
**Submission to the**

# Modernizing Canada's *Privacy Act* Consultation

**Presented by the**
**International Civil Liberties Monitoring Group**

**15 February 2021**

International Civil Liberties Monitoring Group
Coalition pour la surveillance internationale des libertés civiles
508-250 City Centre Ave., Ottawa, Ontario, K1R 6K7
Tel. (613) 241-5298
www.iclmg.ca

**About the ICLMG**

The International Civil Liberties Monitoring Group (ICLMG) is a national coalition of Canadian civil society organizations that was established after the adoption of the *Anti-Terrorism Act* of 2001 in order to protect and promote human rights and civil liberties in the context of the so-called "war on terror." The coalition brings together 45 NGOs, unions, professional associations, faith groups, environmental organizations, human rights and civil liberties advocates, as well as groups representing immigrant and refugee communities in Canada.

Our mandate is to defend the civil liberties and human rights set out in the Canadian Charter of Rights and Freedoms, federal and provincial laws (such as the Canadian Bill of Rights, the *Canadian Human Rights Act*, provincial charters of human rights or privacy legislation), and international human rights instruments (such as the Universal Declaration of Human Rights, the International Covenant on Civil and Political Rights, the Convention against Torture and Other Cruel, Inhuman or Degrading Treatment or Punishment).

Active in the promotion and defense of rights within their own respective sectors of Canadian society, ICLMG members have come together within this coalition to share their concerns about national and international anti-terrorism legislation, and other national security measures, and their impact on civil liberties, human rights, refugee protection, minority groups, political dissent, governance of charities, international cooperation and humanitarian assistance.

Since its inception, ICLMG has served as a round-table for strategic exchange — including international and North/South exchange — among organizations and communities affected by the application, internationally, of new national security ("anti-terrorist") laws.

An important aspect of the role of the ICLMG is the dissemination of information related to human rights in the context of counter-terrorism and the expanding – and largely unaccountable – national security apparatus. This information is distributed to members of the coalition who in turn broadcast it to their own networks.

Finally, further to its mandate, the ICLMG has intervened in individual cases where there have been allegations of serious violation of civil liberties and human rights. The ICLMG has also intervened to contest proposed legislation, regulations and practices that contravene the Canadian Constitution, other Canadian laws and international human rights standards.

## INTRODUCTION

Since our coalition's establishment, we have documented an acute increase of surveillance in the name of national security and the fight against terrorism, and a parallel impact on privacy rights of Canadians and people both within and outside of Canada.

There have been multiple revelations at the domestic and international level of information gathering and sharing practices that pose significant risks to the fundamental rights of individuals and entire communities. This ranges from information sharing with foreign partners leading to the rendition and torture of innocent Canadians like Maher Arar,[1] to illegal bulk collection and retention of personal information by Canadian Security Intelligence Service (CSIS),[2] to the revelations made by Edward Snowden of the vast, interconnected mass surveillance system created by Five Eyes countries including Canada.[3]

The trend among security agencies has reflected the overall trend in both the private and public sector to increasingly see data about individuals as an important resource – whether for profits or for public policy making. This has led to a universal push for the collection, retention, sharing, analysis and use of our personal information. The increase has been driven both by technological advancements, but also by a significant increase in the kinds of data individuals are creating and sharing about themselves.

Security agencies have followed this trend, hoping to achieve what is known as "total information awareness"[4]: collecting as much information as possible, analyzing it, and using it in an attempt to reduce security threats.

But such pushes have significant and negative impacts on privacy and associated rights. Personal information shared consensually, either publicly or directly to private or public agencies, has been covertly disclosed to and/or collected and used by security agencies, including in situations where no legal authorization exists to do so.[5] Pressure has also

---

[1] "Report of the Events Relating to Maher Arar," *Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar*, 2006. Available at: https://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf

[2] Jordan Pearson, "Canadian Spies Illegally Retained Metadata for a Decade," *Vice*, 3 November 2016. Available at: https://www.vice.com/en/article/bmv383/canadian-spies-illegally-retained-metadata-for-a-decade-csis

[3] Dave Seglins, "CSE tracks millions of downloads daily: Snowden documents," *CBC News*, 27 January 2015. Available at: https://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120

[4] Michael Geist, "'Total Information Awareness': The Disastrous Privacy Consequences of Bill C-51," MichaelGeist.ca, 19 February 2015. Available at: https://www.michaelgeist.ca/2015/02/total-information-awareness-disastrous-privacy-consequences-bill-c-51/.

