Office of the Privacy Commissioner of Canada
Commissariat à la protection de la vie privée du Canada

Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the *Digital Charter Implementation Act*, 2020

Table of Contents

May 2021

VIA EMAIL

May 11, 2021

Mr. Chris Warkentin, M.P. (Member of Parliament)

Chair, Standing Committee on Access to Information, Privacy and Ethics
Sixth Floor, 131 Queen Street
House of Commons
Ottawa ON K1A 0A6

Dear Mr. Chair:

Subject: Submission on C-11

Further to my appearance before you on May 10, 2021, please find enclosed our submission on Bill C-11, the *Digital Charter Implementation Act, 2020*. I hope these materials will assist your deliberations on this important piece of privacy legislation.

As I indicated when I appeared before you in the context of the Main Estimates and your study of Facial Recognition Technology, I believe that C-11 represents a step back overall from our current law and needs significant changes if confidence in the digital economy is to be restored. My submission outlines numerous enhancements that are required to help ensure that organizations can responsibly innovate in a manner that recognizes and protects the privacy rights of Canadians.

My opening message provides an overview of our position, while the rest of the document contains a detailed analysis of the bill and recommendations that we believe are necessary.

I am also including an analysis paper prepared for my Office by Dr. Teresa Scassa on the problems with how Bill C-11 would address the issue of trans-border transfers of personal information. It identifies key provisions of C-11 that relate to trans-border data transfers, critically analyzes the extent to which these provisions would substantively protect privacy and offers a series of recommendations for improvement.

I hope these materials will be useful for the Committee. I remain available to meet with Parliament on this important Bill at its convenience.

Sincerely,

(Original signed by)

Daniel Therrien
Commissioner

encl. (enclosure) (1)

c.c.: The Honourable François-Philippe Champagne, P.C., M.P. (Member of Parliament)
Minister of Innovation, Science and Industry

Ms. Miriam Burke
Clerk of the Committee

Commissioner’s message

Bill C-11, which enacts the *Consumer Privacy Protection Act* (CPPA) and the *Personal Information and Data Protection Tribunal Act* (PIDPTA), is an important and concrete step toward privacy law reform in Canada. Arising from the 2019 Digital Charter (https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html), and following years of Parliamentary studies, Bill C-11 represents a serious effort to realize the reform that virtually all – from Parliamentarians, to industry, privacy advocates, and everyday Canadians – have recognized is badly needed. It was

an ambitious endeavour to completely restructure the existing Act. We are pleased to see that the law reform process appears to be truly underway.

The Bill completely rewrites that law and seeks to address several of the privacy concerns that arise in a modern digital economy. It promises more control for individuals, much heavier penalties for organizations that violate privacy, while offering companies a legal environment in which they can innovate and prosper.

We agree that a modern law should both achieve better privacy protection and encourage responsible economic activity, which, in a digital age, relies on the collection and analysis of personal information. However, despite its ambitious goals, our view is that in its current state, the Bill would represent a step back overall for privacy protection. This outcome can be reversed, and the Bill could become a strong piece of legislation that effectively protects the privacy rights of Canadians, with a number of important amendments under three themes:

- a better articulation of the weight of privacy rights and commercial interests;
- specific rights and obligations;
- access to quick and effective remedies and the role of the OPC (Office of the Privacy Commissioner of Canada).

Why do I say that the Bill as drafted would represent a step back? In general terms, because the Bill, although seeking to address most of the privacy issues relevant in a modern digital economy, does so in ways that are frequently misaligned and less protective than laws of other jurisdictions. Our recommendations would lead to greater alignment.

More specifically, I say the Bill as drafted would be a step back overall because the provisions meant to give individuals more control give them less; because the increased flexibility given to organizations to use personal information without consent do not come with the additional accountability one would expect; because administrative penalties will not apply to the most frequent and important violations, those relevant to consent and exceptions to consent; and because my Office would not have the tools required to manage its workload to prioritize activities that are most effective in protecting Canadians. In fact, the OPC (Office of the Privacy Commissioner of Canada) would work under a system of checks and balances (including a new administrative appeal) that would unnecessarily stand in the way of quick and effective remedies for consumers.

Poll after poll suggest there is currently a trust deficit in the digital economy. Improving trust is one of the objectives of the Digital Charter that Bill C-11 seeks to implement. After years of self-regulation, or permissive regulation, polls also suggest this requires more regulation (objective and knowable standards adopted democratically) and oversight (application of these standards by democratically appointed institutions). The regulation required is sensible legislation that allows responsible innovation that serves the public interest and is likely to foster trust, but that prohibits using technology in ways that are incompatible with our rights and values.

Oddly, the government's narrative in presenting the Bill, while positive in many respects, focused on the need for "certainty" and "flexibility" for businesses and the need for "checks and balances" on the regulator. Unfortunately, it appears this was not a slip of the tongue, as we see that philosophy reflected in several provisions of the Bill.

The OPC (Office of the Privacy Commissioner of Canada) welcomes transparency and accountability for its actions, and we agree businesses need some level of certainty and flexibility, *within the law*. But the focus on checks and balances for the regulator and more certainty and greater flexibility for businesses seems misplaced. It leads to the flaws identified earlier and to an imbalance in the law on the importance of rights and commercial interests.

Better articulation of the weight of rights and commercial interests

Digital technologies are at the heart of the fourth industrial revolution and modern economies. As we have seen in the current pandemic, they can serve the public interest. This includes economic prosperity.

For both good and bad, these technologies are disruptive. They have been shown to pose major risks for privacy and other rights. Data breaches have become routine. There is increasing talk of surveillance capitalism – this, a few years after the Snowden revelations of state surveillance. Biometrics heightens those risks. More recently, the Cambridge Analytica scandal highlighted the risks for democracy. Artificial intelligence brings risks to equality rights. And on and on.

Ultimately, it is up to parliamentarians, as elected representatives of the population, to decide how much weight to give to privacy rights and the interests of commercial enterprises.

My Office has argued for a modernization of laws that would give organizations greater flexibility to use personal information without consent for responsible innovation and socially beneficial purposes, but *within* a legal framework that would entrench privacy as a human right and as an essential element for the exercise of other fundamental rights.

The Bill maintains that privacy and commercial interests are competing interests that must be balanced. In fact, the Bill arguably gives more weight to commercial interests than the current law by adding new commercial factors to be considered in the balance, without adding any reference to the lessons of the past twenty years on technology's disruption of rights.

The courts have held that PIPEDA (Personal Information Protection and Electronic Documents Act)'s purpose clause, without the new commercial factors added in Bill C-11, means privacy rights must be "reconciled" with commercial interests. This is a reasonable interpretation of the direction given to courts and the regulator by Parliament when it enacted PIPEDA (Personal Information Protection and Electronic Documents Act) in 2000.

Parliamentarians now have a chance to confirm or amend this direction. There is no dispute that the CPPA (Consumer Privacy Protection Act) should both promote rights and commercial interests. The question is what weight to give to each.

In my view, it would be normal and fair for commercial activities to be permitted within a rights framework, rather than placing rights and commercial interests on the same footing. Generally, it is possible to concurrently achieve both commercial objectives and privacy protection. However, when there is a conflict, I believe rights should prevail. The recent Clearview matter is a good example of that principle.

To adopt a rights-based approach would also send a powerful message as to who we are and what we aspire to be as a country. The *Canadian Charter of Rights and Freedoms* is an integral part of our character and Canada is a signatory to international instruments that recognize privacy as a human right. We are a bijural country, in which the common law and civil law systems coexist in harmony. In Quebec, existing privacy laws seek to implement the right to privacy protected in the *Civil Code* and the *Quebec Charter of Human Rights and Freedoms*. Bill 64 would further protect privacy as a human right. Adopting a rights-based approach in the CPPA (Consumer Privacy Protection Act), including some elements of Bill 64's provisions, would reflect Canada's bijural nature.

Canada also aspires to be a global leader in privacy and it has a rich tradition of mediating differences on the world stage. Adopting a rights-based approach, while maintaining the principles-based and not overly prescriptive approach of our private sector privacy law, would situate Canada as a leader showing the way in defining privacy laws that reflect various approaches and are interoperable.

Our detailed submissions comment further on this and include a new preamble and amendments to sections 5, 12 and 13 of the proposed CPPA (Consumer Privacy Protection Act).

Specific rights and obligations

Again, I refer you to our detailed submissions for a fuller analysis of this theme. Let me now focus on consent, exceptions thereto and accountability.

(i) Valid vs meaningful consent

The Bill seeks to give consumers more control over their personal information. It does this by prescribing elements that must appear in a privacy notice, in plain language. This is similar to the approach taken in our 2018 *Guidelines for obtaining meaningful consent*, with an important omission. Bill C-11 also makes the same omission of a crucial aspect of meaningful consent under the current law (s. (section) 6.1 of PIPEDA (Personal Information Protection and Electronic Documents Act)): "the consent of an individual is only valid if it is reasonable to expect that an individual to whom the organization's activities are directed would *understand* the nature, purpose and consequences of the collection, use or disclosure of the personal information to which they are consenting." (my emphasis)

By prescribing elements of information to appear in privacy notices without maintaining the requirement that consumers must be likely to understand what they are asked to consent to, the CPPA (Consumer Privacy Protection Act) would give individuals less control, not more.

This is exacerbated by the open-ended nature of the purposes for which organizations may seek consent. PIPEDA (Personal Information Protection and Electronic Documents Act) currently requires that purposes be "explicitly specified" and be legitimate. This is consistent with the laws of most other jurisdictions, which prescribe that purposes must be defined "explicitly", or even "as explicitly as possible". This limitation, which is important for consumers to understand what they are consenting to, is also omitted from Bill C-11. With the result that, conceivably, organizations could seek consent for vague and mysterious purposes, such as "improving your consumer experience".

Finally on this point, while s. (section) 15(4) of the CPPA (Consumer Privacy Protection Act) would make express consent the rule, this provision would allow an organization to rely on implied consent where it "establishes" (in French, "conclure" or concludes) that this would be appropriate, in light of certain factors. Bill C-11 therefore seems to give deference to an organization's conclusion that implied consent is appropriate, as opposed to prescribing an objective assessment of the relevant factors. This is another manifestation of the philosophy where businesses would be given certainty and flexibility, rather than be subject to objective standards and oversight. A simple amendment, striking the words "the organization establishes that" in s. (section) 15(4), would solve the problem and would fully implement the recommendation made by the ETHI (Standing Committee on Access to Information, Privacy and Ethics) Committee in 2018. [1](#fn1)

(ii) Exceptions to consent and accountability

The CPPA (Consumer Privacy Protection Act) would add important new exceptions to consent. We think this is appropriate in a modern privacy law.

Among the lessons of the past twenty years is that privacy protection cannot hinge on consent alone. Simply put, it is neither realistic nor reasonable to ask individuals to consent to all possible uses of their data in today's complex information economy. The power dynamic is too uneven.

In fact, consent can be used to legitimize uses that, objectively, are completely unreasonable and contrary to our rights and values. In these circumstances, consent rules do not protect privacy but contribute to its violation. This also leads to the trust deficit affecting the digital economy.

Several of the new exceptions to consent brought by Bill C-11 are reasonable. We have two main concerns: some exceptions are unreasonably broad; and the Bill fails to associate greater authority to use personal information with greater accountability by organizations for how they rely on these broader permissions.

Paragraphs 18(2)(b) and (e) of the CPPA (Consumer Privacy Protection Act) are too broad. The first can likely be narrowed but the second should be repealed. We can find no reasonable justification for an exception to consent based on the impracticability of obtaining consent. This would make the rule (consent) completely hollow. There may be *some* specific activities (for instance those of search engines) that should be permitted for the usefulness of their service even though consent may be impracticable. Or, as recommended in our recent paper on artificial intelligence, the CPPA (Consumer Privacy Protection Act) could include a consent exception for "legitimate business purposes",

but only within a rights-based privacy law.

With Bill C-11, organizations would have much wider permission to collect, use and disclose the personal information of consumers, without consent. Or, put differently, the Bill recognizes that consent is often a fiction and tries to find ways to allow but regulate modern business operations that "(rely) on the analysis, circulation and exchange of personal information" (s. (section) 5), where consent is neither reasonable nor realistic.

Creating newer and broader exceptions to consent means that the law would place less weight on individual control as a means to protect privacy. This form of protection should be replaced by others. Greater permission to use data should come with greater accountability for organizations. There is a consensus on this point in the privacy community, even among industry representatives.

Yet the CPPA (Consumer Privacy Protection Act) would not enhance PIPEDA (Personal Information Protection and Electronic Documents Act)'s principle of accountability. It would arguably weaken it. In part by defining accountability in descriptive rather than normative terms. Accountability would not be, as in other laws and the OPC (Office of the Privacy Commissioner of Canada) guidelines, translated in policies and procedures that ensure (normative goal) compliance with the law, but rather as those policies and procedures that an organization decides to put in place (descriptive) to fulfil its obligations. Again, certainty and flexibility for businesses, rather than standards and oversight.

