CANADIAN CIVIL LIBERTIES ASSOCIATION ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission to the Special Committee to Review the *Personal Information Protection Act* in the Province of British Columbia

August 14, 2020

Canadian Civil Liberties Association

90 Eglinton Ave. E., Suite 900

Toronto, ON M4P 2Y3

Phone: 416-646-1406

www.ccla.org

Table of Contents and Summary of Recommendations

Introduction

The Canadian Civil Liberties Association ("CCLA") provides these submissions to the Members of the Special Committee to Review the Personal Information Protection Act ("Committee"), for consideration in your review of the *Personal Information Protection Act* ("*PIPA*" and "the Act").

The CCLA is an independent, non-governmental, non-partisan, non-profit, national civil liberties organisation. Founded in 1964, the CCLA and its membership promote respect for and recognition of fundamental human rights and civil liberties. For fifty years, CCLA has litigated public interest cases before appellate courts, assisted Canadian governments with developing legislation, and published expert commentary on the state of Canadian law.

The *Personal Information Protection Act* (*PIPA*)1, BC's private sector privacy legislation, is a critical component of the provincial privacy protection regime. Increasingly, as a result of technological advances and evolving business models that rely on rich and detailed data streams about individuals, organisations large and small are collecting more and more personal information about Canadians. Indeed, over the past decade, the "[m]onitoring of individuals now has a routine character, assumed as being a condition of participation in modern life and as the way that we engage with modern public and private organizations."2 However, simply because such monitoring has become routine does not mean that it is either desirable or inevitable. It is incumbent upon us, as a society, to envision and enact social, political, and consumer environments that we believe are just. A stronger, more effective, and better enforced *PIPA* is needed to provide appropriate controls on the private sector use of personal information, to provide residents of BC with the assurance that they may browse, shop, opine—in other words, participate fully—in contemporary life online and trust that the appropriate safeguards are in place to protect not only the information they knowingly provide, but also the information such systems collect or infer about them based on their actions and behaviour.

The root of any successful legal regime is its adaptiveness. Principle-based, technologically-neutral privacy law has served British Columbians well, and CCLA believes this approach remains fundamental to allow the law to remain relevant in the face of rapidly evolving technologies and innovative data uses. At the same time, new, principled protections and some basic updates to align *PIPA* with other privacy laws in Canada are clearly necessary at this time. With this in mind, the CCLA offers the following submissions to the Committee in order that the Committee might be better able to make recommendations that protect fundamental privacy rights in British Columbia.

[1] *The Personal information Protection Act,* SBC 2003, c 63. ("*PIPA*")

[2] Colin J Bennett & Robin M Bayley, "Canadian Federal Political Parties and Personal Privacy Protection: A comparative analysis" (Ottawa: OPCA 28 March 2012) at 4 (emphasis in original).

Previous Special Committee Reviews

To date, the Committee has done two comprehensive reviews of the Act, one in 2007 and another in 2015. The 2007 review generated 31 recommendations concerning accountability for cross-border data flows, mandatory notification of privacy breaches[3], consent provisions, definitions, exceptions to consent access-related topics, oversight provisions, and general provisions.[4] The 2015 review led to an additional 15 recommendations, covering disclosure of security breach, the use of personal information in witness statements, fees, responsibilities for transferring information to a third party, development of new health information and privacy laws, and implementing the recommendations in a timely manner.[5] Since the 2007 review, *PIPA* has received minor amendments but no major updates in response to the critical deficiencies noted in the previous two reviews.

This Committee should regard these previous reviews as setting a benchmark for where its recommendations should begin: *PIPA* is out of date. It has been out of date for at least ten years. The cost of the law's being out of date have only grown since it was first reviewed and now the anachronistic law levies a severe toll on the province.

A human rights-based approach to privacy law

The CCLA believes that the first step in re-imagining Canada's private sector privacy regime is to strengthen *PIPA*'s commitment to privacy as a human right. Particularly in the private sector context, where individuals have far less power than the companies with which they interact, a human rights framework will help to level the imbalance by adding weight to individual claims.