[5] Marco Vigliotti, "Federal Court reprimands CSIS for breaking the law in national security investigations," iPolitics.ca, 16 July 2020. Available at: https://ipolitics.ca/2020/07/16/federal-court-reprimands-csis-for-breaking-the-law-in-national-security-investigations/; Jim Bronskill, "CSIS spies' use of geolocation data may have broken law: watchdog report," The Canadian Press, 11 December 2020. Available at: https://www.thestar.com/politics/2020/12/11/csis-spies-use-of-geolocation-data-may-have-broken-law-watchdog-report.html.

mounted on government agencies to disclose information with national security branches of government.

Canadians have also expressed concern around how their information is handled by security and intelligence agencies. In a 2016 poll by the Office of the Privacy Commissioner of Canada (OPC), 81% of Canadians were at least somewhat concerned about government monitoring of their personal activities for national security or public safety purposes; 70% also stated that intelligence gathering and law enforcement agencies should be required to publicly report how often they make requests for personal information without a court authorization. [6]

It is clear that the legislation has not kept up with these developments. Significant changes have been made to national security laws to create legal basis for collection, retention, analysis and use. These laws have been hotly disputed, and while new safeguards put in place in the form of greater oversight and review, concerns persist.

It is also important to note that potential impact that the collection and use of personal information can have is not equal across communities. Members of BIPOC communities already face disproportionate impacts of national security policing and policies, and any increase in the use or abuse of their personal information can have a much more significant impact on their livelihood than that of White Canadians.

Our coalition believes that some of these issues could be addressed by improving the foundational privacy laws of Canada (although much would also need to be addressed in national security legislation itself). In this regard, we welcome efforts to improve the *Personal Information Protection and Electronic Documents Act* (PIPEDA) via the provisions in Bill C-11, the *Digital Charter Implementation Act, 2020.*[7] It is crucial that a similar process take place with the *Privacy Act*.

While we maintain our criticism of existing wide-ranging exceptions in Canada's privacy laws for national security purposes, we believe that stronger overall privacy laws will nonetheless help clear up ambiguities. For example, while we would ultimately remain concerned about rules regarding disclosure of personal information to national security agencies, new privacy rules that help to regulate and minimize what information is initially collected by government agencies will help limit the possibility of problematic disclosure to security agencies.

---

[6] "2016 Survey of Canadians on Privacy," Prepared for Office of the Privacy Commissioner of Canada by Phoenix Strategic Perspectives Inc., December 2016. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2016/por_2016_12/

[7] *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*, Second Session, Forty-third Parliament, House of Commons of Canada. 17 November 2020. Available at: https://parl.ca/DocumentViewer/en/43-2/bill/C-11/first-reading

A modernized *Privacy Act* would also help to clarify concepts, for example around publicly available information and expectations of privacy. It would also help ensure future-proofing and technological neutrality in the law, allowing for the necessary flexibility in addressing novel situations. Finally, in order to ensure that privacy laws have the required impact, there must be strengthened transparency, accountability and enforcement mechanisms.

These areas are reflected in the sections that follow. But first, it is important to address the necessity to clearly establish the recognition of privacy as a human right.

## PRIVACY AS A HUMAN RIGHT

As a starting point, our coalition supports the call for a rights-based approach to Canada's privacy laws, including the recognition of privacy as a fundamental right in any modernized *Privacy Act*.

Canadian courts have already recognized the quasi-constitutional nature of Canada's privacy legislation.[8] Further, as has been widely documented, including in Supreme Court of Canada rulings, privacy encompasses much more than simply protecting how our personal information is used.[9] For example, it also includes notions such as confidentiality, anonymity, control over access and use of information, as well as protection against surveillance of not just our communication but also of our actions and associations.[10]

Privacy is also foundational to our ability to exercise, unhindered, our other constitutional rights such as freedom of association, assembly, expression, movement and religion. The federal government has also signed on to international human rights and civil liberties accords that recognize the right to privacy. For example, Article 17 of the *International Covenant on Civil and Political Rights* states:

> ***Article 17***
> 1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2. Everyone has the right to the protection of the law against such interference or attacks.[11]

And article of the *Universal Declaration of Human Rights* states:

[8] Office of the Privacy Commissioner of Canada, "Privacy Law Reform - A Pathway to Respecting Rights and Restoring Trust in Government and the Digital Economy: 2018-2019 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*," 2019. Available at: https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/201819/ar_201819/
[9] *ibid.*
[10] *ibid.*
[11] "International Covenant on Civil and Political Rights," United Nations General Assembly resolution 2200A (XXI), 16 December 1966. Available at: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

**Article 12.**
No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.[12]

By formally recognizing privacy as a right, the federal government would establish a strong baseline from which all other privacy protections would flow. It would also demonstrate the seriousness with which all government agencies must treat issues surrounding privacy.

Endorse in large part the model proposed by the Office of the Privacy Commissioner in its 2018-2019 annual report[13], with a few exceptions:

**Preamble**
WHEREAS privacy is a basic human right of every individual and a fundamental value reflected in international human rights instruments to which Canada is a signatory;
WHEREAS the right to privacy protects individual autonomy and dignity, and is linked to the protection of reputation and freedom of thought and expression;
WHEREAS privacy is essential to the relations of mutual trust and confidence that are fundamental to the Canadian social fabric;
WHEREAS privacy is essential to the preservation of democracy and the full and meaningful enjoyment and exercise of many of the rights and freedoms guaranteed by the *Canadian Charter of Rights and Freedoms*;
WHEREAS the current and evolving technological context facilitates the collection of massive quantities of personal data as well as the use of these data, whether in identifiable, aggregate or anonymized forms, in ways that can adversely impact individuals, groups and communities;
WHEREAS all individuals have a constitutional right to be free from unreasonable search or seizure, including the right to be free from unwarranted state surveillance;
WHEREAS the federal government must only collect, use or disclose personal information in ways that are lawful, fair, proportional, transparent and accountable and only to serve individual Canadians or the legitimate public interest;
WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

**Purpose**
The purposes of this *Act* are:
(a) to implement the fundamental right to privacy of all persons with respect to their personal information in the federal public sector through robust data protection that ensures that the processing of personal information is lawful, fair, proportional, transparent and accountable, and respects the fundamental rights and

[12] "Universal Declaration of Human Rights," United Nations General Assembly resolution 217 A, 10 December 1948. Available at: https://www.un.org/en/universal-declaration-human-rights/
[13] OPC, "Privacy Law Reform."

freedoms of individuals;
(b) to ***protect*** the privacy rights of individuals ***while recognizing*** the government's requirement to collect, use and disclose personal information for purposes that demonstrably serve the public interest;
(c) to provide individuals with ***timely*** and effective remedies when their privacy rights have not been respected and to ensure the ongoing compliance by institutions with their obligations under this *Act*.

***[Emphasis ours]***

## LAW ENFORCEMENT & NATIONAL SECURITY

We believe that it is important that, in updating and modernizing Canada's privacy laws, that the government should pay special attention to the interplay between these laws and the powers of law enforcement and intelligence agencies. Like so many government agencies, the ways that law enforcement and intelligence agencies collect and use personal information can have significant implications on the rights and wellbeing of Canadians and people in Canada. Surveillance itself can have detrimental impacts on not just individuals but entire communities, and the eventual use of such information can entail even deeper implications for the rights of those involved.

As mentioned earlier, Canada has also moved to facilitate and increase disclosure of information by all government departments and those departments with national security mandates. The current governing legislation in this regard is the *Security of Canada Information Disclosure Act*.[14] While this act is separate from the *Privacy Act*, the way the two piece of legislation interact is crucial: if protections are not in place to limit the collection of personal information, or to ensure the accuracy of such information, by the government as a whole, there is an increased likelihood that this inappropriately collected information is then shared with national security departments, possibly leading to detrimental impacts for the individuals in question.

Clearer definitions and strong rights-protecting language will also provide guidance in making decisions about what information is appropriate to share with national security agencies. Ideally, there would not be a separate regime that allows for the disclosure of personal information on the basis of it "contributing" to the receiving agencies mandate in relation to the overbroad definition of "activity that undermines the security of Canada." At the same time, a strengthened *Privacy Act* could improve safeguards and provide greater guidance for disclosing institutions.

