schedule 3, which may be added to by Order in Council.

The term "public body," however, is deemed not to include the office of a person who is a member or officer of the Legislative Assembly or the Court of Appeal, Supreme Court, or Provincial Court.[34] Put another way, FIPPA applies by default to all government ministries and local public bodies, can be extended to apply to boards, commissions, professional regulators and agencies on a case-by-case basis, through regulation, but never applies to the office of a member or officer of the Legislative Assembly or the courts.

In furtherance of a purposive expansion, BC should define the term "public body" using a criteria-based definition, adopting the criteria recommended by the House of Commons Standing Committee on Access to Information, Privacy and Ethics (2016), namely:

- institutions publicly funded in whole or in part by the Government (including those with the ability to raise funds through public borrowing) (this would include traditional departments but also other organizations such as publicly funded research institutions);
- institutions publicly controlled in whole or in part by the Government, including those for which the government appoints a majority of the members of the governing body (such as Crown corporations and their subsidiaries);
- institutions that perform a public function, including those in the areas of health and safety, the environment, and economic security;
- institutions established by statute; and
- all institutions covered by the *Financial Administration Act*.[35]

Alternatively, the Government could amend the Act to adopt a criteria-based definition while retaining Schedule 2 as a non-exhaustive list, without restricting the generality of the former. This

[31] *Freedom of Information and Protection of Privacy Act*, RSBC 1996, c 165, s 3(1).
[32] *Ibid*, Sch 1("public body").
[33] *Ibid*, Sch 1("local public body").
[34] *Ibid*, Sch 1("public body").
[35] House of Commons, *Review of the Access to Information Act: Report of the Standing Committee on Access to Information, Privacy and Ethics* (June 2016) (Chair: Blaine Calkins) at 5.

is the approach taken by the United Kingdom, which uses both definitions and listings to circumscribe the scope of its freedom of information law.[36]

Recommendation 4: Amend Section 13 of FIPPA to narrow the scope of the policy "advice" and "recommendations" discretionary exemption

Currently, subsection 13(1) of FIPPA provides that "[t]he head of a public body may refuse to disclose to an applicant information that would reveal advice or recommendations developed by or for a public body or a minister."[37] For greater certainty, the section excludes certain materials from the scope of subsection 13(1): e.g., factual materials, public opinion polls, certain reports and studies, and records that have been in existence for 10 or more years.[38] Where section 13 applies, the head of a public body has a discretionary power to withhold information in accordance with the public interest.[39]

The scope of the section 13 exemption has changed substantially with judicial interpretation. According to the Supreme Court of Canada, in a case involving the equivalent of section 13 in Ontario's *Freedom of Information and Protection of Privacy Act*, the term "advice" has a broader meaning than the term "recommendations."[40] A recommendation is information that relates to a suggested course of action that will ultimately be accepted or rejected.[41] By contrast, advice is broader still, and includes opinions of a public servant as to the range of alternative policy options for a given issue.[42] This includes information that sets forth considerations to take into account by the decision-maker in the decision-making process without expressing any preferred course of action.[43]

The exemption provided for under subsection 13(1) is further enlarged by the narrow reading of the "factual materials" carve-out contained in subsection 13(2)(a).[44] The head of a public body must not refuse to disclose "factual materials."[45] In the context of FIPPA, however, factual materials are a sub-category of information. The distinction turns on whether "the disclosure of the information would enable someone to *infer* the actual advice or recommendations at issue."[46] Put another way, factual materials do not include information likely to reveal the substance of policy advice or recommendations. For instance, "source materials accessed by the experts or background facts not necessary to the expert's 'advice' or the deliberative process at hand would constitute 'factual material'" and are therefore not subject to the discretionary

[36] *Freedom of Information Act 2000* (UK), 2000, s 3.
[37] *FIPPA*, s 13(1).
[38] *Ibid*, ss 13(2-3).
[39] *Ontario (Public Safety and Security) v Criminal Lawyers' Association*, 2010 SCC 23 at para 48.
[40] *Ontario (Minister of Finance) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 36 at para 24.
[41] *British Columbia (Ministry of Forests, Lands, Natural Resources and Rural Development), Re*, 2018 BCIPC 44 at para 10.
[42] *Ontario (Minister of Finance) v Ontario (Information and Privacy Commissioner)*, 2014 SCC 36 at para 46.
[43] *Ibid* at para 47.
[44] *FIPPA*, s 13(2)(a).
[45] *Ibid*, s 13(2)(a).
[46] *Insurance Corporation of British Columbia v Automotive Retailers Association*, 2013 BCSC 2025 at para 41.