We have argued for some time that in the current digital economy, based on complex technologies and business models which are difficult if not impossible to understand for consumers, the OPC (Office of the Privacy Commissioner of Canada) as expert regulator should have the authority to proactively inspect, audit or investigate business practices to verify compliance with the law, without prior evidence or grounds that the law has been violated. This ability to "look under the hood" of these complex technologies and business models, not arbitrarily but based on our expert assessment of privacy risks, and subject to judicial review, is in our view a necessary element of a modern privacy law.

These provisions exist in the privacy laws of Quebec and Alberta and in those of several foreign jurisdictions, including common law countries such as the United Kingdom, Australia and Ireland, and is proposed by the Department of Justice in its latest consultation paper on *Privacy Act* reform. They would ensure that organizations are held accountable for the way in which they use the increased flexibility to collect, use and disclose the personal information of consumers. For instance, they would ensure that automated decision-making systems and artificial intelligence are developed and applied in a privacy compliant manner. They would also help address the concerns of Canadians that underlie the deficit of trust in the digital economy.

Finally, the CPPA (Consumer Privacy Protection Act)'s provisions on accountability should explicitly include a requirement that organizations apply Privacy by Design, as recommended in ETHI (Standing Committee on Access to Information, Privacy and Ethics)'s 2018 report, and that privacy impact assessments (PIAs) be prepared for higher risk activities. Requiring PIAs (Privacy Impact Assessments) for all activities involving personal information would create an excessive burden on organizations, particularly SMEs (small and medium enterprises). But Privacy by Design and PIAs (Privacy Impact Assessments) are important for their proactivity in protecting privacy. Compliance with the law cannot rest only on investigations and penalties. Proactive strategies are equally, and in our view more important in achieving ongoing compliance and respect for the rights of consumers.

Access to quick and effective remedies and the role of the OPC (Office of the Privacy Commissioner of Canada)

The CPPA (Consumer Privacy Protection Act) would give the OPC (Office of the Privacy Commissioner of Canada) order-making powers and allow the OPC (Office of the Privacy Commissioner of Canada) to recommend the imposition of very large penalties on organizations that violate the law, but these provisions are subject to limitations and conditions such that consumers would not have access to quick and effective remedies. To achieve this objective

would require important amendments to the Bill.

(i) Limits on violations subject to administrative penalties

The most striking limitation on penalties is found in s. (section) 93(1) of the CPPA (Consumer Privacy Protection Act), which lists only very few violations as subject to administrative penalties. This list does not include obligations related to the form or validity of consent, nor the numerous exceptions to consent, which are at the core of protecting personal information. It also does not include violations to the principle of accountability, which is supposed to be an important counterbalance to the increased flexibility given to organizations in the processing of data.

Only criminal penalties would be available for violations of these rights and obligations, following a process that in our view would take seven (7) years on average. This process would include an order made by the OPC (Office of the Privacy Commissioner of Canada) and a refusal to comply by the organization. With the amendments we recommend, the process could take fewer than two (2) years. Notably, we recommend that most if not all violations of the CPPA (Consumer Privacy Protection Act) could be subject to administrative penalties, following a notice by the OPC (Office of the Privacy Commissioner of Canada) giving the organization a last opportunity to comply with the law. Criminal sanctions would be reserved for the most egregious violations.

(ii) The Personal Information and Data Protection Tribunal

Among the checks and balances imposed on the OPC (Office of the Privacy Commissioner of Canada) would be the creation of an additional layer of appeal in the form of the Tribunal. According to the government, this would ensure both fairness to organizations and access to quick and effective remedies for consumers.

To reiterate, the OPC (Office of the Privacy Commissioner of Canada) welcomes accountability for its actions. We respectfully suggest that the new Tribunal is both unnecessary to achieve greater accountability and fairness (a role already fulfilled by the Federal Court), and counter-productive in achieving quick and effective remedies. We recommend that this new layer not be added to a process that can already be quite long. However, should Parliament decide that the new Tribunal would add value, we recommend that its composition be strengthened and that appeals from its decisions go directly to the Federal Court of Appeal.

While our submissions elaborate on our analysis of this issue, I wish to emphasize a few points here. First, the addition of such an administrative layer between the privacy regulator and the courts does not exist in other jurisdictions. Second, the experience of these jurisdictions, including some Canadian provinces, shows that effective structures can be created within data protection authorities to enhance fairness through the separation of enforcement and adjudicative functions. Third, the OPC (Office of the Privacy Commissioner of Canada) is already subject to judicial review, and only once in its almost 40-year history was a decision it had made found not compliant with natural justice.

Fourth and probably most important, the fact that the OPC (Office of the Privacy Commissioner of Canada) would not be authorized to impose administrative penalties, and that its orders would be subject to appeal to another administrative structure before reaching the courts, would reduce the incentive organizations have under the model in place in other jurisdictions, to come to a quick agreement with the regulator. In these jurisdictions, where the data protection authority is the final administrative adjudicator and where it can impose financial penalties, organizations have an interest in coming to a negotiated settlement when, during an investigation, it appears likely a violation will be found and a penalty may be imposed. Unfortunately, the creation of the Tribunal would likely incentivize organizations to “play things out” through the judicial process rather than seek a negotiated settlement with the OPC (Office of the Privacy Commissioner of Canada), thus depriving consumers of quick and effective remedies. Sadly, but truly, justice delayed is justice denied.

(iii) Giving the regulator tools to be effective in protecting consumers

Bill C-11 would impose several new responsibilities on the OPC (Office of the Privacy Commissioner of Canada), including the obligation to review codes of practice and certification programs, and advice to individual organizations

on their privacy management programs. We welcome the opportunity to work with businesses in these ways in ensuring their activities comply with the law. However, adding new responsibilities to an already overflowing plate means the OPC (Office of the Privacy Commissioner of Canada) would not be able to prioritize its activities, based on its expert knowledge of evolving privacy risks, to focus on what is likely most harmful to consumers.

The issue here is not primarily money, although in our view additional resources will be required. The issue is whether the OPC (Office of the Privacy Commissioner of Canada) should have the legal discretion to manage its caseload, respond to the requests of organizations and complaints of consumers in the most effective and efficient way possible, and reserve a portion of its time for activities it initiates, based on its assessment of risks for Canadians.

An effective regulator is one that prioritizes its activities based on risk. No regulator has enough resources to handle all the requests it receives from citizens and regulated entities. Yet Bill C-11 adds responsibilities, including the obligation to decide complaints before consumers may file a private right of action, imposes strict time limits to complete our activities, and adds no discretion to manage our caseload. This is not only untenable for us as a bureaucratic organization. It would deprive us of a central tool to ensure we can be effective in protecting Canadians.

We therefore make a number of recommendations under this theme, to ensure we can both be responsive, to the extent our resources allow, to individual requests made by complainants and organizations, and effective as a regulator for all Canadians.

Conclusion

The past few years have opened our eyes to the exciting benefits and worrying risks that new technologies pose to our values and to our rights. The issues we face are complex but the path forward is clear. As a society, we must project our values into the laws that regulate the digital space. Our citizens expect nothing less from their public institutions. It is on this condition that confidence in the digital economy, damaged by numerous scandals, will return.

OPC (Office of the Privacy Commissioner of Canada) review of C-11 – context

Prior to presenting our specific comments on the Bill, it will be of value to provide a brief overview of the lens through which we viewed the Bill.

Our overall position on privacy law reform can also be found in the Commissioner's message from our 2018-19 (/en/opc-actions-and-decisions/ar_index/201819/ar_201819/#heading-0-0-1) and 2019-20 (/en/opc-actions-and-decisions/ar_index/201920/ar_201920/#heading-0-0-1) annual reports, as well as the Commissioner's statement (/en/opc-news/speeches/2020/sp-d_20200924/) before the Quebec National Assembly on Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, and in a September 2020 Hill Times op-ed, titled The value of data, the values of privacy (/en/opc-news/news-and-announcements/2020/op-ed_200908/).

Our submission is based in part on our experience as a regulator and our frequent and deep involvement in privacy matters with other data protection authorities in Canada and across the world. Our recommendations are grounded in precedents, best practice, and research, which has been growing rapidly in recent years and thus forms an impressive pool of knowledge from which we can draw. These recommendations are closely aligned with existing legislation, frequently cited in this submission, that domestic and international jurisdictions have adopted. We also refer to work that the OPC (Office of the Privacy Commissioner of Canada) has commissioned by leading Canadian researchers such as Ignacio Cofone (on artificial intelligence (/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/)) and Teresa

Scassa (on privacy as a human right and on trans-border data flows (/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/)).

Finally, the OPC (Office of the Privacy Commissioner of Canada) agrees that granting organizations the flexibility to responsibly innovate is essential in a modern, data-driven economy – and that this will require new exceptions to consent. Laws should permit the use of personal information in the public interest, and responsible processing of personal information can serve public goods such as health, economic growth, and better public policies and programs.

Artificial intelligence (AI), for instance, holds immense promise, including helping to address some of today's most pressing issues. It can detect and analyze patterns in medical images to assist doctors in diagnosing illness, improve energy efficiency by forecasting demand on power grids, deliver highly individualized learning for students, and manage traffic flows across various modes of transport to reduce accidents and save lives. AI (artificial intelligence) also allows organizations to innovate in consumer products as well as in business operations, such as automating quality control and resource management. AI (artificial intelligence) stands to increase efficiency, productivity, and competitiveness – factors that are critical to the economic recovery and long-term prosperity of the country.

However, the benefits of drawing value from data should not come by ignoring privacy or giving it a secondary role as a suggested best practice that can be too easily set aside for other goals. On the contrary, privacy and innovation are not conflicting values and can be achieved at the same time.

This increased flexibility for organizations to innovate should be exercised within a legal framework that entrenches privacy as a human right. At a minimum, the law should provide objective standards, democratically adopted in the public interest, that assure consumers that their participation in the digital world will no longer depend on their "consent" to practices imposed unilaterally by the private sector. Moreover, the granting of greater flexibility in data processing should be accompanied by increased corporate responsibility. It is on these conditions that trust, eroded by frequent violations of the right to privacy, will return.

Our comments, in brief

Navdeep Bains, the Minister of Innovation, Science and Industry at the time the Bill was introduced has stated that there are three pillars to Bill C-11 (https://www.ourcommons.ca/DocumentViewer/en/43-2/house/sitting-35/hansard#11029328): enhancing consumer control, enabling responsible innovation, and ensuring a strong enforcement and oversight mechanism. Parliament now has a significant job in front of it – including, in our opinion, a need to fully examine whether the Bill appropriately realizes these pillars, and achieves the ultimate end of protecting the privacy of Canadians in the modern, data-centric era.

Despite Bill C-11's ambitious goals, our view is that in its current state the Bill would represent a step back overall for privacy protection. There are serious problems with this Bill. It seeks to address most of the privacy issues relevant in a modern digital economy, but in ways that are frequently misaligned and less protective than the laws of other jurisdictions. However, with some important amendments, the Bill could become a strong piece of legislation that effectively protects the privacy rights of Canadians, while encouraging responsible economic activity.

This submission thus sets out a series of recommended changes, broken into three themes:

- a better articulation of the weight of privacy rights and commercial interests
- specific rights and obligations
- access to quick and effective remedies and the role of the OPC (Office of the Privacy Commissioner of Canada)

Recommended amendments

Theme one: Weighting of privacy rights and commercial interests

Our Office has argued for a modernization of laws that would give organizations greater flexibility to use personal information without consent for responsible innovation and socially beneficial purposes, but within a legal framework that would entrench privacy as a human right and as an essential element for the exercise of other fundamental rights.

Bill C-11 maintains that privacy and commercial interests are competing interests that must be balanced. In fact, the Bill arguably gives more weight to commercial interests than the current law by adding new commercial factors to be considered in the balance, without adding any reference to the lessons of the past twenty years on technology's disruption of rights.

In our view, it would be normal and fair for commercial activities to be permitted within a rights framework, rather than placing rights and commercial interests on the same footing. Generally, it is possible to concurrently achieve both commercial objectives and privacy protection. This is how we conceive responsible innovation. However, when there is a conflict, we believe rights should prevail.

In this section, we set out a number of potential amendments that would help to achieve a more appropriate weighting of privacy rights and commercial interests.