Beyond information sharing between agencies, there exist concerns regarding information sharing with both private and foreign entities. Again, while these are governed by other pieces of legislation, a strengthened *Privacy Act* would only further ensure protections. This

[14] *Security of Canada Information Disclosure Act*, S.C. 2015, c. 20, s. 2, 18 June 2015. Available at: https://laws-lois.justice.gc.ca/eng/acts/S-6.9/page-1.html

could include, for example, governing circumstances of disclosing information with, or accepting information offered up by, private companies. It could also include ensuring that all information-sharing agreements are in writing and are reviewable by outside bodies.

Law enforcement and intelligence agencies also use emerging technologies that carry with them significant privacy implications, and impacting other related rights. One need only look at the current debate around the use of facial recognition technology. The RCMP remains under investigation for its use of Clearview AI's facial recognition technology.[15] This same company was just found to be a tool of mass surveillance in contravention of Canada's privacy laws.[16]

This is simply one example as to why the *Privacy Act* must be updated. This includes ensuring necessity and proportionality principles, updating concepts including personal information and publicly available information, and ensuring strong, enforceable rules – particularly around the adoption of emerging technologies and new uses of personal information.

## PROPORTIONALITY & NECESSITY

Further to a rights-based approach to privacy, we support the inclusion of a necessity and proportionality standard which would underpin the overall approach of government agencies towards the handling of personal information.

As the OPC has written:

> Government institutions should be required to ensure that their measures are necessary and proportionate, which means essentially evidence-based, necessary for the specific purpose identified and not overbroad. In our view, these principles serve to balance the privacy rights of individuals with the government's need to collect, use and disclose personal information for purposes that demonstrably serve the public interest.[17]

Such an approach would address two important issues, among others:

[15] Office of the Privacy Commissioner of Canada, "OPC launches investigation into RCMP's use of facial recognition technology," 28 February 2020. Available at: https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/an_200228/

[16] Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta," 2 February 2021. Available online at: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/

[17] Office of the Privacy Commissioner of Canada, "Letter to shadow ministers," 20 August 2020. Available at https://www.priv.gc.ca/en/opc-news/news-and-announcements/2020/let_mps_200820/.

First, such a standard would help alleviate the potential for the overbroad collection and retention of personal information. Federal agencies would be required to set out clear rationales for the necessity and proportionality of their collection and retention activities, and be able to demonstrate adherence both to the public as well as to watchdog agencies such as the OPC.

Second, it would establish a clear framework when analysing new and novel issues regarding privacy and personal information, including technological changes regarding both how personal information is created (ie, social media platform) as well as how it collected and used (ie, AI-assisted tools for gathering information). This could also help address the debate over the need to define all types of personal information or ways it can be collected – both currently and in the pursuit of "future proofing" the *Act*. By relying on necessity and proportionality, each kind of information will be analyzed in a similar way.

It is important to note that the concept of necessity is not novel in the Canadian context, appearing already in provincial privacy rules.[18] Proportionality is included in the EU General Data Protection Regulation (GDPR), the standard bearer for privacy laws internationally, and is rooted in a human rights approach. As the OPC notes:

> Proportionality derives not from administrative law, but from human rights law where it is a well-known concept for balancing infringements of rights against the protection of other rights or important interests.[19]

## UPDATING TERMS

While clearly establishing privacy as a right and framing all use of personal information in terms of necessity and proportionality would represent important safeguards, there are also areas where foundational terms must be updated.

### Personal information

As others have proposed,[20] the current definition of "personal information," is out-dated and should be amended to remove reference to "recorded" information, recognizing that the expectation of privacy is context sensitive and not related how such information is captured.

[18] OPC, "Privacy Law Reform."
[19] *ibid*.
[20] Department of Justice Canada, "Respect, Accountability, Adaptability: A public consultation about the modernization of the Privacy Act," Government of Canada, 2020. Available at: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/raa-rar.pdf.

There has also been question of whether "identifiable" should be defined in the legislation. As pointed out by the Canadian Bar Association (CBA),[21] an exhaustive list of what is considered identifiable would be impossible to establish. Instead, the onus should remain on government agencies to evaluate the context of the collection and retention of information, particularly the necessity of such collection.

**Publicly available personal information:**

It is crucial that the government address the issue of publicly available personal information in an updated *Privacy Act*. Current debates around whether information shared online should be considered "public information" and therefore fair game for collection and use present a grave threat to the privacy rights of individuals and the other associated rights that flow from the exercise of such privacy.