The Supreme Court of Canada has affirmed the quasi-constitutional status of both federal and provincial privacy legislation, and recognized that we need privacy in order to fully enjoy other rights protected by Canada's *Charter of Rights and Freedoms*, including free expression and equality rights. Canada is a signatory to the *Universal Declaration on Human Rights*[6] and Article 17 of the *International Covenant on Civil and Political Rights*,[7] which both recognize privacy as a human right, and the latter of which specifically protects against privacy incursions by private

[3] The CCLA echoes the concerns of the BC CBA, BC FIPA, and others who spoke to the Committee about how British Columbians need a right to proactive notification about when their privacy has been breached (i.e. "mandatory breach notification").
[4] British Columbia, Legislative Assembly, "Streamlining British Columbia's Private Sector Privacy Law", Special Committee to Review the Personal Information Protection Act (April 2008).
[5] British Columbia, Legislative Assembly, "Special Committee Report to Review the Personal Information Protection Act", Special Committee to Review the Personal Information Protection Act (February 2015).
[6] "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." Online: <https://www.un.org/en/universal-declaration-human-rights/>.
[7] "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." Available at: UN General Assembly, International Covenant on Civil and Political Rights, 16 December 1966, United Nations, Treaty Series, vol. 999, p 171, online: <https://www.refworld.org/docid/3ae6b3aa0.html>.

actors and corporations.[8] Yet *PIPA*, and other Canadian privacy legislation, frame privacy in terms of data protection principles, not the prerequisite for freedom, dignity, and autonomy that it is. In an age of increasing capacity for information about us to be used by corporate entities in ways hard to see, understand, or predict, British Columbians deserve privacy protections that defines privacy as a right they deserve, not a commodity to be bartered or balanced with a corporate interest. This is not to say that there are not legitimate commercial and organisational interests in information, or that there are not social benefits to a thriving and innovative information-based economy. However, there is also an emerging public trust deficit that corporations will use information fairly or transparently that we suggest could be mitigated by legislation that explicitly protects privacy as a right and creates obligations to protect that right.

The federal Privacy Commissioner champions this rights-based approach for reform of the *Personal Information Protection and Electronics Documents Act* (*PIPEDA*)[9], which is relevant for *PIPA*'s status as legislation deemed substantially similar. At the outset, recognition of privacy as a right should be integrated into section 2 of *PIPA*, the section that describes the legislation's overarching purpose. Section 2 is especially important because courts look to a law's overall purpose when interpreting any of its provisions; however, it currently qualifies the right to privacy against the needs of organizations to collect, use, and disclose personal information.

Amending *PIPA* 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,[10] although it is still fundamentally a data protection instrument. Bringing *PIPA* more in line with the GDPR would be beneficial because the EU makes the adequacy of Canadian privacy legislation a precondition for continued transborder data flows.[11]

Recommendation 1: Amend *PIPA* to explicitly recognise privacy as a human right in its statement of purpose.

Evolving Risks to Privacy Make *PIPA* Reform Urgent and Imperative

Evolving and emerging technologies, along with business models built around a relatively unregulated flow of behavioural information gleaned from online interactions, increasingly highlight principled gaps in our existing privacy legislation, and *PIPA* is no exception.

While CCLA supports principle-based, technology neutral privacy legislation, it is nonetheless true that these new technologies require, in some cases, new principled approaches to privacy protections as the quantity and quality of information collected about individuals increases and the

[8] UNHRC, CCPR General Comment no. 16: Article 17 (Right to Privacy), the Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988).
[9] SC 2000, c 5 [*PIPEDA*].

potential uses similarly expand. Conversely, the problems raised in some cases, particularly those raised by over-collection of information beyond that required for the purpose of supplying the product or service, or vague privacy policies that fail to adequately inform users to the level necessary for genuinely informed consent, should already, ostensibly, be prohibited by the current law. In those cases, gaps in the regulator's powers of enforcement are laid bare.