exemption for policy and recommendations, whereas any information "necessary" to the expert's opinion or deliberative process may be withheld.[47]

This distinction is completely untenable in practice. The CCLA believes that subsection 13(2)(a) should be amended to remove all factual information from the discretionary power to refuse disclosure of policy recommendations or advice.

IV. Equitable access and unreasonable delays in the access to information regime

Recommendation 5: Amend Section 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timeline for responding to access requests

The CCLA believes that democracy requires not only that information be accessible, but that accessibility is dependent on timely access. Democracy is an active process: whenever possible, the public should be kept informed before, during, and after the making of a decision. When access is delayed until after a decision has already been implemented or decided, or until the information has become out-of-date or irrelevant, the public is deprived of an opportunity to participate in the business of government. In the informational context, access delayed is often access denied.

By default, the head of a public body in BC must respond to every access request within 30 days.[48] The head of a public body may extend the time for responding to a request for up to 30 additional days if: the applicant has given insufficient detail, the search involves a large number of records and it would therefore be unreasonable to meet the deadline, more time is needed to consult with a third party or another public body, or if the applicant consents.[49] With the permission of the Commissioner, extensions longer than 30 days may be granted.[50]

Response times have improved in BC since September 2017; however, this is far from an unqualified success.[51] The CCLA is deeply troubled by the Commissioner's finding that "between April 1, 2017, and March 31, 2020, government took it upon themselves, in over 4,000 cases, to extend the response time for an access request without any legal right to do so."[52] Similarly, the CCLA is concerned that in one third of all access requests from April 2017 to March 2020, public bodies in BC failed to meet the basic standard of 30 business days.[53]

To help improve response times, the CCLA recommends amending section 75 of FIPPA to provide an automatic fee waiver for applicants when a public body has failed to meet the statutory timelines for responding to access requests, including improper extensions. Section 75 of

---

[47] *Provincial Health Services Authority v British Columbia (Information and Privacy Commissioner)*, 2013 BCSC 2322 at para 94.
[48] *FIPPA*, s 7(1).
[49] *Ibid*, s 10(1).
[50] *Ibid*, s 10(2).
[51] British Columbia, Office of the Information and Privacy Commissioner, *Now is the time: A report card on government's access to information timeliness*, 2020 BCIPC 45 at 5.
[52] *Ibid* at 3.
[53] *Ibid* at 5.

FIPPA currently allows public bodies to require applicants to pay certain fees (set by regulation) for access requests, as well as providing a discretionary power grant fee waivers in some circumstances.[54] Adding an additional clause granting an automatic waiver for unreasonable delays would provide public bodies with an incentive to process access requests more efficiently. To do so, some public bodies may require additional resources or funding to meet this challenge.

Recommendation 6: Amend Section 75 to make fee waivers available as a matter of course, without the applicant having to make a specific request, when there is significant public interest in disclosure

Subsection 75(5) of FIPPA allows the head of a public body to grant a fee waiver upon receipt of an "applicant's written request" if "the applicant cannot afford the payment or for any other reason it is fair to excuse payment, or the record relates to a matter of public interest, including the environment or public health or safety."[55]

The CCLA recommends amending section 75 to dispense with the requirement for a written request. The requirement needlessly imposes additional barriers for access to information where disclosure is in the public interest.

IV. The need for modernization to respond to emerging technologies and the commodification of data

Recommendation 7: Amend FIPPA to explicitly recognize privacy as a human right in its statement of purpose

The CCLA believes that the first step in re-imagining British Columbia's public sector privacy regime is to strengthen FIPPA's commitment to privacy as a human right. Sections 7 and 8 of the *Charter* protect a sphere of individual autonomy within which people have the right "to be let alone" and on which the state cannot intrude without permission.[56] Public sector privacy legislation gives effect to sections 7 and 8 of the *Charter* with respect to the collection, use, and disclosure of personal information by public bodies. The CCLA recommends amending section 2 (Purposes of the Act) to ensure that the entire statute is interpreted in a way that furthers individual privacy rights.