The Supreme Court has already spoken to the fact that privacy is context specific and not an "all or nothing" concept. Specifically, in *Jarvis* they write that "'privacy,' as ordinarily understood, is not an all-or-nothing concept … being in a public or semi-public space does not automatically negate all expectations of privacy."[22] This should also apply to the online sphere, where the context of how and for what purpose information is shared must be considered. As the Office of the Privacy Commission found in a related case regarding the actions of facial recognition company Clearview AI:

> "Information from sources such as social media or professional profiles, collected from public websites and then used for an unrelated purpose, does not fall under the 'publicly available' exception of PIPEDA."[23]

In further statements, the Privacy Commissioner stated that, "The company essentially claims that individuals who placed or permitted their images to be placed on the Internet lacked a reasonable expectation of privacy in such images […] My colleagues and I think these arguments must be rejected."[24]

While this finding was in relation to violations under PIPEDA, the same approach must be applied to the *Privacy Act* and the collection and use of information by federal agencies.

In furtherance of this, the government should consider removing current exclusions under subsection 69(2) so that the entirety of the *Act*'s protections would apply to publicly available personal information.

---

[21] Canadian Bar Association, "*Privacy Act* Modernization," October 2019. Available at: https://www.cba.org/CMSPages/GetFile.aspx?guid=e57b3073-09bd-44a3-91d5-c664b44309f2

[22] 2019 SCC 10 at para. 41.

[23] OPC, "Joint investigation of Clearview AI, Inc."

[24] Office of the Privacy Commissioner of Canada, "Statement by the Privacy Commissioner of Canada following an investigation into Clearview AI," 3 February 2021. Available at: https://www.priv.gc.ca/en/opc-news/speeches/2021/s-d_20210203/.

There is some debate around whether publicly available information should be defined in the *Act*. There could be advantages by having a clear set of criteria of what constitutes publicly available personal information. At the same time, similar to "identifiability," such a definition could fail to capture all types of information. A solution could be to establish, in legislation, the criteria that an agency must consider in regard to publicly available information, without it being framed as exhaustive.

In either case, it must be clear that information cannot be collected simply because it may be considered "publicly available." In drafting new legislation, the government should consider the criteria that the OPC has laid out to be considered when addressing publicly available information:

- Context,
- Reasonable expectation of privacy,
- Accessibility of information, including with new technologies,
- The collecting organizations' obligations for accuracy, currency and completeness.[25]

As above, it must always be shown that the collection, use and disclosure of personal information, public or otherwise, is necessary and proportionate.

Finally, much of the debate on publicly available information has revolved around the ability for law enforcement and intelligence agencies to collect such information without prior authorization. For example, the RCMP has defended its right to collect vast troves of personal information from the internet under the guise of threat prevention without seeking prior judicial authorization.[26] CSIS, for its part, has been granted the power to collect publicly available information as datasets with minimal restriction – including without a specific definition of "public available."[27] It is imperative that rules around the collection and use of publicly available information apply to security and intelligence agencies.

### Other terms, and future-proofing the *Act*

Two other areas where further definition of terms is being debated, both related to technological advancements, is in regards to "biometrics" and "metadata." At various times, our coalition has called for clearer definitions of both to be included in legislation, particularly those governing security agencies themselves (ie, the *CSE Act*, the *CSIS Act*, etc.). This has been in large part to clarify the reasonable expectation of privacy associated

[25] Department of Justice Canada, "Modernizing Canada's *Privacy Act*: What We Heard Report," Summer/Fall 2019. Available online at https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/wwh-cqnae/rep-rap.pdf.
[26] Bryan Carney, "'You Have Zero Privacy' Says an Internal RCMP Presentation. Inside the Force's Web Spying Program," The Tyee, 16 November 2020. Available at: https://thetyee.ca/News/2020/11/16/You-Have-Zero-Privacy-RCMP-Web-Spying/.
[27] International Civil Liberties Monitoring Group, "Brief on Bill C-59, the *National Security Act, 2017*," May 2019. Available online at: https://iclmg.ca/wp-content/uploads/2019/05/C-59-brief-May-2019-update.pdf.

with both these types of data, and to safeguard such data from over-broad collection, use and disclosure.