The following section discusses select technologies as a means to illustrate new issues requiring principled additions to the Act, or to discuss ways in which the changing capabilities and economic models for technological products exacerbate ongoing problems and makes a series of recommendations to address the identified concerns.

Biometrics including Facial Recognition

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 resource that facial recognition services now use to train their software for free. 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 invites the Committee to update the Act.

The nature of biometric data makes it challenging to regulate. Whereas many new privacy-involving technologies can be actively consented to by the user, it is difficult to both give users notice of many biometric services and an opportunity to consent to its use. For example, cameras used in facial recognition technology can passively capture images of people from far away, so in most cases there is no notice, no consent, and the data collection is done surreptitiously.[10] Although in some situations, such as in bars or malls, a person might be deemed to have implicitly consented to this kind of biometric data collection technology by entering the space, not all privacy experts think this suffices for consent. Tunca Bolca argues that the idea of informed consent over this type of data collection amounts to a failure to respect privacy, since everyday users cannot be assumed to understand the privacy practices to which they are consenting.

Other North American jurisdictions are already leading on this issue. In Illinois, the Biometric Information Privacy Act (BIPA)[11] 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. Monetary penalties for violating the Act are levied for

[10] 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.
[11] 740 ILCS 14.

each reckless or negligent violation. The law has empowered children (represented by guardians) to bring a class action suit against Google for its alleged mass collection of their biometric data.[12] California is also breaking ground in protecting biometric data privacy with The California Online Privacy Protection Act of 2003 (CalOPPA).[13] Pursuant to CalOPPA, commercial websites that collect personally identifiable information of California's residents must conspicuously post and comply with a privacy policy. A website operator who fails to post their privacy policy within 30 days of being notified about noncompliance will be deemed to have violated the law. This applies regardless of whether the offending website or its operator was based in California—the law crafts a global remedy to a problem that can arise from anywhere on the globe. Taken together, BIPA and CalOPPA show how the frontier for consent is shifting away from implied consent and towards pro-active notification requirements and consumer protection.

PIPA's framework for implicit consent does not specifically address the challenges to personal privacy posed by the collection of biometric data. Given the particular sensitivity of such information which is uniquely personal, based on attributes of individual bodies, the Committee might wish to consider providing specific recommendations relating to biometric data collection technologies.

Recommendation 2: Amend *PIPA* 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 *PIPA* amendments.

Artificial Intelligence

Automated Decision Making

Automated processing used for decisions about people can have negative effects: algorithms are not neutral and often import the biases of their designers or encourage existing discrimination.[14] For example, online app stores have associated popular dating apps for gay men with sex offender registry lists,[15] while women are shown fewer ads for high-paying jobs than men.[16] These built-in biases can have serious consequences when algorithms are used in high-stakes situations – for example, an Israeli start-up named Faception purports to be able to identify terrorists on the basis of AI analysis of facial features, and the company claims to have already contracted its technology

[12] See *H.K. v. Google*, LLC, 5:20-cv-02257.
[13] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).
[14] See, for e.g., Gideon Mann and Cathay O'Neill, "Hiring Algorithms Are Not Neutral." *Harvard Business Review*. (9 December 2016). Online: <https://hbr.org/2016/12/hiring-algorithms-are-not-neutral>.
[15] 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/>.
[16] Byron Spice, "Fewer Women Than Men Are Shown Online Ads Related to High-Paying Jobs," Carnegie Mellon University School of Computer Science (7 July 2015), online: <https://www.cs.cmu.edu/news/fewer-women-men-are-shown-online-ads-related-high-paying-jobs>.

to an unnamed homeland security agency.[17] The lack of transparency in automated processing further complicates matters – AI decision-making has often been described as a "black box" that even the AI's designers cannot explain.[18]

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. 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 *PIPA* in line with Articles 21 and 22 of the GDPR.

Recommendation 3: Amend *PIPA* to contain a right to be informed about the use of automated decision-making processes they are subject to, a right to object to automated decision-making, a right to correct personal information used to make decisions about them, and should not to be subject to decisions based solely on automated processing.

