CANADIAN CIVIL LIBERTIES ASSOCIATION

ASSOCIATION CANADIENNE DES LIBERTES CIVILES

Submission regarding Ontario Private Sector Privacy Reform: Improving Private Sector Privacy for Ontarians in a Digital Age

October 16, 2020

Tashi Alford-Duguid, Articling Fellow

Brenda McPhail, Director, Privacy, Technology & Surveillance

Canadian Civil Liberties Association

90 Eglinton Ave. E., Suite 900

Toronto, ON M4P 2Y3

Phone: 416-646-1406

www.ccla.org

Ontario Private Sector Privacy Reform: CCLA's Response to Discussion Paper

Introduction

The Canadian Civil Liberties Association ("CCLA") provides these submissions for consideration in the review of Ontario's new framework for privacy in the private sector.

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.

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. 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."[1] However,

[1] Colin J. Bennett and Robin M. Bayley, "Canadian Federal Political Parties and Personal Privacy Protection: A Comparative Analysis" Commissioned by the Office of the Privacy Commissioner of Canada (March 2012),

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. Ontarians need controls on private sector use of personal information to assure them that they may browse, shop, opine—in other words, participate fully—in contemporary life. They should be able to 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.

Ontario's privacy regime today is a composite of federal law, primarily the *Personal Information Protection and Electronic Documents Act* ('PIPEDA'), and various provincial laws, including the *Freedom of Information and Protection or Privacy Act* ('FIPPA'), *Municipal Freedom of Information and Protection of Privacy Act* ('MFIPPA'), and *Personal Health Information Protection Act* ('PHIPA'). Taken together these laws leave critical gaps in Ontarians' privacy protections, such as privacy protections for employees of non-federally regulated enterprises. Moreover, this regulatory regime is undermined by a more fundamental weakness: Ontario's privacy laws are advanced—or more often neglected—by the federal Parliament's intermittent upkeep of PIPEDA. As a result, Ontario is already falling behind both Québec, where Québec's National Assembly is considering an ultra-modern privacy draft law in Bill 64, and international comparators.

This review offers Ontario a chance to not just repair gaps in its privacy regime, but to become a privacy leader too. While CCLA acknowledges that there will be legitimate concerns from businesses about new compliance requirements in an already complicated regulatory landscape, privacy leadership is a precious opportunity at a time when public trust in technology and in political leadership's capacity or will to ethically guide its development is fragile. Jim Balsillie's statement that "data is the new plutonium"[2] is an apt promise and warning, expressing both the potential and incredible risks involved in using personal information to power the data and innovation economy. When access to—and use of—private information is unregulated, people are vulnerable to abuse and exploitation, while the profits from its use and control flow elsewhere. The social license needed by Ontario government to promote innovation potentially fueled by Ontario data will not be granted by residents without an assurance of meaningful privacy protections. In the CCLA's view, the best way to protect the right to privacy and nurture Ontario's modern economy is with a principled, adaptive, and modern privacy law enforced by an empowered Information and Privacy Commissioner. With its 14 million inhabitants, Ontario is both rich in personal data and ripe for exploitation—privacy must therefore be a guiding priority for Ontario's government.

Privacy leadership would also give Ontario a competitive advantage both in North America and around the world. The EU's General Data Protection Regulation ('GDPR') has set a new high bar for privacy. By leveling-up Ontario's privacy regime, Ontario keeps open a commercial bridge to

available online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2012/pp_201203/>.