These arguments have in large part been meant as stop-gaps in a system where privacy laws are not clearly technologically neutral nor "future-proofed." It is therefore possible that, should the *Privacy Act* be reformed in a way to recognize the reasonable expectation of privacy in all forms of data, to incorporate privacy as a right, and to adopt a base-line approach of necessity and proportionality, such specific definitions and safeguards related to individual kinds of data may not be necessary.

At the same time, we would still support greater clarity in the area of these two forms of data. As suggested by the CBA, we would also agree that it would be appropriate to update the list of non-exhaustive examples of personal information to clarify new forms such as metadata and biometric data.[28]

## ACCOUNTABILITY & TRANSPARENCY

In order for any updated provisions in a renewed *Privacy Act* to be effective and impactful, it is crucial that there be significant updates with regards to accountability and transparency measures.

This is particularly important regarding security and intelligence agencies, given their propensity for cloaking in secrecy not just their collection, retention and use of personal information, but also their interpretation of what information carries with it a reasonable expectation of privacy and what surveillance methods are "necessary" or "proportionate."

While this secrecy is defended as being necessary for the effective execution of their mandates, there are multiple examples of these agencies pushing the boundaries of the law and what the public would find reasonable.[29]

In recent years, we have seen increases in review mechanisms, including the establishment of the National Security and Intelligence Agency (NSIRA) and the Intelligence Commissioner (IC). While the IC is a quasi-judicial oversight body, and NSIRA has powers to refer issues to the court, more must be done to ensure the transparency and lawfulness of law enforcement and intelligence agencies' activities overall, including with regards to use of personal information.

---

[28] CBA, "*Privacy Act* Modernization."

[29] See, for example, Bryan Carney, "Keying off Tyee RCMP Revelations, MP Angus Wants an Investigation," The Tyee, 19 November 2020. Available at: https://thetyee.ca/News/2020/11/19/Tyee-RCMP-Revelations-MP-Angus-Wants-Investigation/; ICLMG, "New Revelations Of Spy Agency's Unlawful Activities And Misleading Courts Shows Need For Concrete Action And Accountability," 2 September 2020. Available at: https://iclmg.ca/new-revelations-of-csis-misleading-courts/; ICLMG, "Bill C-59: Mass Surveillance And Cyber Powers," 2019. Available at: https://iclmg.ca/issues/bill-c-59-the-national-security-act-of-2017/bill-c-59s-mass-surveillance-and-cyber-powers/.

**Privacy Impact Assessments**

Privacy Impact Assessments (PIAs) should be mandatory in all instances of initiating or modifying programs that will have an impact on the collection and use of personal information. PIAs should be required to be completed before the start of any new activity, and made public. While security agencies have raised concerns about the time constraints and impact on operational activities, we have seen numerous occasions where lack of PIAs have led to the adoption of new practices that have either violated the law or raised significant ethical concerns. The latest example is the use of facial recognition technology by the RCMP, adopted without a PIA.[30] Similar concerns arise around the RCMP's use of tools to surveil, collect and use social media information.[31]

Along with Privacy Impact Assessments, we would support further, mandatory reporting and transparency. For example, more proactive disclosure regarding what kind of information federal departments collect and what kind of technology is used to collect it. It is important to note that beyond CSIS and the RCMP, the Canada Border Services Agency, the Canadian armed forces, and Immigration, Refugees and Citizenship Canada also collect information for national security purposes and could benfit from additional accountability and transparency rules.

While this may raise concerns around the divulgation of sensitive operational information, this could be offset by, for example, disclosing categories of information and types of technology rather than specifics. Agencies could also publish details about their approach to and management of personal information. Greater transparency could also be brought to information sharing agreements, both between government departments and with third parties. While *SCIDA* requires a certain level of reporting, it does not cover information sharing agreements between federal agencies that fall outside of that act, and does not mandate transparency around the directives and guidelines issued in pursuance of the *Act*. Moreover, despite the existence of guidelines to minimize abuse and mistreatment arising from the sharing and collecting of information, there is even less reporting required with regards to information sharing agreements with private and foreign entities. This should be addressed in an updated *Privacy Act* via new reporting requirements.

At a minimum, it must be made clear in all circumstances that information sharing agreements, even if not publicly disclosed, must be made in writing, must be regularly evaluated for necessity and for impact on rights, must be accessible for evaluation by independent review bodies, and that there must be written records of what information is shared, why, and what measures were taken to ensure accuracy.