Amending FIPPA to recognise privacy as a fundamental and foundational human right would also bring it closer in line with international standards. The EU's General Data Protection Regulation ("GDPR") repeatedly recognises the fundamental rights of individuals in relation to data processing, although it is still fundamentally a data protection instrument.[57]

---

[54] *FIPPA*, s 75(5).
[55] *FIPPA*, s 75(5).
[56] *R. v Ahmad*, 2020 SCC 11 at para 38. See also *Association of Justice Counsel v Canada (Attorney General)*, 2017 SCC 55 at para 49.
[57] Tunca Bolca, "Can *PIPEDA* 'Face' the Challenge? An Analysis of the Adequacy of Canada's Private Sector Privacy Legislation Against Facial Recognition Technology" (2020) 18 Can JL & Tech.

Recommendation 8: Amend FIPPA to codify a presumption that biometric data is quintessentially private data. It would be beneficial for the Committee to engage in a specific analysis of the privacy risks of biometric identifiers to identify additional principled and proactive protections that may be required and could be addressed by FIPPA amendments.

Biometric technologies, including but not limited to facial recognition technologies, present growing challenges to democratic societies. Today, biometrics are hard to escape: most smartphones come equipped with biometric technology, many police forces use fingerprinting and facial recognition technology on both suspects and the public at large, and passive surveillance, like security cameras, can provide extensive biometric data. Whereas private biometric data of all kinds is inherently vulnerable, facial recognition shows how quickly the technology can spread out of users' control. The vast library of images of people's faces on the Internet is a goldmine for the public and private sectors alike. In just the past few years, civil society has been catapulted towards a level of intelligent surveillance and biometric data collection that was previously only common in science fiction. The fact of contemporary biometric data gathering technology requires the Committee's attention and the CCLA invites the Committee to update the Act.

The use of biometric data by public bodies has been considered by the OIPC in the past. For example, in 2011, the OIPC determined that the Insurance Corporation of British Columbia, a Crown corporation listed in Schedule 2 of FIPPA, had used and disclosed biometric data to law enforcement in a manner contrary to the Act.[58] ICBC had previous implemented facial recognition technology to address identity fraud.[59] In the aftermath of the Stanley Cup riot in 2011, ICBC offered the use of its facial recognition software to the Vancouver Police Department.[60] Without judicial authorization, the OIPC considered this purpose improper. The ICBC case illustrates the dangers of function creep, i.e., when personal information is collected or disclosed for a particular purpose (e.g., driver licence fraud prevention) is then repurposed for something entirely different without legal authority.[61]

The CCLA believes that FIPPA would benefit from a presumption that biometric data is quintessentially private. In Illinois, the *Biometric Information Privacy Act* provides that no private entity may collect, store, or use biometric identifiers or information without providing prior notice to and obtaining a written release or consent from the data's subject.[62] Similarly, Quebec's *Act to establish a legal framework for information technology* stipulates that "[a] person's identity may not be verified or confirmed by means of a process that allows biometric characteristics or

[58] *Investigation into the Use of Facial Recognition Technology by the Insurance Corporation of British Columbia*, Investigation Report F12-01, 2011 BCIPC No. 5 at para 110.
[59] When any individual applies for a new or replacement drivers license or BC ID, that person's picture is taken, and a new facial recognition template is created. That template is compared against all existing templates to determine whether the individual is who they say the are and to determine if perhaps the individual has more than one identity. In the fall of 2010, ICBC purchased an enhancement to its FR technology. The enhancement included both the ability to import images and the ability to adjust the error margins/threshold used to compare those images to other images in the database. The ability to import images meant that ICBC could apply the technology to images from sources other than ICBC's own digital picture identification database: *Ibid* at paras 22-4.
[60] *Ibid* at para 10.
[61] British Columbia, Office of the Information and Privacy Commissioner, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (Victoria: OIPC, June 2021) at 20.
[62] *Biometric Information Privacy Act*, 740 ILCS 14, s 15 (IL).

measurements to be recorded, except with the express consent of the person concerned."[63] In the same vein, FIPPA should be amended to require public bodies to obtain express consent, except in the case of a warrant or subpoena, before collecting, using, or disclosing biometric data.