Human rights framework

In advance of the 2018-19 Annual Report (/en/opc-actions-and-decisions/ar_index/201819/ar_201819/) to Parliament, the OPC (Office of the Privacy Commissioner of Canada) engaged Dr. Teresa Scassa in an examination of whether and how a human-rights based approach to data protection law could be implemented in Canada. [2](#fn2) As described by Dr. Scassa:

> A human rights-based approach to privacy is one that places the human rights values that underlie privacy protection at the normative centre of any privacy legislation. Approaching privacy as a human right does not eliminate the need to balance privacy with competing rights and interests (some of which also have constitutional status). Rather, it acknowledges the nature and value of privacy as a human right so as to give privacy its appropriate weight in any balancing exercise.

Dr. Scassa highlights that privacy is clearly recognized as a basic human right in international treaties to which Canada is a signatory including the Universal Declaration on Human Rights (see Article 12 (https://www.un.org/en/universal-declaration-human-rights/)) and the International Covenant on Civil and Political Rights (see Article 17 (https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx)). Not only has the Federal Court specifically referred to PIPEDA (Personal Information Protection and Electronic Documents Act) as quasi-constitutional [3](#fn3), the Supreme Court of Canada has also repeatedly recognized the quasi-constitutional nature of privacy rights "because of the fundamental role privacy plays in the preservation of a free and democratic society." [4](#fn4)

Beyond this recognition of the status of privacy, approaching privacy through a human rights lens can also allow it to evolve. Initial conceptions of privacy focused on the individual, centering consent as a means of permitting control (at least in theory) over access to and use of personal information.

However, as noted by Dr. Scassa, there is a growing recognition that breaches of individual privacy can produce collective harms. For instance, though mass surveillance impacts individuals, it may cause collective harm through larger-scale behavioural changes or through a widespread lessening of dignity and autonomy. As well, contemporary data analytics can reduce individuals to shared characteristics within groups, potentially leading to both individual and collective harms being experienced when assumptions made about the group's characteristics are applied to both the group and to those considered part of it. Here, privacy harms are closely tied to the right to equality and to be free from discrimination.

[A further examination of the need for a rights-based framework is available in the aforementioned annual report; we refer you to that document for further discussion.]

A human rights-based framework does not, however, require privacy legislation to come at the cost of innovation. In fact, it should be seen as an opportunity for Canada. In its submission to a review of the *Australian Privacy Act* (https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/), the Office of the Australian Privacy Commissioner writes:

> However, balancing privacy rights with economic, security and other important public interest objectives is not a zero-sum game. There are mutual benefits to individuals and regulated entities if the rights and responsibilities in the [Australian] *Privacy Act* are in the correct proportion. Effective privacy laws support economic growth by building trust and confidence that innovative uses of data are occurring within a framework that promotes accountability and sustainable data handling practices. Increasing individuals' confidence in the way their personal information is managed will likely lead to greater support for services and initiatives that propose to handle this information. These are essential ingredients to a vibrant digital economy and digital government.

We have made similar arguments, including in our 2018-19 annual report:

> The incorporation of a rights-based framework in our privacy laws would help support responsible innovation and foster trust in government, giving individuals the confidence to fully participate in the digital age. We are certain that both private and public sector organizations will be able to continue to innovate and thrive in an environment that both supports and encourages innovation and recognizes and protects the privacy rights of individuals. In fact, a greater focus on privacy rights, responsible practices, and transparency could assist the business community and public sector in ensuring that they remain competitive and relevant on both a domestic and international level given global developments in this regard.

In fact, Microsoft CEO (Chief Executive Officer) Satya Nadella highlighted that trust in personal data use is fundamental to ensuring economic growth, in his comments at the 2020 World Economic Forum:

> The one way we can in fact not only have lack of economic growth, we can go backwards, is if you don't have trust in the very factor of production that's supposed to fuel the fourth industrial revolution. So, whether it's cyber, whether it's privacy…AI (artificial intelligence) ethics or Internet safety, these are all big topics where we will need global norms to ensure that there is trust in technology and we, as the platform creators, will have to do our part in it. [5](#fn5)

In other words, protecting privacy as a fundamental right is entirely in line with the government's objective of fostering trust in the digital and information-based economy.

A year prior, in addressing the 41st International Conference of Data Protection and Privacy Commissioners, Microsoft President, Brad Smith, noted:

> Privacy is not just a fundamental human right. It is a foundational right. [6](#fn6)

Earlier this year, in his remarks at the Computers, Privacy and Data Protection conference, Apple CEO (Chief Executive Officer) Tim Cook said:

> If we accept as normal and unavoidable that everything in our lives can be aggregated and sold, we lose so much more than data …We lose the freedom to be human. [7](#fn7)

In his testimony given before the House of Commons ETHI (Standing Committee on Access to Information, Privacy and Ethics) Committee Study in May 2018 (https://www.ourcommons.ca/Content/Committee/421/ETHI/Evidence/EV9861805/ETHIEV106-E.PDF), Jim Balsillie, former co-CEO (Chief Executive Officer) of Research in Motion and co-founder of the Council of Canadian Innovators stated:

> Canadians need to be formally empowered in this new type of economy, because it affects our entire lives … personal information has already been used as a potent tool to manipulate individuals, social relationships, and autonomy. Any data collected can be reprocessed, used, and analyzed in the future, in ways that are unanticipated at the time of collection. This has major implications for our freedom and democracy … It is the role of liberal democratic government to enhance liberty by protecting the private sphere. The private sphere is what makes us free people.

It should also be noted that recognizing privacy as a human right is not incompatible with a principles-based data protection framework and need not result in a law that is overly prescriptive. The prescriptive nature of a law is often related to the level of detail associated with the definition of specific privacy principles. A rights-based framework operates at the same level of generality as a principles-based law. Neither is strictly prescriptive. They are both equally flexible and adaptable to regulate a rapidly changing environment such as the world of technology and the digital economy.

As there is a growing appreciation of privacy as a right that is linked to the exercise of other human rights, a clearer

articulation of the meaning, scope and importance of this right is required. Thereby, for example, the challenges of the big data society have made it more urgent to make clear the connections between data protection and the human rights footing on which it rests. The adoption of a rights based framework would maintain flexibility but provide necessary guidance as to the underlying values, principles and objectives that should shape the interpretation and application of the statute, particularly where there may be some ambiguity in those provisions. This approach would offer consumers much better assurance that their rights would be respected by the organizations to which they entrust their personal information.

Having set out our rationale for the inclusion of a human rights-based framework in the CPPA (Consumer Privacy Protection Act), we make the following recommendations.

Addition of a preamble

Our first recommendation is to once again propose the CPPA (Consumer Privacy Protection Act) include a preamble. We previously proposed a preamble to a revised PIPEDA (Personal Information Protection and Electronic Documents Act) in our 2018-19 Annual Report and set out proposed wording. Such a preamble would serve to provide guidance as to the values, principles and objectives that should shape the interpretation and application of the CPPA (Consumer Privacy Protection Act). For instance, the addition of these clauses would make clear to those interpreting s. (section) 12(1) that "appropriate" and therefore permissible purposes under the law are to be assessed with regard to the rights and values mentioned, while recognizing the legitimate interest of organizations to process personal information responsibly.

Some raised objections to this proposal on the basis that it would be inconsistent with the constitutional grounding of the Act in the federal trade and commerce power. However, if the law is in pith and substance about regulating trade and commerce then it can include privacy protections, including privacy as a human right. In fact, a preamble would strengthen the constitutional footing of the legislation by identifying the purpose and background to the legislation. [8](#fn8) The absence of a preamble has been noted by the Supreme Court as creating difficulties in carrying out a division of powers analysis. [9](#fn9) Given the constitutional doubts that have been raised around PIPEDA (Personal Information Protection and Electronic Documents Act), a preamble would provide much needed interpretive guidance to the courts about the law's objective and constitutional basis.

We therefore propose the following preamble based on the version from our 2018-19 Annual Report with some additions to better capture the constitutional basis of the CPPA (Consumer Privacy Protection Act) in the federal trade and commerce power:

> **Proposed 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 relations of mutual trust and confidence that are fundamental to the Canadian social fabric and economy;
>
> 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 economic and 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 the processing of personal data should be designed to serve humankind and, in particular, must

respect the best interests of children;

WHEREAS the digital and information-based economy has the potential to bring economic, social and cultural benefits to the people of Canada;

WHEREAS the objective of this law is to promote and support electronic commerce by ensuring that individuals can engage in the digital and information-based economy with the knowledge that their privacy rights will be respected, thereby ensuring the benefits of this economy can be realized for all;

WHEREAS this law protects the privacy rights of individuals while recognizing the legitimate interest of organizations to collect, use and disclose personal information for purposes that a reasonable person would consider appropriate in the circumstances and in ways that do not represent surveillance;

WHEREAS the right to privacy must be balanced with other fundamental rights such as the right to freedom of expression in circumstances in which the collection, use or disclosure of personal information serves a legitimate public interest;

AND WHEREAS this statute has been recognized by the courts as being quasi-constitutional in nature;

Recommendation 1: That the CPPA (Consumer Privacy Protection Act) be amended to introduce the proposed preamble.

Revised sections 5, 12, and 13

In addition to including a preamble, we believe that amendments to sections 5, 12 and 13 of the CPPA (Consumer Privacy Protection Act) can introduce a more appropriate weighting of privacy rights and commercial interests while strengthening the law's grounding in Parliament's jurisdiction to legislate in respect of trade and commerce under the *Constitution Act, 1867*.

The amendments we are proposing build on the existing structure of ss. (sections) 3 and 5(3) of PIPEDA (Personal Information Protection and Electronic Documents Act), to become ss. (sections) 5 and 12 of the CPPA (Consumer Privacy Protection Act). Within this structure, section 5 of the CPPA (Consumer Privacy Protection Act) already recognizes "the right to privacy of individuals." We also note that sections 12 and 13 incorporate aspects of necessity and proportionality, concepts derived from human rights law, in order to assess whether an infringement of privacy is reasonable. We are proposing amendments to these provisions to ensure that more appropriate weight is given to the right to privacy, all within a structure previously approved by Parliament and, therefore, likely constitutional.

Section 5

Section 5 – the CPPA (Consumer Privacy Protection Act)'s purpose clause – should be amended to no longer refer to privacy rights in a technical and narrow sense, and instead recognize their true nature as a quasi-constitutional right. It should also provide a more appropriate weighting for privacy rights by adding privacy considerations to balance the new economic factors. Lastly, it should provide a more clear statement of the law's purpose and constitutional grounding. As with the preamble, these changes will make the law stronger, not weaker, from a constitutional perspective.

Our proposal, which seeks to more clearly state the purpose of the legislation, is set out in the box below.

In the same way that the purpose clause provides new context for the interpretation of business purposes it should provide new context and clarification to the reference to privacy rights.

The reference to fair and lawful we are proposing here mirrors PIPEDA (Personal Information Protection and

Electronic Documents Act) Principle 4, Clause 4.4 ("Information shall be collected by fair and lawful means"), paragraph 7 (Principle 1) of the OECD (Organisation for Economic Co-operation and Development) Guidelines (http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf) governing the protection of privacy and trans-border flows of personal data (personal data "should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject"), as well as Article 5(1)(a) of the General Data Protection Regulation (GDPR) ("personal data shall be processed lawfully, fairly and in a transparent manner").

Recommendation 2: That section 5 of the CPPA (Consumer Privacy Protection Act) be amended as follow:

In an era in which significant economic activity relies on the analysis, circulation and exchange of personal information and its movement across interprovincial and international borders, the purpose of this Act is ~~to establish rules to govern the protection of personal information~~ **to promote confidence and therefore the sustainability of information-based commerce by establishing rules** ~~to govern the protection~~ **for the lawful, fair, proportional, transparent and accountable collection, use and disclosure** of personal information ~~in a manner~~ that recognize

a. the **fundamental** right of privacy of individuals,
b. ~~with respect to their personal information~~ the need of organizations to collect, use or disclose personal information for purposes **and in a manner** that a reasonable person would consider appropriate in the circumstances, and
c. **where personal information moves outside Canada, that the level of protection guaranteed under Canadian law should not be undermined.**

Section 12

Next, we recommend amendments to subsection 12(1).

First, we believe that it would be beneficial to make explicit that an examination of appropriateness requires an assessment of not only the organization's purposes but also the means by which it seeks to achieve that purpose. This would not be a novel measure, but rather a codification of how the equivalent subsection in PIPEDA (Personal Information Protection and Electronic Documents Act) (ss. (sections) 5(3)) has been interpreted and applied by the Courts and our Office. We have proposed a similar reference in the purpose clause mentioned above.

Recommendation 3: That subsection 12(1) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

An organization may collect, use or disclose personal information only for the purposes **and in a manner** that a reasonable person would consider appropriate in the circumstances.

Second, subsection 12(2) and the factors it describes should also be amended.

Subsection 12(2) should be amended in two ways. First, a reference should be added to the appropriateness of the manner of collection, use or disclosure, and not only their purposes, to mirror the proposed amendment to subsection 12(1). A proportionality analysis includes an assessment of both purposes and means.