[2] Jim Balsille, Testimony to the *International Grand Committee on Big Data, Privacy and Democracy*, *Financial Post* (28 May 2019), available online: <https://financialpost.com/technology/jim-balsillie-data-is-not-the-new-oil-its-the-new-plutonium>.

the EU at a time when Canada's adequacy under the GDPR may soon be scrutinzed. Moreover, if Ontario does not build this bridge soon, there is a real risk that it will be left behind as Québec and other jurisdictions move towards a future that puts privacy first. CCLA therefore urges the government to pursue privacy laws that could support a finding that Canadian privacy law is up to—or exceeds—EU standards.[3]

The root of any successful legal regime is its adaptiveness. Principle-based, technologically neutral privacy law has served Ontarians well in the past and CCLA believes this approach remains fundamental the law's remaining relevant today, in the face of rapidly evolving technologies and innovative data uses. The CCLA offers the following submissions, which directly respond to, and in some cases build upon or extend beyond, the discussion topics raised in the consultation's Discussion Paper. At this early stage of consideration, we appreciate that the Ministry of Government and Consumer Services has cast the net wide and is thinking big and conceptually when it comes to the scope of a made-in-Ontario privacy law, and we have done the same.

Privacy as a Human Right

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 equality rights and the right to free expression. Canada is a signatory to the *Universal Declaration on Human Rights*[4] and Article 17 of the *International Covenant on Civil and Political Rights*,[5] both of which recognize privacy as a human right, and the latter of which specifically protects against privacy incursions by private actors and corporations.[6] Yet Canadian privacy legislation to date frames privacy in terms of data protection principles, not the prerequisite for freedom, dignity, and autonomy that it is. In an age of where personal information about us to be used by corporate entities in ways hard to see, understand, or predict, Ontarians deserve protections that define privacy as a right they deserve, not a commodity to be bartered or balanced against corporate interests. 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

[3] See 2002/2/EC: Commission Decision (20 December 2001) pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the *Canadian Personal Information Protection and Electronic Documents Act*.

[4] "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." Available online: <https://www.un.org/en/universal-declaration-human-rights/>.

[5] "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." See UN General Assembly, International Covenant on Civil and Political Rights (16 December 1966), United Nations, Treaty Series, vol. 999, p 171, available online: <https://www.refworld.org/docid/3ae6b3aa0.html>.

[6] 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).

also an emerging deficit in the public's trust that corporations will use information fairly or transparently. We suggest that this deficit could be mitigated by legislation in Ontario that explicitly protects privacy as a right and creates legal obligations to protect that right.

CCLA therefore encourages Ontario to take an ambitious starting point in its framework for privacy: Ontario should recognise a human right to privacy. While the details of how this right could work would need to be assessed by the legislature in consultation with stakeholders and civil society organisations, this starting point would meaningfully contribute to how public conversations about privacy unfold in Ontario. Privacy is both a tool for protecting people's fundamental interests and a value in and of itself. Privacy is not optional—it is fundamental—and the law should reflect that fact.

Framing privacy as a human right can also inform the structure of privacy protections themselves. Human rights are principled instruments, given dimension and effect by legislatures and courts. Privacy should work the same way. Privacy is a principled matter, and whether they are using telegrams or smartphones Ontarians' principled interest in protecting their personal privacy remains the same. The practical upshot of this framework is that it would be more resilient to changes in technology, since our privacy interests are not in technologies themselves but in what those technologies mean for the people who use or are subject to those technologies.

Increased Consent and Clear Transparency

To position a conversation about consent and its role in a new privacy law for Ontario, it is instructive to consider the furor unleashed when Apple announced that iOS14 would require opt-in consent for allowing third parties to access advertising identifiers.[7] The pushback from advertisers was unabashedly direct: they expressed concern that there would be a "high risk of user refusal" if people are given that choice.[8] The sense of entitlement to a non-consensual use of personal information that lay behind that objection speaks volumes about the need for a contemporary privacy law to address consent, with the rights of individuals at the fore.