Explainability and Transparency

One of the greatest concerns about AI from a privacy perspective is the inability for individuals to gain a sufficiently clear understanding of the ways their information may be used in AI applications. *PIPA* should include a provision requiring any company 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 – companies 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 corporate accountability - corporations 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

[17] Sue Surkes, "New Israeli facial imaging claims to identify terrorists and pedophiles" *The Times of Israel.* (May 24, 2016). Online: <https://www.timesofisrael.com/new-israeli-facial-imaging-claims-to-identify-terrorists-and-pedophiles/>.

[18] See, for e.g., Bathaee, Yavar. "The Artificial Intelligence Black Box and the Failure of Intent and Creation" *Harvard Journal of Law & Technology*, Volume 31, Number 2 Spring 2018, online: <https://jolt.law.harvard.edu/assets/articlePDFs/v31/The-Artificial-Intelligence-Black-Box-and-the-Failure-of-Intent-and-Causation-Yavar-Bathaee.pdf>.

also increase, since individuals would have the confidence that they knew what factors went into each decision-making process.

Recommendation 4: Amend *PIPA* to include a right to explanation and increased transparency every time an individual interacts with or is subject to automated processing.

The Internet of Things

The 'Internet of Things' refers to 'smart' objects that are connected to the internet and often to one another as well, creating surveillance networks that gather information about private individuals. Products such as 'smart' fridges, smart watches, and intelligent home hardware like thermostats are examples of such devices. Such devices are marketed as providing benefits based on their ability to "learn" and respond to human behaviours, yet it is not always clear how much of the information collected by such devices is necessary for device functionality, and how much is an additional revenue stream, or contributory to a secondary purpose such as new product development. Consent on many such devices consists of installing it or plugging it in, as many 'smart' devices do not even have an interface by which one could obtain explicit consent. These objects may breach *PIPA*'s rules about implicit consent under section 8 of the Act.

Systemic inattention to privacy and security has also led these products to be reliable portals by which hackers and private surveillance can breach individuals' privacy, as documented by a growing body of media reports and research on breaches on devices ranging from baby monitors[19] to connected cars.[20] In this regard, the absence of breach notification provisions in *PIPA* becomes particularly concerning given that other private sector laws elsewhere in Canada provide such protection for residents of their jurisdictions.[21]

Recommendation 5: Amend *PIPA* to include mandatory breach notification where there is a risk of significant harm to an individual, language which aligns with *PIPEDA*.[22] The Commissioner should have powers to compel notification where necessary.

De-identified Information

Since *PIPA* 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 *PIPA*,

[19] The Nest baby monitor camera came to media attention, for example: <https://www.washingtonpost.com/technology/2018/12/20/nest-cam-baby-monitor-hacked-kidnap-threat-came-device-parents-say/>.
[20] Some of the concerns regarding connected vehicles are documented in a recent Consumer Watchdog report, online: <https://www.consumerwatchdog.org/sites/default/files/2019-07/KILL%20SWITCH%20%207-29-19.pdf>. Past work funded by the Office of the Privacy Commissioner of Canada and conducted by the BC FIPA has assessed the compliance of connected vehicles with Canadian privacy legislation. See: <https://fipa.bc.ca/2019-update-to-the-connected-car/>.
[21] *PIPEDA* requires federally regulated organisations to report personal information breaches to the Privacy Commissioner (s 10.1) as does Alberta's Personal Information Protection Act (s 34.1). Quebec's recently introduced Bill 64 introduces a breach notification provision also.
[22] *PIPEDA*, sections 10.1 and 10.2.

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.[23] First, the mosaic effect involves piecing 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.[24] 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.[25] Second, pattern-spotting can re-identify large "de-identified" datasets because of the uniqueness of human behaviour.[26] 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.[27] 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 *PIPA*. 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.[28] CCLA prefers a higher standard than "serious possibility", given the risks outlined above regarding re-identification. The text of *PIPA* should therefore be amended to reflect that "supposedly de-identified data can only be excluded from the scope of *PIPA* if it can be proven beyond a reasonable doubt (or potentially, to an formally established industry standard) that the data can never be re-identified."