Recommendation 9: Amend FIPPA to contain a right for individuals to be informed about the use of automated decision-making processes they are subject to, a right to object to automated decision-making, and a right to correct personal information used to make decisions about them

In the public sector, "[p]eople have no choice but to interact with government and the decisions of government can have serious, long-lasting impacts on our lives."[64] The use of AI by public bodies ranges from relatively limited applications, such as automated virtual assistants, to highly sophisticated systems relying on machine learning algorithms trained using large datasets of historical examples, such as predictive policing systems.[65] In the latter case, the inner workings of these algorithms are not always intelligible to human understanding – the so-called "black box" problem.[66] Moreover, when the data used to train a machine learning system is itself corrupted, incomplete, inaccurate, or exhibits bias, a second problem emerges, i.e., the use of "dirty data."[67]

FIPPA was not designed with artificial intelligence in mind.[68] The legal authority for collection most widely used by public bodies requires that personal information only be collected if it relates to and is necessary for carrying out a program or activity of the public body.[69] Meeting this threshold may be difficult for a public body to justify the large amount of training data required by an AI system to run programs that previously operated without.[70] FIPPA also does not impose any specific transparency obligations with respect to AI algorithms, nor does it give individuals any right to object to decisions made against them by automated decision-makers.[71] By contrast, Quebec has updated its privacy laws (effective September 2023) to require public bodies and enterprises to provide certain information to the person concerned when they collect personal information using technology that includes functions allowing the person concerned to be

[63] *Act to establish a legal framework for information technology*, CQLR c C-1.1, s 44.
[64] British Columbia, Office of the Information and Privacy Commissioner, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (Victoria: OIPC, June 2021) at 5.
[65] *Ibid* at 8.
[66] Citizen Lab, *To Surveil and Protect: A Human Rights Analysis of Algorithmic Policing in Canada* (Toronto: University of Toronto, 2020) at 31, online: <citizenlab.ca/wp-content/uploads/2020/09/To-Surveil-and-Predict.pdf>.
[67] *Ibid* at 32.
[68] British Columbia, Office of the Information and Privacy Commissioner, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (Victoria: OIPC, June 2021) at 20.
[69] *FIPPA*, s 26(c). See also *ibid* at 20.
[70] British Columbia, Office of the Information and Privacy Commissioner, *Getting Ahead of the Curve: Meeting the challenges to privacy and fairness arising from the use of artificial intelligence in the public sector* (Victoria: OIPC, June 2021) at 20.
[71] *Ibid*.

identified, located or profiled, or when they use personal information to render a decision based exclusively on an automated processing of such information.[72]

Given the opacity and potential discriminatory effects of automated decision-making, CCLA supports a legal right to object to automated decision-making and to be free from such decision-making, subject to limited exceptions. This is a step further than the Quebec reforms. All persons should be granted the right to object to automated decision-making, which should be effective immediately upon objection. That right should include the right to request human intervention, to contest any automated decision that has been taken, and to express the objector's point of view on the automated decision. Similarly, there should be a legal right to be free of automated processing, including profiling, without having to actively object. Exceptions to that right can include situations where explicit consent has been obtained, where an automated decision is necessary for a contract that was freely entered into, or when automated decision-making is prescribed by law. These proposals would bring FIPPA in line with Articles 21 and 22 of the GDPR.

The CCLA also recommends amending FIPPA to include a provision requiring any public body that uses AI to process personal data to clearly explain where automated processing has been used, the logic behind the decisions of the automated processing, and verify or ideally publish some version of the privacy impact and AI impact assessments conducted. Such an amendment would increase public awareness of AI decision-making – public bodies having to publicly explain the different factors that go into algorithms will assist in busting the myth of the neutral algorithm. That amendment would also enhance government accountability - public bodies would have to explain each automated decision process and bear the burden of ensuring that those processes do not have a discriminatory impact. Public trust in algorithmic decision-making would also increase, since individuals would have the confidence that they knew what factors went into each decision-making process.