Although "consent" for collecting and using individuals' data is ostensibly a clear standard, in practice we know that this is not the case. Consent should be free, clear, informed, and—increasingly important in an online big data world—meaningful. The CCLA therefore agrees with the Discussion Paper's suggestion that Ontario needs transparency requirements to facilitate both traditional and alternative models for consent, so long as they support genuine informational self-determination for Ontarians. Ontarians need a legal regime that increases transparency for people

[7] Apple, "User Privacy and Data Use," available online: <https://developer.apple.com/app-store/user-privacy-and-data-use/>.
[8] Stephen Nellis and Paresh Dave, "Google-backed ad associations criticize Apple's new user warnings on data tracking." *Globe and Mail* (9 July 2020), available online: <https://www.theglobeandmail.com/business/technology/article-google-backed-ad-associations-criticize-apples-new-user-warnings-on/>.

dealing with private organisations. Although PIPEDA provides some transparency, Ontario should raise the bar in two ways. First, a strong and effective privacy law can empower Ontarians by giving them tools to help them be responsible users and consumers of private services, but the onus cannot remain on individuals. The law must also ensure that those with a commercial interest in Ontarians personal information have fair, clear, and enforceable rules about how and when consent is required. As a general principle, purpose specification, although at risk in a big data world, matters a lot to facilitate strong privacy protection. This requires consent to be granular. Personal information should be used by and within an organisation for the purposes for which it was initially collected; secondary uses should be clear and consent for such uses should be explicit, and opt-in. Organisations must publish clear and accessible privacy statements, designed to give users a clear sense of what they are consenting to, how their personal information might be used, and directions for how to seek redress for any breaches of their privacy rights.

The Discussion Paper mentions 'exceptions' to consent, such as for 'de-identified' information. The CCLA recommends that the government very closely scrutinise this category and take a principled approach to its application. "De-identifying" data is a difficult and context-sensitive activity. As a consequence, supposedly "de-identified" data is rarely actually de-identified. Research shows that de-identification is a highly case-specific exercise which should be understood in terms of the nature of the data at issue, reasonable expectations of privacy, the availability of linkable data, and perverse incentives for agents to reidentify data. Any statutory framework designed to incorporate or encourage de-identification should therefore be principled, to keep up with changes in technological capacity, and should be promulgated alongside educational resources to assist individuals and companies with understanding just how difficult it is to de-identify personal information. As part of this principle framework, there should be clear definitions for the terms "de-identified information", "anonymized information", "pseudonymized information," and "aggregate information".

When addressing issues of consent, it is also important to highlight the issue of "publicly available information," a term that is critically underdefined. Such information is often claimed by those who wish to use it for their own purposes to be an exception to the general provisions for consent. As the CCLA first explained in its Submission to the Standing Committee on Public Safety and National Security regarding Bill C-59, leaving a back door open to gather and use 'publicly available' information creates uncertainty and risks corroding individuals' privacy.

One needs only to consider the story of Clearview AI in Canada to lay bare the problem; that company is built around a database of information they claim was publicly available and scraped from a wide range of online platforms. However, their acquisition of the information was in many cases explicitly against the terms of service that should have protected users from having their information subjected to non-consensual use by a third party. Ultimately, there is a larger social question about what information is public in an age where we live online and sometimes have little control about what information others either provide, create, or collect about us without our own involvement, never mind the status of information we ourselves provide in specific contexts for specific purposes. The basic principle, as the federal Privacy Commissioner has identified, is that publicly available information still requires protection from misuse. A modern privacy law must

grapple with what it means for information to be public, to what extent such information may be legitimately used for secondary purposes, and when it should be protected from such uses.

Exceptions to the standard consent-based framework should be both principled and in the public interest. For example, there could be a reasonable exception for the use of personal information that is clearly and primarily for the benefit of the person concerned. As a general rule, however, consent should be required for the use of individuals' most sensitive personal information, regardless of circumstance. A high level of privacy should thus be the default standard whenever the private sector handles of sensitive personal information.

Data Rights: Erasure and Portability

Data Erasure

The CCLA supports a framework for individuals to de-index themselves or their information where that information is no longer required to deliver a service. The root of CCLA's support stems from how such a framework might express the more fundamental right to control one's own personal information, even as it is sometimes held by others. As the Discussion Paper mentions, this right requires deft application: the right to control another entity's use of your personal information risks trespassing on that entity's freedom of expression, as well as related freedoms including the freedom of association. The right to erasure should be subject to principled exceptions and will require in-depth consideration of the best way to ensure that journalistic and other forms of expression in the public interest are strongly protected and balanced with a new right to de-indexing or erasure.