This is not to suggest that de-identification does not provide a form of privacy protection, only that it does not and should not take personal information subjected to such processing outside of the scope of *PIPA* to regulate. To that end, we echo the recommendations of the BC FIPA and BCCLA that the terms "de-identified information," "anonymized information," "pseudonymized

---

[23] 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>.
[24] 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>.
[25] *Ibid.*
[26] 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/>.
[27] 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).
[28] *PIPEDA* Case Summary #2009-018, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2009/*PIPEDA*-2009-018/>.

information," and "aggregate information" be clearly defined in *PIPA*, and that specific requirements for such information be established.

Recommendation 6: Amend *PIPA* to cover all "de-identified data" unless it can be proven beyond a reasonable doubt that the information is truly de-identified.

Recommendation 7: Amend *PIPA* to clearly define "de-identified information," "anonymized information," "pseudonymized information," and "aggregate information".

Recommendation 8: Organisations who wish to de-identify personal information should be required to inform data subjects regarding how they de-identify data, and about the level of risk that data could be re-identified.

Recommendation 9: 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 companies are alleged to fail to adhere to such standards.

Aggregate Information

The privacy risks of data aggregation have relatively recently been highlighted in a different context—the official *Charter* analysis for Bill C-59, now Canada's *Act respecting national security matters*—which notes: "Considering the information about individuals that can be aggregated, and the things that can be learned from such aggregations using modern technologies and then offered for sale by data-brokers, CSE's acquisition and use of such information . . . has the potential to affect privacy interests protected by section 8 of the Charter."

If there is cause for principled concern that the nature and scope of information to be gleaned from data aggregation engages privacy interests in a public safety context, it seems reasonable that some of the same concerns remain when data aggregation is used by the private sector. The CCLA believes that consumers have a right to know when their information is being aggregated in this way, and that the onus should be on companies who collect it during a primary transaction, but then share or sell it for secondary uses, to make the processes and the privacy risks transparent. Without this information, consumers cannot grant meaningful consent for these practices. Users who prefer not to allow secondary uses of their data should minimally be allowed to opt out, and ideally asked to opt in.

Recommendation 10: Users should be informed of when their data will be aggregated and sold, and allowed to opt in or out of secondary uses of data unnecessary for the provision of the primary service provided.

Enhanced Privacy Protection for Specific Vulnerable Groups

Not all people are at equal risk of discriminatory impacts when information about them is collected, used or disclosed. The following discussion identifies two groups where there is a particularly significant power differential between collectors of information and group members, and makes recommendations to ensure *PIPA* provides strong protections to mitigate the risks of that imbalance.

Employee Privacy

Under the BC *PIPA*, employers may collect, use, and disclose personal information for the general purpose of managing an employment relationship so long as the collection, use, and disclosure of the information is reasonable. Employers may in some cases collect information about their employees without their employees' consent.[29] This poses a challenge for privacy in the workplace, particularly given the rapid development and refinement of new workplace surveillance tools, combined with shifting perceptions of what information it is indeed, in the language of *PIPA*, "reasonable" to collect for purposes of establishing, managing or terminating an employment relationship."[30] This warrants consideration of ways to appropriately constrain information collection about employees, either by revising the reasonableness standard, providing better protections embedded in the statute for workers who wish to challenge the reasonableness of any particular form of collection, or both. The COVID-19 pandemic highlights this concern, as many workplaces are looking to institute programs such as temperature screening, contact tracing, and location monitoring which may expand the information employers wish to routinely collect to sensitive biomedical and location data, potentially including information collected outside the workplace,

There are addition concerns about workers' privacy rights which are uniquely relevant in the COVID pandemic when many workers must work from home. Where workers are monitored in their own homes, workplace surveillance becomes home surveillance. There is a significant risk that work productivity monitoring tools will incidentally collect information about workers' personal lives, family members, and homes, especially given that many remote workers use their own computers.[31] The Committee should therefore pay special attention to what the COVID and post-COVID eras will mean for workers' privacy in British Columbia.