Recommendation 10: Amend FIPPA to cover all "de-identified data," as well as introduce appropriate definitions, enforcement, and accountability mechanisms

Since Part 3 of FIPPA covers only "personal information," defined as information about an "identifiable individual," there is a level of debate around whether or not de-identified data is covered by FIPPA, with many believing or behaving as if it is not. That is a lacuna in the law because truly de-identified data is an elusive, if not impossible, concept. Even if directly identifying information such as names or identity numbers are removed, the data can often be re-identified.

Ben Green has described two ways of re-identifying "de-identified data" to yield sensitive information: the mosaic effect, and pattern-spotting.[73] First, the mosaic effect involves piecing

[72] Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, 1st Sess, 42nd Leg, Quebec, 2020 (Royal Assent granted 22 September 2021), SQ 2021, c 25, s 21, amending the *Act respecting access to documents held by public bodies and the protecting of personal information* to include new AI requirements (coming into force 22 September 2023).
[73] Ben Green, *Affidavit and Opinion on the Sidewalk Labs Litigation.* (24 May 2019), at 3. Online: <https://ccla.org/cclanewsite/wp-content/uploads/2019/06/Affidavit-of-Ben-Green-2019-05-24-..pdf>.

together disparate data sets to form a mosaic that reveals personal information. In 2014, New York City released data for all licensed taxi rides on a given day; the data lacked personally identifying information such as names but contained information such as pickup and drop-off locations or the taxi licence plate numbers.[74] A data scientist processed that information together with published reports of someone's location, such as a Facebook location check-in, and found that it was possible to track where specific individuals were travelling.[75] Second, pattern-spotting can re-identify large "de-identified" datasets because of the uniqueness of human behaviour.[76] Two experiments analyzed the mobile phone location data and credit card information of more than one million individuals; over 90% of the people could be uniquely identified with just four data points of where they were going and when they had been at that location.[77] The rapid processing speed enabled by AI will increasingly make such analysis easier to perform.

There is thus no principled reason why supposedly de-identified data should be excluded from the scope of FIPPA. When we look to PIPEDA, it has already recognised that "de-identified data" should still count as "personal information" that is covered by PIPEDA if there was a "serious possibility" that the data could be re-identified.[78] CCLA prefers a higher standard than "serious possibility", given the risks outlined above regarding re-identification. While we recognise that de-identification, correctly implemented, does provide a form of privacy protection, it does not and should not take personal information subjected to such processing outside of the scope of privacy law to regulate.

The CCLA further recommends FIPPA be amended to clearly define "de-identified information," "anonymized information," "pseudonymized information," and "aggregate information" and explicitly bring them within the scope of the law, including the addition of appropriate accountability and transparency provisions. These should include requiring public bodies who wish to de-identify personal information to inform data subjects regarding how they de-identify data, and about the level of risk that data could be re-identified. The Commissioner should have authority to enforce the use of best practices and industry-recognised standards for de-identification, including the ability to assess individual complaints when public bodies are alleged to fail to adhere to such standards.

---

[74] Anthony Tockar, "Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset," *Neustar Research* (2014), online: <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset>.

[75] Anthony Tockar, "Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset," *Neustar Research* (2014), online: <https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset>.

[76] Mike Ananny, "The Curious Connection Between Apps for Gay Men and Sex Offenders" The Atlantic (14 April 2011), online: <https://www.theatlantic.com/technology/archive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340/>.

[77] Yves-Alexandre de Montjoye et al, "Unique in the Crowd: The privacy bounds of human mobility," *Nature srep.* 3 (2013); Yves-Alexandre de Montjoye et al, "Unique in the shopping mall: On the reidentifiability of credit card metadata," *Science* 347, no 6221 (2015).

[78] *PIPEDA* Case Summary #2009-018, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/*PIPEDA*-2009-018/>.