Additionally, the proposed enumeration of factors which must be taken into account in evaluating appropriateness is unduly inflexible and does not reflect the approach of the Federal Court. The Federal Court has held (in *Eastmond*)

that PIPEDA (Personal Information Protection and Electronic Documents Act)'s s. (section) 5(3) – the precursor to the CPPA (Consumer Privacy Protection Act)'s s. (section) 12 – required an assessment of appropriateness "in a contextual manner looking at the particular circumstances of why, how, when, and where collection takes place … all of which suggests flexibility and variability in accordance with the circumstances." The Federal Court of Appeal has also recognized that the test of what a reasonable person would consider appropriate must be assessed against the particular circumstances that exist at a given time. [10](#fn10)

So, whereas Federal Court jurisprudence requires a contextual assessment of appropriateness, s. (section) 12(2) of the CPPA (Consumer Privacy Protection Act) would dictate a consideration of specific factors, some of which may be irrelevant in some circumstances, to the exclusion of others that may well be relevant.

As such, we propose new text for subsection 12(2) which clarifies that the factors to be considered in an assessment of appropriateness will vary by context, and that the enumerated factors are non-exhaustive.

Recommendation 4: That subsection 12(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

The ~~following~~ factors ~~must~~ **to** be taken into account in determining whether the purposes **and manner** referred to in subsection (1) are appropriate **include**:
…
(g) any other relevant factors in the circumstances

Lastly, in this section, we also recommend amendments to the factors set out in paragraphs 12(2)(a) to (e). In particular:

First, if subsection 12(2) is not amended to clarify that the application of the factors will vary based on the circumstances of the collection, use or disclosure, we recommend the deletion of the first factor (sensitivity of the information). Without this amendment, there is an implication that the appropriateness of the collection, use or disclosure of information deemed 'not sensitive' need not be as closely examined as that of more sensitive information. However, our preference would be to retain this criteria as part of a contextual, non-exhaustive list of factors.

Paragraphs (d) and (e) should also be amended to strike a more appropriate balance between the right to privacy and commercial interests. In the case of paragraph (d) – which speaks to the existence of less intrusive means of achieving a purpose at a "comparable cost and with comparable benefits," while costs and benefits to the organization are relevant factors to what is, essentially, a proportionality analysis, the notion that slightly higher costs might justify more privacy intrusive measures is plainly inappropriate. Similarly, paragraph (e) – which speaks to whether benefits are proportionate to the individual's loss of privacy – ends with the consideration of mitigations implemented by the organization, without equally considering aggravating factors with respect to the magnitude of the loss of rights. For both s. (section) 12(d) and (e), we recommend the deletion of the qualifier at the end of the paragraph not due to irrelevance, but to address a lack of balance.

Paragraph (e) is also too narrow in its reference to privacy, in that it does not characterize privacy as a fundamental or quasi-constitutional right. The benefits obtained by an organization should not be weighed solely against a loss of privacy in a narrow and technical sense, but against all fundamental rights and interests such as an individual's autonomy, dignity or equality rights, that are impacted by a collection, use or disclosure. We have proposed two options for revised language.

First, and our preference, is to weigh broadly the individual's loss of privacy or other fundamental rights and interests as the counterbalance to any benefits obtained. In the alternative, we would propose language as suggested by the

Government of Canada in the Department of Justice paper "Respect, Accountability, Adaptability: A public consultation about modernization of the *Privacy Act*", which recognizes the association of privacy with "dignity, autonomy, and self-determination." While we believe there is significant benefit to the breadth of our first formulation, which recognizes the relationship between privacy and the exercise of other fundamental rights, inclusion of the language found in the *Privacy Act* discussion paper would nonetheless be a meaningful improvement.

Lastly, we have proposed two additional factors. First, we recommend that if our proposal to refer to the "manner" of the collection, use or disclosure in s. (section) 12(1) and the opening words of s. (section) 12(2) is accepted, then the list of factors in s. (section) 12(2) should include one relevant to means. We suggest that this factor require consideration of whether information was collected, used or disclosed in a fair, lawful and transparent means.

Second, as noted above, a new final factor under (g) – 'any other relevant factors(s) in the circumstances' – is being proposed to emphasize that the list of factors is not exhaustive.

Recommendation 5: That the factors set out in subsection 12(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

a. the sensitivity of the information; **[delete if the proposed amendment make to subsection 12(2) non-exhaustive is not adopted]**
b. whether the purposes represent legitimate business needs of the organization;
c. the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs;
d. whether there are less intrusive means of achieving those purposes ~~at a comparable cost and with comparable benefits~~; ~~and~~
e. whether the individual's loss of privacy **or other fundamental rights and interests** is proportionate to the benefits ~~in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual~~;

> [Alternatively, the clause could be amended as: "whether the individual's loss of privacy, **dignity, autonomy and self-determination** is proportionate to the benefits."]

f. **[if subsections 12(1) and 12(2) are amended as proposed to refer to means] whether the personal information is collected, used or disclosed in a fair, lawful and transparent manner; and**
g. **any other relevant factor(s) in the circumstances.**

Section 13

Section 13 incorporates in the CPPA (Consumer Privacy Protection Act) the data minimization principle, an adaptation into privacy law of the necessity analysis under human rights law. In fact, s. (section) 13 uses the word "necessary" in relation to the collection of personal information.

In the laws of other jurisdictions, data minimization requires that only personal information necessary for "specified, explicit and legitimate purposes" may be collected: see for instance article 5(1)(b) of the GDPR (General Data Protection Regulation). Article 15 of Japan's *Protection of Personal Information Act* requires that purposes must be defined "as explicitly as possible." The current federal law in Canada, in Principle 4.3.3 of PIPEDA (Personal Information Protection and Electronic Documents Act), also makes reference to "explicitly specified, and legitimate purposes."

This requirement that purposes be specific or explicitly specified has been removed in Bill C-11, giving organizations much more discretion in defining the purposes for which they will collect information. With the result that, conceivably, organizations could seek consent for vague and mysterious purposes, such as “improving your consumer experience.”

As such, amending section 13 to require that purposes be specific, explicit and legitimate would both strengthen the necessity analysis and make consent more meaningful by ensuring that the purposes at the centre of consent are understandable.

Recommendation 6: That subsection 13 of the CPPA (Consumer Privacy Protection Act) be amended as follows:

The organization may collect only the personal information that is necessary for the **specific, explicit, and legitimate** purposes determined and recorded under subsection 12(3).

Finally, with respect to the human rights framework, we will address the issue of key definitions within the CPPA (Consumer Privacy Protection Act).

Other considerations

Definition of personal information

As discussed in the OPC (Office of the Privacy Commissioner of Canada)’s recent publication, A Regulatory Framework for AI (artificial intelligence): Recommendations for PIPEDA (Personal Information Protection and Electronic Documents Act) Reform (/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/reg-fw_202011/) (AI (artificial intelligence) paper) and elaborated in the accompanying paper (/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-ai/pol-ai_202011/) from Professor Ignacio Cofone, an important measure related to the human-rights approach would be to amend the definition of personal information so that it explicitly includes inferences drawn about individuals.

Inferences refer to a conclusion that is formed about an individual based on evidence and reasoning. In the age of AI (artificial intelligence) and big data, inferences can lead to a depth of revelations, such as those relating to political affinity, interests, financial class, race, etc. This is important because the misuse of such information can lead to harms to individuals and groups in the same way as collected information – a position confirmed by the Supreme Court in *Ewert v. (versus) Canada*. In fact, as noted (https://iapp.org/media/pdf/resource_center/wp203_purpose-limitation_04-2013.pdf) by the former European Article 29 Data Protection Working Party, “[m]ore often than not, it is not the information collected in itself that is sensitive, but rather the inferences that are drawn from it and the way in which those inferences are drawn, that could give cause for concern.”

General support for the idea that inferences constitute personal information can be found in past OPC (Office of the Privacy Commissioner of Canada) decisions and Canadian jurisprudence. For instance, the OPC (Office of the Privacy Commissioner of Canada) has found that credit scores amount to personal information (PIPEDA (Personal Information Protection and Electronic Documents Act) Report of Findings #2013-008 (/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2013/pipeda-2013-008/), among others), and that inferences amount to personal information under the *Privacy Act* (Accidental disclosure by Health Canada (/en/opc-actions-and-decisions/investigations/investigations-into-federal-institutions/2014-15/pa_20150303/), paragraph 46). This is also consistent with the Supreme Court’s understanding of informational privacy, which

includes inferences and assumptions drawn from information. [11](#fn11)

However, despite this, there remains some debate as to how inferences are regarded. Some view them as an output derived from personal information, like a decision or an opinion might be, and argue these are outside the purview of privacy legislation. Given that inferences are typically drawn using an analytical process, such as through algorithms, others claim that these are products created by organizations using their own estimations, and that they do not belong to individuals.

In light of these conflicting viewpoints, we believe the law should be clarified to include explicit reference to inferences under the definition of personal information. This would be in accordance with modern privacy legislation such as the *California Consumer Privacy Act* (CCPA), which explicitly includes inferences in its definition of personal information. The OAIC (Office of the Australian Information Commissioner)'s proposed amendments (https://www.oaic.gov.au/assets/engage-with-us/submissions/Privacy-Act-Review-Issues-Paper-submission.pdf) to the *Australian Privacy Act* also support this approach.

Importantly, even where there is agreement that inferences are personal information, the fact that they could reveal commercial trade secrets is used by some as a basis to deny individuals certain privacy rights, such as to access or correction. Our recommendations for automated decision-making propose a fair way to resolve this contention.

Recommendation 7: That the definition of personal information be amended to expressly include inferred information.

Definition of sensitive information

Under subsection 12(2)(a), one of the factors to consider when determining whether a reasonable person would consider an organization's purposes appropriate under the circumstances is "the sensitivity of the information." This is also a consideration that organizations must take into account with respect to the form of consent (s. (section) 15(4)), the development of an organization's privacy management program (s. (section) 9(2)), the level of protection provided by security safeguards (s. (section) 57(1)), the evaluation of whether a breach creates a real risk of significant harm (s. (section) 58(8)), and other requirements within the CPPA (Consumer Privacy Protection Act).

While the OPC (Office of the Privacy Commissioner of Canada) and the courts have provided some interpretations of sensitive information, it would be preferable to have a legislative definition that sets out a general principle and is context-specific, followed by an explicitly non-exhaustive list of examples (such as those included in article 9 of the GDPR (General Data Protection Regulation)). This would provide greater certainty for organizations and consumers as to the interpretation of the term. For instance, such a definition might read:

> **Sensitive information** means personal information for which an individual has a heightened expectation of privacy, or for which collection, use or disclosure creates a heightened risk of harm to the individual. This may include, but is not limited to, information revealing racial or ethnic origin, gender identity, sexual orientation, political opinions, or religious or philosophical beliefs; genetic information; biometric information for the purpose of uniquely identifying an individual; financial information; information concerning health; or information revealing an individual's geolocation.

Further, we note that the French version of PIPEDA (Personal Information Protection and Electronic Documents Act) currently refers to "renseignements … sensibles" contrary to the CPPA (Consumer Privacy Protection Act) which

proposes to rely on the term “de nature délicate”. Quebec’s Bill 64 also refers to “renseignement personnel sensible”, while the GDPR (General Data Protection Regulation) uses the term “données sensibles”. To ensure consistency with the current statute and to promote alignment with the laws of Quebec and the EU (European Union), we suggest that the French version of the CPPA (Consumer Privacy Protection Act) revert to the term “sensible” as opposed to “de nature delicate”.

Recommendation 8: That a definition of sensitive information be included in the CPPA (Consumer Privacy Protection Act), that would establish a general principle for sensitivity followed by an open-ended list of examples.

Definition of commercial activity

For what we understand are reasons of clarity, rather than a desire to change the scope of the activities governed by federal private-sector privacy law, the CPPA (Consumer Privacy Protection Act) would add a contextually-dependent approach (adding the words “taking into account an organization’s objectives…”) to characterizing commercial activity. We find this very interesting, but are concerned that this change in structure from the PIPEDA (Personal Information Protection and Electronic Documents Act) definition may exclude certain activities that are commercial in nature but carried out by organizations that overall do not have commercial objectives. These activities, undertaken by charities, professional associations or non-profit organizations, are currently governed, properly in our view, by PIPEDA (Personal Information Protection and Electronic Documents Act).

To ensure commercial activities carried out by non-commercial entities continue to be governed by privacy law, we recommend that the definition be divided in two paragraphs, one referring to commercial activities carried out by any entity, whether commercial or not, and the other referring to any activity, commercial or not, carried out by a commercial organization. This would maximize, within a reasonable understanding of what is “commercial”, privacy protection for all activities related to personal data.