Data Portability

The CCLA supports data portability in principle. We recommend, however, that any legislation regulating data portability also regulate portable data's accessibility and intelligibility. Where an individual has requested their data from a service provider, that data should in principle also be accessible to the individual – not just to providers who might use proprietary services or technology to access packages of an individual's stored data. No individual who requests their data from a service provider should be in doubt about what that data includes or be without the means to reasonably access that data on their own terms.

Oversight, Enforcement, and Fines

For any new privacy legislation to be effective it must be both enforceable and provide the impression that it *will* be enforced. The CCLA therefore recommends empowering Ontario's Information and Privacy Commissioner to effectively enforce any new privacy legislation and to develop educational materials to inform the general public about their rights under the new law. The law should grant the Commissioner the power to make binding orders but should also provide recourse for independent review of any such orders. Enforcement powers should also include the ability to levy fines akin to those issued under the EU's GDPR. However, given that the law's scope will include multinational technology firms and small volunteer-run non-profits, enforcement provisions will need to be proportionate, tailored, and knowable.

An important element of enforcement must be to enable the Commissioner to initiate investigations into suspected privacy violations, in addition to responding to individual or group complaints. It is increasingly likely that many privacy invasions happen behind the scenes in complex information processing environments that are largely invisible and unknown to the average person. The Commissioner therefore must have the mandate to address such systemic issues in an independent and meaningful manner—and be resourced to do so effectively.

The new law should similarly include provisions that regulate breach management and breach reporting. As soon as an organization has reason to believe that a privacy breach involving personal information has reached a threshold of significant harm, the organisation should be required to take reasonable measures to reduce any risk of prejudice and to prevent similar incidents from occurring. Moreover, privacy incidents should be logged by organisations, so that the organisation has a clear record of how and when individuals' privacy may have been compromised. If paired with an onus to notify the Commissioner about serious privacy breaches, as well as mandatory notification requirements, this scheme would protect privacy across the province while also making the Commissioner's office a partner in remedying the most serious privacy beaches.

We will include legislative oversight in this section and conclude by noting that to keep Ontario's new law up to date, CCLA would encourage Ontario to adopt a rule to keep any new law current, as is the case in British Columbia, where legislative committees review the law on a regular schedule.

Application to Non-commercial Organizations

CCLA supports extending the reach of provincial privacy protections to include non-profits, professional associations, trade unions, and political parties. However, there are significant differences between ways in which these types of body operate, including in some cases being subject to different regulatory regimes which may or may not address some aspects of their information collection, use, or disclosure obligations. These types of organisations also vary widely in size, budget, and sophistication. In particular, given that many non-profit organisations

have unstable budgets and are vulnerable to contraction in poor economic climates—such as the recession caused by the COVID-19 pandemic—we recommend that the law be designed to accommodate these bodies' more modest means and inconsistent budgets. Ontario's new privacy regime should both guard privacy and be sensitive to the fragility of many of these organisations. This sensitivity, however, should not prevent the law from applying in meaningful ways to the NGOs, charity, or other not-for-profit entities.

In particular, it is long past time for there to be a privacy framework for political parties. In a Nanos poll commissioned for the *Globe and Mail* in 2018, 73% of Canadians said they were concerned or somewhat concerned about how political parties use the personal information they collect about voters.[9] There is no reason to believe such concern has diminished in the interim and arguably, given the plethora of revelations since that time about privacy breaches and a growing public understanding of the sophisticated ways in which data can be used, it may well have increased. The status quo is thus inadequate and ripe for a new regulatory framework.

While there are no principled reasons why privacy law should not apply to political parties in the same way it does to virtually every other public and private sector data collector, fair implementation would be essential. Any proposed legislation must be carefully considered, principled and fair: no political gamesmanship can be allowed in the name of privacy protections. CCLA therefore recommends a robust privacy framework for political parties that both empowers them to meaningfully represent their constituencies while also protecting the privacy of their supporters and the public at large.