V. The need to strengthen data residency requirements

Recommendation 11: Amend FIPPA to include minimum requirements for the storage of personal information outside Canada by public bodies, such as by permitting data storage or disclosure outside of Canada only in jurisdictions with substantially similar privacy laws

Prior to the passage of Bill 22 in November 2021, public bodies in BC were required to ensure personal information in their custody or under their control was stored only in Canada and accessible only in Canada, with very limited exceptions.[79] Namely, under section 30.1 of FIPPA, public bodies could only store or make accessible personal information outside of Canada with consent,[80] for the purpose of processing a payment,[81] or when otherwise authorized to do so under the Act.[82] Bill 22 repealed this provision.[83]

In its present form, FIPPA allows public bodies to disclose or store personal information "outside of Canada only if the disclosure is in accordance with the regulations."[84] The regulations, in turn, stipulate that "[t]he head of a public body must [conduct a privacy impact assessment] with respect to each of the public body's programs, projects and systems in which personal information that is sensitive is disclosed to be stored outside of Canada."[85] However, this requirement does not apply to programs or systems in existence on November 26, 2021, or if the information is made available to the public under an enactment that authorizes or requires the information to be made public.[86] According to the BC Ministry of Citizens' Services, the amendments made to the data residency requirements under FIPPA are meant to "help public bodies keep pace with new technology and provide the services people expect in a modern age."[87]

While the CCLA welcomes the requirement that a privacy impact assessment be conducted prior to storing data outside Canada, the addition of a PIA requirement coincides with the loss of other important safeguards. When information is stored or accessible electronically in another country, data sovereignty may be compromised. For instance, the US *Patriot Act* allows US authorities to, among other things, obtain records and other "tangible things" to protect against international terrorism and against clandestine intelligence activities.[88] In Hong Kong, under the *National Security Law*, the Secretary for Justice may seek an order to require any person to produce any material that reasonably appears to relate to any matter relevant to an investigation for an offence endangering "national security."[89] Canadian data is endangered by such laws when stored or made accessible in those jurisdictions. The CCLA recognizes that some latitude must be

---

[79] *FIPPA*, s 30.1, as it appeared on 24 November 2021.
[80] *FIPPA*, s 30.1(a), as it appeared on 24 November 2021.
[81] *FIPPA*, ss 30.1(c), 33.1(1)(i.1), as it appeared on 24 November 2021.
[82] *FIPPA*, s 30.1(b), as it appeared on 24 November 2021.
[83] Bill 22, *Freedom of Information and Protection of Privacy Amendment Act, 2021*, 2nd Sess, 42nd Parl, British Columbia (Royal Assent granted 25 November 2021), SBC 2021, c 39, s 17.
[84] *FIPPA*, s 33.1.
[85] *Personal Information Disclosure for Storage Outside of Canada Regulation*, BC Reg 294/2021, s 2(1).
[86] *Ibid*, s 3. See also *FIPPA*, s 33(2)(f).
[87] British Columbia, Citizens' Services, "Amendments strengthen access to information, protect people's privacy" (18 October 2021), online: <news.gov.bc.ca/releases/2021CITZ0048-001990>.
[88] *Patriot Act*, 115 Stat 272, s 215 (US).
[89] *Implementation Rules for Article 43 of the Law of the People's Republic of China on Safeguarding National Security in the Hong Kong Special Administrative Region*, LN 139 of 2020, Sch 7 (HK).

afforded to public bodies to store, process or make accessible personal information outside of Canada, particularly where cloud services are concerned. However, since the passage of Bill 22, FIPPA clearly skews towards convenience over data sovereignty and security, at least insofar as data residency requirements are concerned.

The CCLA recommends adopting the data residency requirements under FIPPA proposed by the OIPC in October 2021.[90] FIPPA should be amended to impose at least a baseline level of protections for personal information disclosed outside of Canada. At present, if the government chooses to repeal its regulations for data disclosure and storage outside of Canada, there would be no applicable protections at all.[91] The executive should not possess an unfettered power to remove all requirements for public bodies seeking to store personal information outside of Canada. At the very least, FIPPA should outline a minimum level or protection or guiding principles. Alternatively, the CCLA recommends amending FIPPA to only permit storing or disclosing personal information outside Canada in jurisdictions with substantially similar privacy legislation, or with individual consent. All of which is in addition to retaining the privacy impact assessment requirement introduced by Bill 22.

The CCLA is grateful to the Special Committee to Review the Freedom of Information and Protection of Privacy Act for providing the opportunity to make submissions as a part of your important and timely examination of British Columbia's public sector privacy and access legislation.

[90] Letter from Michael McEvoy to Minister Lisa Beare (20 October 2021), online: <oipc.bc.ca/public-comments/3592>.
[91] *FIPPA*, s 33.1.