Recommendation 9: That the definition of commercial activity be clarified as follows:

Commercial activity means:

a. any particular transaction, act or conduct ~~or any regular course of conduct~~ that is of a commercial character, **whether or not it is committed by an organization whose general objectives are of a commercial character**; or
b. any regular course of conduct that is of a commercial character, **including any activity that is part of a regular course of conduct that is of a commercial character** taking into account an organization’s objectives ~~for carrying out the transaction, act or conduct~~ **and** the context in which it takes place~~, the persons involved and its outcome~~.

Political Parties

Related to the scope of activities governed by the CPPA (Consumer Privacy Protection Act), we affirm our position that political parties should be subject to privacy obligations, and that it would be reasonable for federal political parties to be regulated under the CPPA (Consumer Privacy Protection Act).

The question of whether federal political parties should be subject to privacy regulation – one of the matters discussed in ETHI (Standing Committee on Access to Information, Privacy and Ethics)’s 2018 report, Democracy

Under Threat (https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf) – is, at this point, largely no longer a contentious one. Political parties collect significant amounts of information about voters (as well as volunteers, employees, and candidates) and use this data for micro-targeted political campaigning, among other things. These practices have the potential to have significant privacy impacts and, done improperly, threaten trust in the democratic system. Jurisdictions around the world – including the European Union (EU), United Kingdom (UK), New Zealand, Argentina and Hong Kong, not to mention British Columbia and, if Bill 64 is adopted, Quebec – have privacy laws that govern political parties, and even a decade ago (long before the Cambridge Analytica scandal) an OPC (Office of the Privacy Commissioner of Canada) survey found that 92% of Canadians supported the notion that political parties should be subject to some form of privacy regulation.

The question then becomes not whether but how to regulate federal political parties' collection and use of personal information.

Broadly, there are four options available: inclusion of federal political parties under the CPPA (Consumer Privacy Protection Act), inclusion under the *Privacy Act*, amendment of the *Canada Elections Act*, or introduction of new, standalone legislation. While there are merits to each approach, the timeliness of the first makes it worthy of significant consideration.

While federal political parties do not explicitly fall under the ambit of the CPPA (Consumer Privacy Protection Act) as currently drafted, subsection 6(3) and paragraph 119(2)(c) provide a mechanism by which the Governor-in-Council can list an organization as being subject to the Act. Currently, the World Anti-Doping Agency (WADA) has been made subject to the Act in this manner.

That federal political parties are different in nature from commercial organizations must be recognized, but British Columbia and Quebec provide two potential models for accommodating this within a private sector-focused legislation. British Columbia's *Personal Information Protection Act* (PIPA) does not include any special considerations for political parties, but instead provides an exception to consent for collection of personal information when authorized by law. This, in combination with the BC *Election Act*, permit (and restrict) the use of voter list information for (and to) the "electoral purposes" for which it was collected. Quebec's Bill 64, on the other hand, specifically exempts political parties from the application of certain sections of the proposed Act (exemptions which, it should be noted, are not supported by the Commission d'accès à l'information du Québec).

We would support a slight variation on the British Columbian approach to regulation. Acknowledging the importance of permitting democratic outreach, an exception to consent could be introduced which narrowly applies to such activities.

Recommendation 10: Subject federal political parties to the CPPA (Consumer Privacy Protection Act), for example by registering them in the schedule pursuant to subsection 6(3) and paragraph 119(2)(c).

Theme two: Specific rights and obligations

Having considered the overall underpinnings of the legislation, we turn our attention to operational considerations – specifically how this framework will apply in practice. We focus on three particular areas: consent and the exceptions thereto; organizational obligations, and individual data rights.

Valid vs. meaningful consent

One of the proposed pillars of Bill C-11 is to enhance consumers' control over their personal information. To achieve

this, rules governing consent must ensure it is informed and meaningful.

In 2015, section 6.1 was added to PIPEDA (Personal Information Protection and Electronic Documents Act) to specify that consent would only be considered valid if "it is reasonable to expect that an individual to whom the organization's activities are directed would understand the nature, purpose, and consequence of [the activity to which they are consenting]."

The "understanding" requirement, which is key to the validity of consent, is unfortunately absent from the CPPA (Consumer Privacy Protection Act). Instead, the Bill seeks to give consumers more control by prescribing elements that must appear in a privacy notice, in plain language. While this seems similar to the approach taken in our 2018 Guidelines for obtaining meaningful consent (/en/privacy-topics/collecting-personal-information/consent/gl_omc_201805/), it is not the case because again, the requirement of "understanding" is missing. Compare our guidelines, which require that purposes for which information is collected must be explained "in sufficient detail for individuals to meaningfully understand what they are consenting to," with s. (section) 15(3) of the CPPA (Consumer Privacy Protection Act), which simply requires that consumers be informed of "the purposes for the collection, use or disclosure of the personal information determined by the organization…"

As noted earlier in theme one, under the Bill the purposes "determined by the organization" do not have to be "specific, explicit and legitimate."

By prescribing elements of information to appear in privacy notices without maintaining the requirement that consumers must be likely to understand what they are asked to consent to, the CPPA (Consumer Privacy Protection Act) does not achieve its goal of giving individuals more control over their personal information; it provides less. This is exacerbated by the open-ended nature of the purposes for which organizations may seek consent.

In our view, this is because the Bill is incorrectly calibrated. We agree that organizations should be able to innovate, to have flexibility in the processing of personal data and to define the purposes for which they wish to collect, use and disclose personal information, but this flexibility should be exercised within a legal framework that provides objective standards, enforced by an independent regulator in the public interest.

As drafted, the Bill places too much emphasis on providing organizations flexibility in defining the purposes for which personal information may be used and in obtaining consumer consent. Legislators should enact objective standards such as the one in section 6.1 of the current Act (the "understanding" factor) and the requirement that purposes be defined in a specific, explicit and legitimate manner, as set out in Principle 4.3.3 of PIPEDA (Personal Information Protection and Electronic Documents Act) and in the laws of other jurisdictions.

Also relevant to understanding is how information is presented. The CPPA (Consumer Privacy Protection Act) does not speak to format, content structure, or accessibility. Each of these is a factor that contributes to an individual's understanding of how their personal information is being used. Plain language information that is difficult to find, or presented in a format that makes comprehension difficult, does not lead to understanding (or meaningful consent). Poorly designed or formatted information may ultimately be as inaccessible as poorly drafted language – particularly for individuals who rely on accessibility tools, such as screen readers, or in certain circumstances, minors. As such, we recommend that s. (section) 15(3) speak to the format of information being provided to individuals, in addition to the plain language requirement.

Recommendation 11: That subsection 15(3) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with **the following information, in a manner such that it is reasonable to expect that the individual would understand the nature, purpose and consequences of the intended**

collection, use or disclosure. This information **must be presented in an intelligible and easily accessible format, using clear and** ~~in~~ plain language.

Next, while the OPC (Office of the Privacy Commissioner of Canada) is supportive of subsection 15(4)'s recognition of express consent as the default form of consent, as drafted this provision would allow an organization to rely on implied consent where it "establishes" (in French, "*conclure*") that this would be appropriate, in light of listed factors. Bill C-11 therefore seems to give deference to an organization's conclusion that implied consent is appropriate, as opposed to prescribing an objective assessment of the relevant factors. We recommend that the phrase "the organization establishes that" be removed. As a result, organizations would, of course, continue to determine in the first instance if the objective conditions for implied consent are met, but this assessment would be reviewable independently by the regulator and ultimately the courts, as a matter of law and without improper deference to the organization's opinion of the law.

Recommendation 12: That subsection 15(4) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

Consent must be expressly obtained unless ~~the organization establishes that~~ it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed.

Exceptions to consent

Consent, which forms the basis of many data protection laws across the globe, including PIPEDA (Personal Information Protection and Electronic Documents Act) and the CPPA (Consumer Privacy Protection Act), is not without its challenges. As outlined in our AI (artificial intelligence) paper, for individuals, long, legalistic and often incomprehensible policies and terms of use agreements make it nearly impossible to exert any real control over personal information or to make meaningful decisions about consent. For organizations, consent does not always work in the increasingly complex digital environment, such as where consumers do not have a relationship with the organization using their data, and where uses of personal information are not known at the time of collection, or are too complex to explain. These shortcomings are more pronounced in certain contexts, such as with AI (artificial intelligence).

While the CPPA (Consumer Privacy Protection Act) seeks to enhance consent in some respects, it adds important new exceptions to the consent principle. We believe that such an approach is appropriate within the framework of a modern privacy law. Among the lessons of the past twenty years, since PIPEDA (Personal Information Protection and Electronic Documents Act) was adopted, is that privacy protection cannot hinge on consent alone. In fact, consent can be used to legitimize uses that, objectively, are completely unreasonable and contrary to our rights and values. Additionally, refusal to provide consent can sometimes be a disservice to the public interest when there are potential societal benefits to be gained from use of data.

Several of the new exceptions to consent brought by Bill C-11 are reasonable. We have two main concerns: some exceptions are unreasonably broad; and the Bill fails to associate greater authority to use personal information with greater accountability by organizations for how they will use these permissions.

Business activities (s. (section) 18)

Section 18 permits the collection and use of personal information without the knowledge or consent of individuals for

defined business activities, where a reasonable person would expect the collection or use for the activity, so long as it is not for the purpose of influencing an individual's behaviour or decisions.

For an individual to understand what specific activities may be carried out under paragraphs 18(2)(a) to (f), it is critical that these be defined clearly and be within the expectations of an individual. We do not find that this is the case with respect to 18(2)(b) and 18(2)(e).

Paragraph 18(2)(b) introduces an exception to consent for activities "carried out in the exercise of due diligence to prevent or reduce the organization's commercial risk." Without a definition of "commercial risk," we would note that a plain language interpretation of this term may include any risk to commercial enterprise, such as loss of revenue. This would clearly be unacceptably broad.

If a narrower meaning is intended, such as the possibility of non-payment due to problems such as bankruptcy or insolvency, the language of s. (section) 18(2)(b) should be clarified accordingly.

Recommendation 13: That the scope of the "commercial risk" exception be limited.

More concerning to us, however, is the potential scope of the exception under paragraph 18(2)(e), which relates to activities for which obtaining consent would be impracticable because the organization does not have a direct relationship with the individual.

On one hand, it appears the intent of this provision may be in part to allow for activities such as search engines, but we do not think it achieves this goal. In our opinion, paragraph 18(2)(e) would cover search engines crawling and indexing of the web without consent. However, as this exception relates only to "collection and use," and not disclosure, it does not appear to permit all aspects of a search engine's operations such as the display of search results.

The wording of paragraph 18(2)(e) also raises more fundamental concerns. First, we note that the potential scope of activities which could fall under this exception is extremely broad. It is difficult to conceive if there are any real limitations on the kinds of activities which could be pursued by an organization pursuant to this provision. The limit prescribed by s. (section) 18(1)(a), that "a reasonable person would expect such a collection or use for that activity," utterly fails to provide consumers with any certainty as to how their personal information will be used, moreover, by an organization they likely do not know. This is far removed from giving consumers more control over their personal information.

Among organizations that would appear to benefit from s. (section) 18(2)(e) are data brokers, who could thus have much greater freedom to operate than the organizations with which individuals regularly and directly interact. The business model of data brokers is opaque and creates risks for privacy. They should be more regulated, not granted greater freedom in the use of data without consent.

Lastly, the basis for the exception in paragraph 18(2)(e) simply does not withstand rigorous scrutiny. In general, we note that it would be obvious why the various provisions of s. (section) 18(2) could permit activity without consent. For instance, paragraphs 18(2)(c) and (d) appear intended to enable (in short) network security, and product safety, respectively. Other exceptions to consent in PIPEDA (Personal Information Protection and Electronic Documents Act) and in the Bill point to specific purposes and activities such as preventing or investigating financial abuse or fraud.

This is not the case with respect to paragraph 18(2)(e). As it is written now, paragraph 18(2)(e) removes the consent requirement from certain activities simply because obtaining consent is impracticable, not because there is an offsetting benefit to justify such an action. In other words, the fundamental principle of consent is put aside for the simple reason that it is impractical to obtain it.

In our opinion, this is inappropriate, and paragraph 18(2)(e) should be repealed. Should there be any additional, specific, legitimate activities such as search engines that were intended to be enabled via an exception, they should instead be authorized via an exception defined on the basis of explicit and knowable purpose(s) for which the data will be collected, used or disclosed.

Alternatively, as described in our AI (artificial intelligence) paper, we would also support the introduction of an exception to consent based on “legitimate commercial interests”. Such an exception would provide considerable flexibility to authorize unforeseen reasonable purposes but, unlike 18(2)(e), would be based on the particular and knowable purposes being pursued by the organization.