The nuance and complication involved in extending the proposed law to this wide range of non-commercial organisations is going to require a sincere commitment to consult with the relevant sectors and stakeholders, a process well-begun at this stage and which we encourage Ontario to continue with moving forward.

De-identified Personal Information, Data Derived from Personal Information

There is debate about whether or not de-identified information is or should be covered by privacy law, 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.

There is thus no principled reason why supposedly de-identified data should be excluded from the scope of privacy regulation. 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

[9] Bill Curry, "Canadians concerned about how Facebook, political parties protect their privacy: poll," *Globe and Mail* (19 December 2018), available online: https://www.theglobeandmail.com/politics/article-canadians-concerned-about-how-facebook-political-parties-protect/.

was a "serious possibility" that the data could be re-identified.[10] CCLA prefers a higher standard than "serious possibility", given the risks outlined above regarding re-identification. Further, such information is still about individuals, and it is unclear why simply removing some identifiers should eliminate a person's right to decide, via a consent process, whether their information in de-identified form can be used for any particular purpose. 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 privacy law to regulate. A made-in-Ontario privacy law should cover de-identified data and address the differences between anonymized information, pseudonymized information and aggregate information. Provisions regarding requirements to inform data subjects about the ways in which their information will be de-identified, the risk of re-identification, and provide redress for incidents where re-identification causes harm to individuals will be important components of a new law.

Enabling Data-sharing for Innovation, while Protecting Privacy

CCLA sees innovations in data sharing and data collection as both full of opportunities and hidden dangers. We therefore recommend that any prospective Ontario privacy overhaul give specific consideration to the following issues.

Desire for data sharing is often grounded in the reality that artificial intelligence applications require huge quantities of data for training purposes. At the same time, algorithmic processing is a paradigmatic example of how innovations in data processing technology can benefit or harm people on the basis of their personal information. Algorithmic processing and artificial intelligence applications, sometimes in conjunction with machine learning are rapidly becoming ubiquitous tools for analysing and sorting data, detecting patterns, and engaging in social sorting. Predictive systems are becoming commonplace. Depending on their construction, such systems, whether aimed at assessing, influencing, or predicting behaviour, can lead to discriminatory outcomes under the guise of an impersonal and neutral assessment. Moreover, these outcomes may be difficult to spot or challenge when the algorithms themselves are either hidden or inscrutable. Many important decisions—affecting issues like employment, housing, and pay equity—are made in some part on the basis of algorithmic assessments. Where these algorithms are not in public view, those harmed by their use can have little recourse.

Concomitant with any regime that facilitates data sharing, Ontarians need transparency with respect to automated or machine-assisted decisions made about them. 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

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

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.

There are a range of data sharing frameworks that have emerged to attempt to address privacy concerns while facilitating sharing, particularly when it is in the public interest. The particular way in which "public interest" is defined is highly consequential in considering the desirability of any such framework. The concept of a data trust, in particular, is explicitly highlighted in the Discussion Paper. CCLA would like to highlight research we participated in, funded by the Privacy Commissioner of Canada's Contributions Grant Program. The resulting report addresses some of the privacy and other considerations inherent to using such a model and may be of assistance to an analysis of data stewardship models for the purposes of this consultation. It is linked below.[11]

Additional Challenges and Opportunities

Particularly Intrusive Technologies

There is a difficult tension between maintaining a technologically neutral privacy law and recognising the unique challenges presented by particular new technologies. This could be dealt with in the proposed privacy law, or may be more appropriately addressed in separate legislation. However, at this initial and exploratory stage in Ontario's journey towards a privacy law, it is necessary to consider the challenges raised by biometric and facial recognition technologies because of the unique challenge they pose to personal privacy in general and consent and transparency principles in particular. 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 government's attention.

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

[11] David Fewer, Stephanie Perrin, Brenda McPhail and Andrew Clement. *The Price of Trust? An analysis of emerging digital stewardship models*. Available online: <https://cippic.ca/index.php?q=en/data-governance>.