[30] ICLMG, "Open Letter: Canadian Government Must Ban Use Of Facial Recognition By Federal Law Enforcement, Intelligence Agencies," 8 July 2020. Available at: https://iclmg.ca/facial-recognition-letter/
[31] Carney, "'You Have Zero Privacy.'"

## Breach disclosure

It is crucial that an updated *Privacy Act* include stringent rules around disclosure when there is a breach of personal information held by government agencies. It is also imperative that such breach disclosures apply to law enforcement and security agencies. It is deeply concerning that in their submissions to the Justice Department during internal consultations, that CSIS argued for exemptions to mandatory breach disclosures.[32] CSIS and the Communications Security Establishment (CSE) have been granted sweeping new powers of data collection, including personal information relating to Canadians, people in Canada, and people outside of Canada. Any breach that results in the disclosure of their personal information risks violating their fundamental rights, and such risk would be exponentially worsened if they are not informed of the breach. This risk greatly outweighs the risk to the operations of Canada's security agencies. It must be noted that if CSIS were granted such an exemption, it would likely be extended to include other departments involved in security-related activities, including those previously listed (immigration, armed forces, etc.), creating a troubling precedent that would undermine the goal of any breach disclosure policy.

If these agencies wish to enjoy the privilege of collecting, retaining and using personal information of individuals, all without disclosing these activities, they must accept the consequences of those actions when a breach occurs. It should be incumbent upon them to establish clear provisions that would comply with breach disclosure legislation while maintaining the integrity of their operations. Under no circumstances should there be a blanket exception, nor should there be an allowance to delay breach disclosures indefinitely.

## Algorithmic decision-making

In line with the provisions included in Bill C-11, we would support new guidelines around the use of artificial intelligence and/or algorithmic decision-making by federal agencies. As more departments use this technology to make decisions that can have deep implications for an individual's livelihood, it is imperative that there are legislated rules around its use. We must ensure that decisions are not allowed to be simply derived from "black box" algorithms that can neither be explained nor challenged.

This should include public disclosure when such tools are being used, independent review and oversight of the algorithms being used, public reporting of findings, ability to request the information used in rendering a decision, the ability to request human review of a decision, and the ability to challenge decisions reached algorithmically.

Further, it is conceivable that certain kinds of sensitive decision-making should not be subject to algorithmic decision-making, particularly those that raise fundamental questions

[32] Jim Bronskill, "CSIS says proposed federal privacy reforms could hinder spy operations," The Canadian Press, 17 May 2020. Available at: https://www.theglobeandmail.com/canada/article-csis-says-proposed-federal-privacy-reforms-could-hinder-spy-operations-2/.

of liberty or security of the person. This must be examined before any new legislation is proposed.

Finally, it is important again to note that such rules are particularly important when it comes to security and intelligence agencies, given the significant impact the actions of the agencies have on the rights of people both within and outside of Canada.

**Powers of the Privacy Commissioner**

Finally, we support calls for stronger enforcement mechanisms in the *Privacy Act* that would help ensure compliance across government agencies and allow for timely and effective remedies for individual complaints. We believe this should include allowing the Privacy Commissioner to conduct proactive inspections, enter into compliance agreements with federal agencies and make binding orders to ensure compliance with the law.

Increased enforcement powers should be established to run alongside, and not replace, the OPC's consultative function for agencies seeking out advice. In fact, this consultative and guidance role could be strengthened by granting the OPC a clearer mandate for making advance rulings and/or advisory opinions.

The rationale and need for new enforcement mechanisms have been documented by both the OPC[33] and by the Justice Department.[34] Our coalition has also taken note of various incidents where law enforcement and intelligence agencies have either ignored or delayed implementing guidance from the Privacy Commissioner. For example, the RCMP has agreed to provide the OPC with an audit of its social media surveillance operations, but has yet to do so.[35] Greater enforcement powers would allow the Privacy Commissioner to address these issues in a timely and clear fashion.

[33] OPC, "Privacy Law Reform."
[34] Department of Justice Canada, "*Privacy Act* Modernization: A Discussion Paper," 21 August 2019. Available at: https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/pdf/dp-4.pdf.
[35] Jim Bronskill, "RCMP defends practice of profiling people by scouring their online presence," The Canadian Press, 2 January 2020. Available at: https://globalnews.ca/news/6360410/rcmp-social-media-profiling/.