On the other hand, as we said in our AI (artificial intelligence) paper, we believe that such an exception should only be permitted in a rights-based regime, as described in Theme 1 of this submission. Other prerequisites should also be met in order to ensure it is used appropriately. Such pre-conditions would include the completion of a privacy impact assessment (PIA) and a balancing test similar to that found under the GDPR (General Data Protection Regulation)’s legitimate interests basis for processing. This balancing test would assess the purpose, the necessity and proportionality of the measure, and consider the interests and fundamental rights and freedoms of the individual to determine whether they override the legitimate commercial interests of organizations. Finally, such a broad exception to the consent principle should only be permitted if its application could be monitored through proactive compliance audits by the OPC (Office of the Privacy Commissioner of Canada).

Recommendation 14: That paragraph 18(2)(e) be repealed, and that either:

i. Any legitimate commercial interests which would have been enabled by paragraph 18(2)(e) be authorized via an explicit and knowable exception to consent; or,
ii. A legitimate commercial interests exception to consent be introduced if accompanied by the introduction of a rights-based regime and pre-conditions such as the conduct of a PIA (Privacy Impact Assessment) and a balancing test, and if monitoring of its application was possible through proactive compliance checks by the OPC (Office of the Privacy Commissioner of Canada).

Socially beneficial purposes (s. (section) 39)

Overall, the OPC (Office of the Privacy Commissioner of Canada) is supportive of the introduction of an exception to consent related to socially beneficial purposes as proposed in the CPPA (Consumer Privacy Protection Act). There are clearly significant advantages to permitting the processing of personal information for socially beneficial purposes, and modern privacy legislation should responsibly facilitate such uses. We examine this issue in detail in our AI (artificial intelligence) paper.

While we have certain, limited recommendations to make on how this measure could be enhanced, we note that certain features have manifestly been added to limit the potential privacy risks associated with the provision.

For example, only de-identified information may be disclosed, which is an important privacy protective measure. Additionally, the exception only applies to disclosures of personal information to listed or prescribed entities. These classes of organizations and entities appear to be those that implicitly or explicitly have a mandate to carry out activities of a socially beneficial character. All of these are positive aspects from a privacy perspective.

Despite these positive aspects, we propose a number of recommendations which aim to establish appropriate checks and balances for the sharing of information between organizations, inspired in part by provisions related to research and statistical analysis in Quebec’s Bill 64 (s. (section) 21):

1. An entity should be required to make a written request for the information and provide certain assurances prior

to the disclosure occurring. This will allow the disclosing organization to do so responsibly knowing that the information will indeed be used for a socially beneficial purpose.

2. Both parties to the disclosure should also be required to enter into an agreement which would prohibit the recipient from re-identifying the information as well as from using the information for secondary purposes which are not of a societal benefit. These agreements should be available for review by the OPC (Office of the Privacy Commissioner of Canada) on request. Importantly, while it is an offence under the CPPA (Consumer Privacy Protection Act) to use de-identified information to identify an individual, this would not likely extend to entities to whom de-identified information is disclosed. Re-identification should therefore be prohibited under agreement.
3. Finally, the CPPA (Consumer Privacy Protection Act) would authorize the making of regulations prescribing new socially beneficial purposes and new entities who might be authorized to use personal information for these purposes. We find this appropriate, as it is clear that new socially beneficial purposes will arise from time to time after the CPPA (Consumer Privacy Protection Act) becomes law, but we think this flexibility to regulate should be subject to objective limits set by Parliament. For example, the definition of “socially beneficial purposes” could be modified to only include “activities that are beneficial to society and not simply of individual or commercial interest or profit.” [12](#fn12)

Recommendation 15: That s. (section) 39 of the CPPA (Consumer Privacy Protection Act) be amended to require:

- A written request be made prior to information being disclosed to ensure that the use is of societal benefit as defined in the CPPA (Consumer Privacy Protection Act);
- An information sharing agreement be entered into, which would prohibit the recipient from re-identifying the information as well as from using the information for secondary purposes which are not of a societal benefit; and
- The definition of "socially beneficial purposes" should be amended to include a limit on regulatory power, for example by indicating that they must be “purposes that are beneficial to society and not simply of individual or commercial interest or profit.”

Publicly available personal information (s. (section) 51)

With respect to publicly available personal information, the OPC (Office of the Privacy Commissioner of Canada) generally supports the approach taken in the CPPA (Consumer Privacy Protection Act) (which mirrors existing provisions under PIPEDA (Personal Information Protection and Electronic Documents Act)) so long as appropriate limitations are established in the Act to frame any modifications or additions to the list of publicly available information to be specified by regulation.

In the context of *Privacy Act* reform, we have recommended that any definition of publicly available information should address, among other considerations,

> …the context in which the information is made public, including whether the individual has a reasonable expectation of privacy in the information irrespective of the fact that it is publicly available.

While the types of information listed in the current regulations are very much a product of the time in which those regulations were introduced, we suggest that the overall approach of recognizing the context of publication should be maintained, with added emphasis on whether individuals have a reasonable expectation of privacy in the information.

Under PIPEDA (Personal Information Protection and Electronic Documents Act), the OPC (Office of the Privacy Commissioner of Canada) has seen multiple instances in which an organization has argued for the legitimacy of their activities based at least in part on their reliance on information that was accessible to the public. Among the best known of these is Globe24h (/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2015/pipeda-2015-002/), which operated what was effectively an extortion scheme in which sensitive court findings were scraped and re-posted in a way that made them accessible to search engines, only to be taken down upon receipt of payment.

More recently, the OPC (Office of the Privacy Commissioner of Canada) released its findings from an investigation of Clearview AI (artificial intelligence) (/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/), a company whose technology allowed law enforcement and commercial organizations to match photographs of unknown people against the company's databank of more than 3 billion images, including of Canadians and children, for investigation purposes. The company argued the images scraped from websites across the Internet (including social media) were publicly available, and that individuals had no reasonable expectation of privacy. This ignores that no person would have a reasonable expectation that photos posted on social media would be used for such a purpose. It also ignores the fundamental affront caused by this technology to individuals' privacy rights, and the broad-based harm inflicted on all members of society, who find themselves under continual mass surveillance by Clearview based on its indiscriminate scraping and processing of their facial images.

These experiences show there is a need to avoid an overly broad interpretation of how "publicly available information" can be used without consent, as such an interpretation could lead to serious harms. In particular, the legislation must ensure that an individual's reasonable expectations are taken into consideration in determining whether information is "publicly available".

Recommendation 16: That s. (section) 51 of the CPPA (Consumer Privacy Protection Act) be amended to provide, in addition to the conditions already present, that the personal information is such that the individual would have no reasonable expectation of privacy.

De-identification

On the whole, the OPC (Office of the Privacy Commissioner of Canada) supports the scheme proposed in the CPPA (Consumer Privacy Protection Act) with respect to de-identified information. The CPPA (Consumer Privacy Protection Act) would create flexibility in the use of this information, while ensuring that it remains under the legislation's protection. We recommend that any modification to this regime preserve this general principle.

However, there are some that have argued that under the CPPA (Consumer Privacy Protection Act) de-identified information is not personal information and therefore is out of scope, except for specific defined uses. We recommend that the more privacy protective interpretation that we believe was intended be made explicit to address any ambiguity and to be clear on the CPPA (Consumer Privacy Protection Act)'s application to de-identified personal information.

By treating de-identified information as "personal information," the CPPA (Consumer Privacy Protection Act) prevents this information from falling outside the scope of the law. Given the ever-present potential for de-identified information to be re-identified, as well as the potential for such information to be used in ways which could have significant impacts on individuals' rights, it is important that organizations clearly understand that, though additional flexibility is granted for certain uses, privacy legislation will remain in effect when de-identified information is used.

The CPPA (Consumer Privacy Protection Act) also sets a high threshold for de-identification procedures, both in how it defines "de-identify" and in the requirements it sets out for doing so. For example, the CPPA (Consumer Privacy Protection Act) requires organizations to use de-identification procedures that are proportionate to the purposes of de-

identification and to the sensitivity of personal information involved (s. (section) 74), and which ensure personal information could not be used to identify someone in reasonably foreseeable circumstances. The OPC (Office of the Privacy Commissioner of Canada) supports this approach, which provides organizations with flexibility in their use of de-identification techniques while also holding those organizations accountable.

The OPC (Office of the Privacy Commissioner of Canada) has long been addressing the issue of data de-identification. For instance, in our 2016-17 Annual Report (/en/opc-actions-and-decisions/ar_index/201617/ar_201617/), which included our *Report on Consent* (/en/opc-actions-and-decisions/ar_index/201617/ar_201617/#heading-0-0-3-1), the outcome of a significant public consultation on the concept of consent under PIPEDA (Personal Information Protection and Electronic Documents Act), we wrote:

> Given the vast amounts of personal information being processed in the digital environment, de-identification may seem like a promising measure for enhancing privacy protection. At the same time, we acknowledge concerns that re-identification is a real risk not only because of the availability of data sets that can be used to re-identify personal information, but also because of the lack of rigour in de-identification methods. Nonetheless, we are guardedly optimistic that de-identification can be a viable solution provided it is managed appropriately.

We maintain this overall optimism, having formulated the following as recommendations in our response to consultations on modernization of the *Privacy Act* (/en/opc-actions-and-decisions/submissions-to-consultations/sub_jus_pa_2103/):

- The Act should recognize that re-identification of personal information is always a possibility, depending on the context.
- The Act should define de-identified information to allow for a more targeted and nuanced application of certain rules. For instance, while de-identified information might be exempted from certain provisions of the *Privacy Act*, or their application nuanced, other provisions would continue to apply; de-identified information should not be completely carved out.

We believe that the CPPA (Consumer Privacy Protection Act) has struck an appropriate balance with respect to de-identification, encouraging innovation by providing flexibility to organization while maintaining necessary controls and oversight. However, as referenced, we recommend the Act be amended to be explicit that it applies to de-identified information as we believe is the intention.

Recommendation 17: That the CPPA (Consumer Privacy Protection Act) maintains its current balance of providing organizations flexibility with respect to use of de-identified personal information while maintaining necessary controls and oversight by including de-identified information within the scope of the law.

That the Act be amended to be explicit that it applies to de-identified information to address any potential ambiguity in this interpretation.

Disclosures to law enforcement

Lastly, we consider the issue of the disclosure of personal information to law enforcement and other government agencies under sections 44 to 50 of the CPPA (Consumer Privacy Protection Act). While we believe the drafting of

these sections is an improvement on the equivalent provisions in PIPEDA (Personal Information Protection and Electronic Documents Act), we nonetheless believe that they should be enhanced by (i) clarifying organizations' obligations following the 2014 *R. v (versus) Spencer* Supreme Court decision, and (ii) introducing reporting requirements for government and record-keeping (and/or basic transparency reporting) obligations for organizations.

Post-Spencer, disclosure to government under this section remains controversial, as government agencies (including law enforcement) continue to make requests to organizations to obtain personal information absent court authorization. Furthermore, at present, there is little in the way of record keeping, transparency, ongoing oversight, or accountability requirements associated with this exception to consent – despite the fact that those companies which voluntarily publish transparency reports indicate hundreds of thousands of customer records requests being received annually.

As such, we propose two modifications to the Bill in support of enhanced transparency.

First, that disclosures under sections 43, 44, 45 and 50 only be permitted to government requestors that are subject to a record keeping requirement – an option specifically posed in the Department of Justice's *Privacy Act* modernization paper ("Where proactive publication of information was not possible because of its sensitive nature, record-keeping requirements [for government organizations] subject to the Privacy Commissioner's oversight could serve as an accountability substitute.")

Second, organizations should have a similar requirement to maintain records of – and, ideally, make transparent on an annual basis – the number and nature of requests received from government for personal information under sections 43 to 50, and the outcome of those requests.

Recommendation 18: That record-keeping and reporting requirements be established with respect to disclosures of personal information to government organizations, especially with respect to disclosures to law enforcement.

Beyond transparency, clarity is also required with respect to the impact of the 2014 *R v. (versus) Spencer* decision with respect to when the state can obtain personal information via warrantless access. When Bill S-4 was before Parliament, the OPC (Office of the Privacy Commissioner of Canada) recommended (https://www.priv.gc.ca/en/opc-actions-and-decisions/advice-to-parliament/2015/parl_sub_150212/) that:

> a legal framework, based on the Spencer decision, is needed to provide clarity and guidance to help organizations comply with PIPEDA (Personal Information Protection and Electronic Documents Act) and ensure that state authorities respect the Supreme Court of Canada's decision. Such a framework would provide Canadians with greater transparency about private sector disclosures of personal information to state agencies.