[29] Avner Levin, "Big and Little Brother: The Potential Erosion of Workplace Privacy in Canada" (2007) 22 Can JL & Society.
[30] *PIPA* s 13(1) (b).
[31] Kris Klein & Dustin Moores, "Privacy Issues Arising from the COVID-19 Pandemic", 3 Emerging Areas of Practice Series-COVID-19 (Coronavirus), (2020).

Recommendation 11: Consider whether the reasonableness standard for collection of employee information, particularly without consent, provides sufficient guidance for employers and appropriate protections for workers, particularly in light of the power imbalance between them which may be exacerbated by contemporary workplace surveillance tools.

Recommendation 12: Employers should have a positive legal duty to ensure both that their workers are aware of how they are monitored and that any tools for monitoring workers are not unduly burdensome on workers' privacy. Moreover, there should be a presumption that information gathered incidentally about remote workers via workplace monitoring tools is not admissible in core employment decisions, such as hiring, firing, or adjustments to compensation.

Youth Privacy

One of *PIPA*'s most significant gaps is its lack of safeguards for young people's privacy. There are currently no safeguards in place in *PIPA* that address young people's specific privacy needs. Whereas the federal privacy commissioner has stated that a minors' consent may be gathered from a minor's legal guardian under *PIPEDA*, *PIPA* offers no comparable framework.[32] *PIPA* does not mention information specific to underage children or whether they can legally consent to the collection, use, and disclosure of their information.[33] Given that young people now access the internet in their homes, at libraries, at school, or anywhere else with their phones, it is imperative that *PIPA* be revised to protect minors who may not know or comprehend the potential risks or exposures they create for themselves or their families when sharing information online.

Many Canadian firms have echoed the *American Children's Online Privacy Protection Act* (*COPPA*) by requiring that users consent to their data being collected, that their data being shared with third parties, and which attempt to get verifiable parental consent from users under 13 years old.[34] These efforts have run into three main problems. First, many firms attempt to follow these requirements by relying on generic statements advising users that their websites are not intended for children. This approach lacks mechanisms to ensure accountability and is critically undermined by the fact that many children lie about their ages. Second, even where individuals' user data is aggregated and anonymized, we should worry about the bulk collection and trade of children's private information. This worry becomes more pressing when we consider how aggregated data is often used to manipulate users online, either by tailored advertisements or, more perniciously, by tailored political and ideological messaging.[35] Commentators suggest that privacy laws, like *PIPA*, can be amended to declare that the collection of children's personal information for the purposes

[32] Valerie Steeves, "It's not Child's Play: The Online Invasion of Children's Privacy" (2006) 3 U Ottawa L & Tech J.
[33] Agathon Firic, "Access of Evil? Legislating Online Youth Privacy in the Information Age" (2014) 12 Can JL & Tech.
[34] Valerie Steeves, *Children's Privacy-Overview of the Federal Legislative Landscape*, (1 July 2009), online: <https://www.researchgate.net/publication/289839778_Children's_Privacy_-_Overview_of_the_Federal_Legislative_Lanscape>.
[35] See: Colin Bennett, "Politicians must defend Canadians' online privacy from Big Tech – and from politicians themselves", *The Globe and Mail* (26 December 2019), online: <https://www.theglobeandmail.com/opinion/article-politicians-must-defend-canadians-online-privacy-from-big-tech-and/>.

of targeting their behaviour is unreasonable and prohibited.[36] The third problem with this approach is simply how heavily it relies on users' consent. The issue of whether and how a given youth user has consented to their data being collected and used by third parties could be sidestepped entirely by a rule against youth's information being collected and used this way at all. If consent must be a part of *PIPA*'s regime for youth privacy, however, then the act would be improved by the addition of an *COPPA*-like model for parental consent, with an express opt-in requirement for behavioural targeting practices.