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 on private property such as 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 and CCLA would agree. CCLA's position on facial recognition includes the need for democratic debate regarding whether it has a place in a free democracy; one important element of such a debate would be whether or not there is a democratically-debated law providing safeguards for rights in relation to uses of the technology.

Other North American jurisdictions are already leading on this issue. In Illinois, the Biometric Information Privacy Act (BIPA)[12] 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 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.[13] California is also breaking ground in protecting biometric data privacy with *The California Online Privacy Protection Act of 2003* (CalOPPA).[14] 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.

Privacy Protections for Employees

As we mentioned in the introduction to these submissions, employee privacy is a major gap in Ontario's current privacy framework. This gap must be closed and CCLA expects the government will turn its mind to it in due course. We would like to highlight at this juncture, however, the novel privacy issues facing employees as a consequence of the COVID-19 pandemic. The first issue is employers' invasive and potentially coercive inquiries into employees' health and private life. This can occur when employers pursue policies such as temperature screening, contact tracing, and location monitoring. Not only do these tactics inherently engage employees' privacy interests, but they also risk incidentally invading employees' privacy by divulging more information than the policies themselves were meant to collect, such as lifestyle habits and pre-existing medical conditions.

The second employee privacy concern we would highlight in the context of the pandemic has to do with monitoring employees' behaviour in the workplace. Due to COVID, many Ontarians' workplaces have fused with their home living arrangements. This makes it difficult to separate

[12] 740 ILCS 14.
[13] See *H.K. v. Google*, LLC, 5:20-cv-02257.
[14] The Online Privacy Protection Act of 2003, Cal. Bus. & Prof. Code §§ 22575-22579 (2004).

workplace surveillance from home surveillance. There is thus a significant risk that productivity monitoring tools, such as software, may incidentally collect information about workers' personal lives, family members, and homes, especially given that many remote workers use their personal computers for work.[15] These concerns are illustrative of the range of issues a new law will need to consider, but there are of course also a large number of longstanding concerns around employee privacy protections that are equally pressing to address in a new law.

Privacy Protections for Children and Youths

Innovations in data sharing have also highlighted one of the perennial challenges in privacy policy more generally: how to both respect children's privacy online while also recognising parents' prerogative with respect to their children's privacy. 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 Ontario's privacy law protect minors who may not know or comprehend the potential risks they create when sharing information online. It is similarly imperative, however, that privacy law does not simply become a means for the government to wantonly stifle children's free expression and association. The government should therefore take a careful and considered approach to protecting young people's personal information against exploitation.

Many Canadian businesses already echo 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.[16] 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.[17] Commentators suggest that privacy laws can be amended to declare that the collection of children's personal information for the purposes of targeting their behaviour is itself unreasonable and prohibited.[18] The third problem with this approach is simply how heavily it relies

[15] Kris Klein & Dustin Moores, "Privacy Issues Arising from the COVID-19 Pandemic", 3 Emerging Areas of Practice Series-COVID-19 (Coronavirus), (2020).
[16] 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>.
[17] 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/>.
[18] 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.

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 Ontario's regime for youth privacy, however, then the law may 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 government may consider. The first is a stepped model, 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.[19] 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.

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 government should therefore consider itself to have both the prerogative and means to safeguard youths' privacy in digital spaces.

Cross-border Data Flows

The last issue CCLA would highlight is the regulatory challenge posed by third-party outsourcing and cross-border data flows. We do not at this time recommend a specific framework but urge Ontario to treat these information flows as a priority for privacy and as an important diplomatic objective, given the EU's commitment to trading with partners who protect privacy to a similar degree as does the GDPR.

CCLA wishes to thank the Ministry of Government and Consumer Services for framing this consultation ambitiously and comprehensively, and Ontario's Chief Privacy Officer and Archivist of Ontario, John Roberts, for his leadership in the consultation process thus far. We are grateful for this opportunity to provide submissions and very much look forward to further opportunities to participate as this process moves forward.

[19] See: Steeves *ibid*.