The ambiguity with respect to the meaning of "lawful authority" that existed in PIPEDA (Personal Information Protection and Electronic Documents Act) remains in the CPPA (Consumer Privacy Protection Act), as evidenced by companies' continued disclosures of personal information without consent to police and other law enforcement agencies absent a court order.

As such, we reiterate and update for Bill C-11 a recommendation previously made in our 2015 submission to Parliament on Bill S-4, that a clarifying provision be introduced that defines lawful authority for the purposes of section 44. This provision would make clear that discretionary disclosures to law enforcement following a request should be

permissible only where there are exigent circumstances, pursuant to a reasonable law other than section 44 of the CPPA (Consumer Privacy Protection Act), or in prescribed circumstances where personal information would not attract a reasonable expectation of privacy.

Recommendation 19: That a definition clarifying the meaning of "lawful authority" for the purposes of section 44 be introduced.

Organizational obligations

As noted in the introduction to this submission, the increased flexibility afforded by Bill C-11 during data processing – particularly where exceptions to consent are introduced – needs to be accompanied by increased corporate responsibility. This includes heightened accountability as well as clearly delineated expectations and responsibilities. We explore these below.

Accountability

Accountability is a central and fundamental principle of privacy law, connected to and underpinning all other principles and obligations. It is also one of the primary counter-balances to the increased ability for organizations to use information without consent, as afforded by the CPPA (Consumer Privacy Protection Act). As such, it is critical that the accountability principle be clearly defined in the CPPA (Consumer Privacy Protection Act) and that the legislation provide protective measures such that the accountability of organizations is real and demonstrable.

As currently drafted, we do not consider the CPPA (Consumer Privacy Protection Act) to have hit these marks, and believe that numerous amendments are required.

First, we note that the CPPA (Consumer Privacy Protection Act) does not define accountability, except indirectly and implicitly through the requirement in s. (section) 9 to document, under the concept of a "privacy management program," certain policies, practices and procedures. Section 9 does not set an objective standard for what is accountability. It is merely descriptive (in that it identifies steps organizations may decide to take), as opposed to normative (defining what should be the intended goal, namely compliance with obligations under the law).

By contrast, Article 5(2) of the GDPR (General Data Protection Regulation) defines accountability as the controller's responsibility and ability to demonstrate compliance with all other GDPR (General Data Protection Regulation) principles. The 2012 guidance Getting Accountability Right with a Privacy Management Program (/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-compliance-and-training-tools/gl_acc_201204/), published by our Office and provincial colleagues provides that the outcome of privacy management programs "is a demonstrable capacity to comply, at a minimum, with applicable privacy laws."

Due to the fundamental importance of accountability as a means to ensure privacy protection in a law that gives organizations greater authority to process personal information without consent, we recommend that s. (section) 9 of the CPPA (Consumer Privacy Protection Act) clearly define accountability through the objective standard of compliance with the law.

Recommendation 20: That s. (section) 9 of the CPPA (Consumer Privacy Protection Act) be amended to prescribe an objective standard for accountability, as follows:

9(1) Every accountable organization must implement a privacy management program to ensure compliance with its obligations under the Act.

> (2) A privacy management program includes the organization's policies, practices and procedures that serve to ensure compliance with the Act, and includes policies, practices and procedures respecting …

Second, an increasingly important characteristic of accountability in modern privacy laws is that it be demonstrable. The OPC (Office of the Privacy Commissioner of Canada) has been a leader in this area with the publication in 2012 of our accountability guidance. Further to this publication, other jurisdictions have made their own contributions by making accountability a legal requirement, as shown by the earlier reference to Article 5(2) of the GDPR (General Data Protection Regulation). It is time that Canada's federal law incorporate this concept.

It is not sufficient that organizations comply with the law; they should have the ability to demonstrate it, principally to the regulator, by giving access upon request to the policies, practices and procedures that form part of their privacy management program, as well as other relevant records. In this way, the regulator is able to verify compliance with the law, a critical factor leading to consumer trust. In Part 3, we discuss the amendments that we believe are required with respect to the Commissioner's powers to make accountability truly demonstrable; here, we focus on record keeping as an organizational obligation.

The maintenance of adequate records to demonstrate compliance is required because, in our experience, some organizations simply "paper over" their obligations through the adoption of policies, practices and procedures, which show what should have taken place if they had been followed, without having evidence of what actually happened. Records of past activities are therefore necessary to demonstrate past compliance.

A requirement to maintain adequate records, as the requirement to develop a privacy management program, should be scalable. We note that subsection 9(2) of the CPPA (Consumer Privacy Protection Act) provides that privacy management programs may be scaled with regard to the volume and sensitivity of the personal information under the control of an organization. Section 108 refers to similar considerations, as well as the size and revenue of organizations.

We also note that Quebec's Bill 64 requires that an organization's governance policies and practices regarding personal information "be proportionate to the nature and scope of the enterprise's activities." The Office of the Australian Information Commissioner (OAIC) makes a similar point in its recent law reform submission (https://www.oaic.gov.au/engage-with-us/submissions/privacy-act-review-issues-paper-submission/), stating that the "concept of accountability focusses on whether a regulated entity has translated its privacy obligations into internal privacy management processes that are commensurate with, and scalable to, the risks and threats associated with its personal information handling activities."

In our view, volume and sensitivity of information are relevant but too narrow as considerations for scaling accountability obligations. They are subsumed in the criteria found in Bill 64 and the Australia model, but the latter two are more appropriate as they are more comprehensive.

In the context of automated decision-making, and in light of the new proposed rights to explanation and contestation, organizations should be required to log and trace the collection and use of personal information in order to adequately fulfill these rights and as part of record keeping obligations. Tracing supports demonstrable accountability as it provides documentation that the regulator could consult through the course of an inspection or investigation, to determine the personal information fed into the AI (artificial intelligence) system, as well as compliance.

As noted in our AI (artificial intelligence) paper, within Canada, Ontario's recent PHIPA (Personal Health Information Protection Act) amendments require the maintenance of an electronic audit log in the context of electronic personal health information, which must be provided to the Ontario Information and Privacy Commissioner on request. Bill 64 also includes traceability rights related to automated decision-making for individuals on request, including the right to know the personal information used to render the decision, the reasons or factors that led to the decision, as well as the right to have the personal information used to render the decision corrected.

Recommendation 21: That accountability be strengthened in the CPPA (Consumer Privacy Protection Act), by:

- Introducing a provision requiring organizations to maintain adequate records to demonstrate compliance with their privacy obligations under the Act, including an explicit traceability requirement in the context of automated decision-making;
- Amending s. (section) 9(2) so that the scaling of accountability and record-keeping obligations be dependent on the nature and importance of the personal information under an organization's control, the size and revenue of the organization, as well as relevant risks and threats.

Finally, the CPPA (Consumer Privacy Protection Act)'s provisions on accountability should explicitly include a requirement that organizations apply Privacy by Design, as recommended in ETHI (Standing Committee on Access to Information, Privacy and Ethics)'s 2018 report, *Towards Privacy by Design* (https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP9690701/ethirp12/ethirp12-e.pdf), and that PIAs (Privacy Impact Assessments) be prepared for higher risk activities. Requiring PIAs (Privacy Impact Assessments) for all activities involving personal information would create an excessive burden on organizations, particularly small and medium-sized enterprises (SMEs). But Privacy by Design and PIAs (Privacy Impact Assessments) are important for their proactivity in protecting privacy. Compliance with the law cannot rest only on investigations and penalties. Proactive strategies are equally, and in our view, more important in achieving ongoing compliance and respect for the rights of consumers.

Recommendation 22: That accountability provisions include two important proactive practices that will improve privacy compliance and respect for rights:

- Requiring that organizations practice privacy by design; and
- Requiring that PIAs (Privacy Impact Assessments) be undertaken for high risk activities.

Trans-border data flows and service providers

The cross-border flow of personal information is a specific example of an activity that reiterates the importance of the accountability principle. We recognize that trans-border data flows can create significant benefits for consumers and organizations, and that they are the subject of international trade agreements. However, they can also create inherent risks for privacy, different from the risks associated with domestic transfers of information.

As such, most modern privacy laws explicitly and separately address trans-border data flows. The EU (European Union)'s adequacy regime is best known in that regard, but countries such as Australia and New Zealand, for example, also specifically provide for the protection of the personal data of their residents when it flows outside the country. New Zealand reworked its scheme in a new law that took effect in 2020. Quebec's Bill 64 also proposes specific obligations when personal information leaves its territory. While each of these jurisdictions adopts its own approach, what is shared by all is the acknowledgement of the importance of adopting rules specific to the trans-border context.

In a paper commissioned by the OPC (Office of the Privacy Commissioner of Canada) titled *Bill C-11's Treatment of Cross-Border Transfers of Personal Information* (/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_scassa_2105/), Dr. Teresa Scassa sets out four key considerations that must be addressed in any legislation or other privacy protection framework that

addresses trans-border data flows (with our comments added):

- **To whom will the obligations apply, and in what circumstances?** Principle 4.1.3 of PIPEDA (Personal Information Protection and Electronic Documents Act) speaks to information "transferred to a third party for processing" – the conventional model of trans-border data flows. However, in the modern digital environment, personal data may flow across borders for a broad range of purposes and subject to a wide variety of arrangements between organizations, their affiliates and service providers. A law like the CPPA (Consumer Privacy Protection Act), that regulates these activities only as transfers for processing between an organization and a service provider, fails to adequately protect consumers where the data flow is of a different nature.
- **Who is accountable for the personal data that flow across borders, and in what circumstances?** In some situations, accountability will remain with the primary organization; in others, it will shift to the service provider. Again, who is accountable when the data flow is not a simple transfer between an organization and a service provider?
- **What conditions must be met before the personal data can flow across borders?** This may include notice to individuals, the level of protection required for personal information, or the safeguards and contractual or other measures which must be in place prior to a trans-border data flow taking place. On this point, the CPPA (Consumer Privacy Protection Act) interestingly sets a new threshold for the level of protection expected in a data transfer scenario, namely "substantially the same level of protection" as if the information had not been transferred. However, the reference to "otherwise" in s. (section) 11(1) should be clarified.
- **How will the level of protection afforded by the destination state's privacy regime be addressed?** Even where a contractual agreement is in place between parties, and the organization transferring the personal information retains accountability for the personal information in question, it is important to consider the destination state's privacy regime. The most frequently cited concern here is the risk of access by law enforcement or national security agencies of the receiving country. However, more generally, it will be important to understand the impact of the destination regime on the effectiveness of any and all clauses of contract governing a trans-border data flow.

The federal government is clearly aware of the significance of trans-border data flows. For instance, section 5, which sets out the law's purpose, adds language that identifies the current context as "an era in which data is constantly flowing across borders and geographical boundaries and significant economic activity relies on the analysis, circulation and exchange of personal information." Paragraphs 6(2)(a) and 62(2)(d) also refer to international transfers of personal information.

Despite these acknowledgements, and despite the fact that many jurisdictions have comprehensive schemes to govern trans-border data flows in their privacy legislation, Bill C-11 does not establish such a framework within the CPPA (Consumer Privacy Protection Act).

In order to ensure the significance and complexity of trans-border data flows and their associated privacy risks are appropriately addressed, we recommend that the CPPA (Consumer Privacy Protection Act) be amended to contain specific provisions on trans-border data flows so that rights and obligations are clear and accessible.

We recommend that separate sections be added to the CPPA (Consumer Privacy Protection Act) to address trans-border data flows. These sections would be interpreted through the amended and more balanced purpose clause found at recommendation 2. Such a clause would direct that the interpretation of the relevant sections should have regard to the benefits of trans-border data flows and also add, as a new element, the need to ensure that they do not undermine the level of protection guaranteed under Canadian law. We believe a clause such as this would be helpful in determining whether contractual or other measures adopted by organizations would, as required by s. (section) 11(1) of the CPPA (Consumer Privacy Protection Act), provide "substantially the same protection" that they are required to offer under Canadian law. Additionally, the recommended section on trans-border data flows should also, at a minimum, clearly address each of the above considerations as set forth by Dr. Scassa. In line with this, Dr. Scassa has set out extensive recommendations within her aforementioned paper, which the OPC (Office of the Privacy Commissioner of Canada) endorses. We have included these recommendations as Annex B (#toc5) to this

submission.

In addition to Professor Scassa's recommendations, there are two additional issues that we believe should be addressed. First, the CPPA (Consumer Privacy Protection Act)'s protections should be expanded to include "disclosures" to entities outside of the country, consistent with the approach taken by Canada's peers.

The CPPA (Consumer Privacy Protection Act) does not impose any special requirements on cross-border disclosures, apart from the limited transparency obligation in paragraph 62(2)(d). This approach is in contrast to the GDPR (General Data Protection Regulation), Australia, New Zealand and Quebec's Bill 64, all of which also capture disclosures in their obligations related to cross-border data flows. In other words, their rules around cross-border data flows and ensuring comparable protections are not limited to situations involving transfers to "service providers".