There are two other models for youth privacy protections that the Committee should consider. The first is a stepped process, where young children would not be eligible to have their data collected, older children could only have their data collected with express parental consent, and teenagers could consent to their data being collected, but not distributed without parental consent.[37] This would balance youths' privacy interests with parental rights and a default presumption in favour of youths' privacy. The second model would be to give youths the right to delete all data previously collected about them once they reach the age of majority, a "get out of targeted marketing free!" card. Each recommendation could be included in *PIPA* without significantly altering the structure of the Act.

Research indicates that parental consent models should only be one part of the regulatory regime protecting youths' privacy. This is because even high levels of parental supervision have only ever been found to reduce the risk to youth's privacy caused by access to the internet, not eliminate it. The Committee should therefore consider itself to have both the prerogative and means to safeguard youths' privacy in digital spaces.

Recommendation 13: Create a regime within *PIPA* for protecting youths' privacy that takes account of youths' particular needs and interests. Younger and more vulnerable children need stronger privacy protections and older youths should have a right to control data about their persons gathered before they reached the age of majority.

[36] See: Steeves. This conclusion is supported by the Supreme Court of Canada's seminal decision in *The Attorney General of Quebec v Irwin Toy Limited* [1989] 1 SCR 927, where the Court found that Quebec could lawfully prohibit "commercial advertising directed at persons under thirteen years of age" without unjustifiably infringing on retailer's freedom of speech and expression.
[37] See: Steeves *Ibid*.

Additional measures to enhance accountability

Alternatives to Informed Consent

Informed consent supports individual control and autonomy and thus consent requirements—already supported in *PIPA*—should not be weakened. CCLA adopts the position of the BC Freedom of Information and Privacy Association (BC FIPA) and the BC Civil Liberties Association (BCCLA) in their submission before this Committee on the importance of enhanced protections for meaningful and informed consent.

There are, however, increasingly conversations emerging regarding alternative grounds for information processing in addition to informed consent. In particular, one ground sometimes debated is that of "socially beneficial uses" or, in a report produced by the Internet Accountability Foundation for the Canadian Ministry of Innovation, Science and Economic Development, "people beneficial data activities."[38] CCLA cautions that while there may be a role for such concepts, in specific circumstances defined in legislation, such amendments should not be made without a serious public debate regarding what constitute socially beneficial uses of information. CCLA rejects the notion that the public interest can be weighed against privacy rights – privacy rights are central to the public interest. Instead, any new ground of processing should be tested for being in accordance with the public interest, which includes the degree to which the new ground respects privacy rights. Commercial and public assessments of what is socially beneficial may vary sharply; for example, while a company might argue that their economic success results in a stronger tax revenues which benefit a local population, individuals might not feel that benefit accrues broadly enough to warrant non-consensual use of their personal information. In other words, it matters a great deal how public interest is defined, which body defines it, and the quality of mechanisms for redress or dispute resolution. In all cases, however, commercial interests cannot abrogate a clear privacy interest, and any new ground for processing should be as minimally privacy invasive as possible.

Recommendation 14: Any consideration of alternative grounds for processing, in lieu of informed consent, for socially beneficial purposes should require public debate and safeguards to ensure acceptable definitions of "public interest" or "social benefit" form the basis of the legislative provision authorising such processing.

Third Party Outsourcing

Another salient gap in *PIPA* is a requirement that when an organization transfers data to a third party, the transferring organization must ensure that the third party will observe a similar level of

[38] Information Accountability Foundation, *A Path to Trustworthy People Beneficial Data Activities: A report prepared for Innovation, Science and Economic Development Canada*, March 2020. Online: <https://b1f.827.myftpupload.com/wp-content/uploads/2020/04/People-Benefical-Data-Report-and-Recomendations-IAF-v3.pdf>.

privacy protection as the transferring party. Both previous Committee reviews spoke to this issue. Under *PIPEDA*, when organizations are transferring data for processing to a third party, the organization must ensure that there is a comparable level of privacy protection for the data through contractual or other means by the third party.[39] *PIPA*, however, lags behind the federal standard by only requiring that organizations must protect personal information by making "reasonable security arrangements". Whether or not this standard equals *PIPEDA*'s requirement in practice, British Columbians would be better protected were *PIPA* amended to more explicitly reflect *PIPEDA*'s standards for third party outsourcing.

Recommendation 15: CCLA endorses the Committee's previous recommendations that *PIPA* be amended to expressly provide that organizations are responsible for the personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization; and that organizations must use contractual or other means to ensure compliance with *PIPA*, or to provide a comparable level of protection, for personal information they transfer to a third party for processing or for providing services to or on behalf of the transferring organization.

Exemptions

PIPA provides for exemptions for the collection, storage, and disclosure of information for a broad and varied range of purposes, including personal or domestic use, and artistic, literary, or journalistic reasons.[40] Some expert commentators argue that these exemptions are too wide—that they do not capture a wide range of privacy-invading conduct.[41] This concern is rooted in how the statutory exemptions are *jurisdictional*: if they happen to apply then *PIPA* provides no other jurisdiction within which to impose restrictions on an organisation dealing with personal information.

Given these blanket exemptions, it would be prudent for the Committee to review the exemptions to ensure that they comport with the realities of today's personal information technologies. When the exemptions were drafted, smart phones were not common, and Facebook did not exist. These regulations should therefore be reviewed in the context of today's technology and the prospects for its growing adoption.

Recommendation 16: It would be beneficial to review and update *PIPA*'s exemptions for the collection, storage, and disclosure of information to reorient them around contemporary personal information technologies.

[39] Principles set out in the National Standard of Canada entitled *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-96 section 4.1.3. Also see Michael Geist & Milana Homsi, "Outsourcing Our Privacy: Privacy and Security in a Borderless Commercial World" (2005) 54 UNB LJ.
[40] *PIPA* at 3(2)(b).
[41] Chris DL Hunt, "Forum Topic: An Update in the Law of Privacy The Common Law's Hodgepodge Protection of Privacy" (2015) 66 UNBLJ 66.

Support for Recommendations submitted by other parties

CCLA commends the Committee and wishes to express its support for the following recommendations for *PIPA* amendments made in submissions by the BC FIPA and the BCCLA, reproduced below:

Recommendation: In order to maintain meaningful consent, *PIPA* should be amended to require organizations to provide the purpose of collection to individuals at the time of collection, in a manner that is specific, accessible, and understandable.

Recommendation: Amend *PIPA* to specify that an organization's privacy policies must be accessible and understandable, as defined in their submission.

Recommendation: Amend *PIPA* to require that an organization's privacy policies be publicly available, rather than available on request.

Recommendation: Amend *PIPA* to require organizations to perform mandatory PIAs, to enhance transparency and accountability by organizations. In accordance with this, the Commissioner should be empowered to require an organization to produce reports of these assessments when necessary. The frequency, content, and reporting requirement of PIAs should be defined by regulations.

Recommendation: Amend *PIPA* amended to require an organization to seek consent from an individual before transferring their personal information outside of Canada.

Recommendation: Amend *PIPA* to provide the Commissioner with the ability to issue administrative monetary penalties for non-compliance.

Recommendation: Amend *PIPA* so that where the Commissioner conducts investigations without a complaint, they have order-making powers for non-compliant organizations.

Conclusions

PIPA is out of date and in dire need of revision. BC has an opportunity for leadership in privacy protection, a role the province has taken in the past and may wish to embrace once again. While the federal government's long-promised modernisation of *PIPEDA* has yet to materialise, it remains imperative that *PIPA* anticipate the need to provide superior or substantially similar privacy protections for BC residents

The stakes are clear; in BC FIPA's recent survey of British Columbians, only 43% of respondents believed that existing laws and organisational practices provide sufficient protection for their personal information.[42] Strong, modern, effective privacy legislation is required to counter that trust deficit.

The CCLA thanks the Committee for the opportunity to make this submission and to contribute to its timely and important review of BC's *PIPA*.

[42] BC Freedom of Information and Privacy Association, "British Columbians want action on privacy protection: Polling results", (3 June 2020), online: <https://fipa.bc.ca/category/libraries/publications/publication-types/surveys-and-polling/>.