The premise underlying these approaches is that regardless of whether personal information is being transferred or disclosed, personal information may be at greater risk when it leaves the country. An organization should therefore take steps to ensure that there are protections in place before sending it abroad to another organization, either via contract, assessing the protections offered by foreign law or through other means. We agree with this logic and recommend the CPPA (Consumer Privacy Protection Act)'s protections be expanded accordingly to address this gap.

Second, the CPPA (Consumer Privacy Protection Act) should be amended to address asymmetries in how the CPPA (Consumer Privacy Protection Act)'s transparency obligations apply to foreign organizations that collect data in Canada but store and process it abroad.

Under the CPPA (Consumer Privacy Protection Act) as drafted, organizations must disclose if they carry out an international transfer or disclosure that may have reasonably foreseeable privacy implications (s. (section) 62(2)(d)). However, this obligation would not apply to a foreign organization with a real and substantial connection to Canada that collects personal information in Canada (for instance, via a website) but stores and processes it abroad using its own infrastructure. Such movement of data across borders within an organization would be neither a "transfer" nor a "disclosure" under the CPPA (Consumer Privacy Protection Act) and therefore would not trigger the transparency obligation.

In our view, there is no obvious reason to impose a greater transparency obligation on a Canadian organization that transfers personal information to a foreign service provider than on a foreign organization that moves personal information outside of the country. In both cases, if the flow of personal information out of the country may have reasonably foreseeable privacy implications, for instance, because of the risks posed by foreign law in the destination jurisdiction, then an organization should be required to be transparent about the risks posed. The transparency obligation in s. (section) 62(2)(d) should be broadened to include such situations.

Recommendation 23: That organizational requirements with respect to trans-border data flows be set out explicitly and separately, in a manner consistent with the recommendations set out in Annex B (#toc5).

Safeguarding

The CPPA (Consumer Privacy Protection Act) incorporates without much change the provisions of PIPEDA (Personal Information Protection and Electronic Documents Act) with respect to security measures organizations must take to protect consumers' personal information. We believe that there is an opportunity to improve these provisions to better reflect lessons learned through our investigations and the approach taken by other modern privacy laws. In particular, we recommend that safeguard obligations take into account not just the sensitive nature of the information being processed, but also the risks associated with the nature and type of processing being undertaken.

In 2016, the OPC (Office of the Privacy Commissioner of Canada) became aware of a breach of personal information

at the World Anti-Doping Agency (WADA), headquartered in Montreal. This breach involved the sensitive medical information of several athletes. Our investigation found that while a robust safeguard framework must, of course, take into account the sensitivity of the data, there are many other factors, including the risk that an organization and the information it holds will be hacked because it is a valuable target. In this case, it was very easy to see how malicious actors could be motivated to try to hack into the WADA (World Anti-Doping Agency) database.

As noted, this risk-based approach is found in other jurisdictions. For example, Article 25.1 of the GDPR (General Data Protection Regulation) requires that organizations, in determining the appropriate technical and organizational measures to implement data-protection principles, take into account "the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing." Similarly, Article 8 of the recently updated Swiss *Federal Act on Data Protection* requires organizations establish "une sécurité adéquate des données personnelles par rapport au risque encouru" (security adequate to the risks incurred).

Australia's *Privacy Act* also sets out distinct legal obligations (including security obligations) for Credit Reporting Bodies (s. (section) 20Q) and Credit Providers (s. (section) 21S). The OAIC (Office of the Australian Information Commissioner) has also interpreted that its legislation requires the adoption of privacy by design, noting in its non-binding guidance that when assessing risks, the complexity of business operations and an organization's business model are relevant factors in determining what steps would be reasonable to protect personal information.

Recommendation 24: That subsection 57(2) of the CPPA (Consumer Privacy Protection Act) be replaced by:

> In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the risks to consumers, in the event of a breach, associated with the nature, scope, and context of its use of personal information, in light of the organization's business activities.

Breach reporting

The OPC (Office of the Privacy Commissioner of Canada) must obtain timely and accurate information from organizations to assess the level of risk a specific breach presents and act accordingly. However, the timeliness for reporting is often poor; for instance, in 2020, 40% of breach reports to our office occurred three months or more after detection of the breach.

To address this, we recommend a standard by which breaches should be reported to the OPC (Office of the Privacy Commissioner of Canada) without unreasonable delay – the term used in the Alberta *Personal Information Protection Act* (PIPA) – but also within a defined time period. Globally, this period can vary, for example from 72 hours (the GDPR (General Data Protection Regulation); Egypt; Philippines; Uruguay) to 5 days (Costa Rica) to 14-15 days (Indonesia, Colombia). The OPC (Office of the Privacy Commissioner of Canada) recommends a middle ground: reporting breaches to the OPC (Office of the Privacy Commissioner of Canada) without unreasonable delay, but within 7 calendar days.

We must also consider the point from which the above timelines start. Generally, organizational awareness of a breach will be the point at which the 'clock starts', such as the GDPR (General Data Protection Regulation)'s "72 hours after having become aware of [the breach]." The CPPA (Consumer Privacy Protection Act) uses "as soon as feasible after the organization determines the breach has occurred", which is the same as PIPEDA (Personal Information Protection and Electronic Documents Act). However, it has happened quite often that a significant amount of time was taken (for example, to assess real risk of significant harm or to investigate a breach reported by a service provider or another source) between when an organization becomes aware of a breach and when it is reported to the OPC (Office of the Privacy Commissioner of Canada).

Accordingly, we recommend that the provision specify that the time for reporting to the OPC (Office of the Privacy Commissioner of Canada) begins to be calculated when the organization becomes aware of the breach. To the extent that there is any initial uncertainty about a breach including whether it poses a real risk of significant harm, the organization would be permitted to, later, make additional representations or amendments to its initial report should it have further information to provide.

Regardless, it is generally preferable that the OPC (Office of the Privacy Commissioner of Canada) be made aware of a potential breach that meets the reporting threshold at an early moment, even if some uncertainty remains. The sooner the OPC (Office of the Privacy Commissioner of Canada) is notified, the sooner we can ensure that a breach is properly contained, managed, and appropriate mitigation actions have been taken. Based on the OPC (Office of the Privacy Commissioner of Canada)'s experience and expertise in this area, we are also able to provide early guidance to organizations with respect to appropriate steps.

Individuals should also be notified as quickly as possible, given that they are the impacted parties and need to know what (if any) corrective steps they can or should take. However, we believe that the imposition of a specific maximum timeline could result in the disclosure of preliminary (and thus confusing or incorrect) information, and thus recommend that such notifications occur without unreasonable delay, without specifying the number of days.

Recommendation 25: That subsection 58(2) of the CPPA (Consumer Privacy Protection Act) be amended as:

> The report must contain the prescribed information and must be made in the prescribed form and manner ~~as soon as feasible~~ **without unreasonable delay, but no more than 7 calendar days,** after the organization **becomes aware of the breach** ~~determines that the breach has occurred~~.

and that subsection 58(6) of the CPPA (Consumer Privacy Protection Act) be amended as:

> The notification must be given ~~as soon as feasible~~ **without unreasonable delay** after the organization determines that the breach has occurred.

Domestic service providers

We have previously discussed the issue of trans-border data flows with a series of recommendations outlined at Annex B (#toc5).

The use of service providers within Canada does not raise the same risks as does the use of overseas service providers. Among other things, it can be safely assumed that the domestic service provider is subject to legislation that provides equivalent protection to the CPPA (Consumer Privacy Protection Act) (either the CPPA (Consumer Privacy Protection Act) itself, or a substantially similar provincial legislation, or both). However, this does not mean that no consideration needs to be given to this situation. At a minimum, according to Dr. Scassa, the first two considerations still apply: to whom will the obligations apply, and in what circumstances? And, who is accountable for the personal data, and in what circumstances?

We believe the overall scheme provided by s. (section) 11 is reasonable (requiring that the transferring organization ensures by contract or otherwise that "substantially the same protection" as that required under the Act is provided). However, in certain areas additional details or amendments would be beneficial. For instance, references to information "transferred" for processing in s. (section) 11(2) are problematic in an environment where service providers are envisioned as potentially collecting personal information on behalf of an organization.

We also are concerned about the potential re-use of personal information by service providers under s. (section) 18(2)(e), given that (as a rule) service providers will not have a direct relationship with individuals. Considering the essentially unlimited nature of the activities that could be permitted under 18(2)(e), without either knowledge or

consent of the individual, we again reiterate our recommendation to delete this provision.

Given that the CPPA (Consumer Privacy Protection Act) does not distinguish between domestic and international service providers in its requirements, certain recommendations outlined at Annex B (#toc5) in the context of trans-border data flows apply equally to the domestic context. More specifically, recommendations 3, 4, 5 and 7 of Annex B (#toc5) also apply to domestic service providers.

Recommendation 26: That recommendations 3, 4, 5, and 7 of Annex B (#toc5) also be applied in the context of domestic service providers.

Individual rights

In examining the structure of privacy legislation, the complement to organizational obligations are individual rights. Just as organizations should know what is expected of them, individuals should have clarity with respect to both what rights they can exercise and how to do so. As with consent, this is a critical element of the pillar of ensuring individuals have a level of control over their personal information. Having examined consent above, here, we focus on other rights which are (or should be) provided under the CPPA (Consumer Privacy Protection Act).

Automated decision-making

As described in the introduction to this submission, it is clear that one of the objectives of this legislation is to enable the use of personal information for innovative purposes – and that in many cases, this will include the use of automated decision-making or artificial intelligence. The OPC (Office of the Privacy Commissioner of Canada) is supportive of this overall goal, so long as appropriate privacy protections are part of the legislative framework. This, again, is the lens through which we have viewed both the CPPA (Consumer Privacy Protection Act) as a whole, and its provisions related to automated decision-making.

AI (artificial intelligence) marks a transformative point in society, introducing novel ways in which personal information is processed. However, uses of AI (artificial intelligence) that are based on individuals' personal information can have serious consequences for their privacy.

AI (artificial intelligence) models have the capability to analyze, infer and predict aspects of individuals' behaviour, interests and even their emotions in striking ways. AI (artificial intelligence) systems can use such insights to make automated decisions about individuals, including whether they get a job offer, qualify for a loan, pay a higher insurance premium, or are suspected of suspicious or unlawful behaviour. Such decisions have a real impact on individuals' lives, and raise concerns about how they are reached, as well as issues of fairness, accuracy, bias, and discrimination. AI (artificial intelligence) systems can also be used to influence, micro-target, and "nudge" individuals' behaviour without their knowledge. Such practices can lead to troubling effects for society as a whole, particularly when used to influence democratic processes.

It is encouraging to see the CPPA (Consumer Privacy Protection Act) include specific provisions to address this important and growing form of processing, and the risks it presents. The CPPA (Consumer Privacy Protection Act) includes elements of the approach outlined in our AI (artificial intelligence) paper, such as defining automated decision-making (instead of AI (artificial intelligence)), and adopting a level of flexibility for using de-identified information.

The CPPA (Consumer Privacy Protection Act) also provides for the right to receive an explanation for automated decisions. However, we believe modifications are necessary to denote a clearer standard for such explanations, create a right to contest automated decisions, and strengthen accountability through privacy by design and algorithmic traceability. Our recommendations to this end align with the values-based OECD (Organisation for

Economic Co-operation and Development) AI (artificial intelligence) principles (https://www.oecd.org/going-digital/ai/principles/), which include respect for the rule of law, human rights, and safeguards such as human intervention to ensure fairness. We share the objective of ensuring that "people understand AI (artificial intelligence)-based outcomes and can challenge them", and that organizations are accountable for the use of AI (artificial intelligence).

Many of the recommendations in this submission relate directly to automated decision-making. For example, the need to include inferred information within the scope of personal information and the need to establish a requirement that organizations maintain adequate records to ensure compliance with the law. In the case of automated decision-making, this might include measures to ensure privacy is designed into systems such as PIAs (Privacy Impact Assessments) and/or algorithmic impact assessments (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/responsible-use-ai/algorithmic-impact-assessment.html) . In this section, we will not repeat analysis of those issues, but focus specifically on recommendations related to paragraph 62(2)(c) and s. (section) 63(3).

First, while we acknowledge the addition in s. (section) 63(3) of the CPPA (Consumer Privacy Protection Act) of a new right to an explanation in relation to automated decision-making, we recommend that amendments must be made to ensure the meaningfulness of that explanation.

The right to a meaningful explanation relates to existing principles for the protection of personal information, namely accuracy, openness, and individual access. This right, provided for in section 63(3) of the CPPA (Consumer Privacy Protection Act), should aim to allow individuals to understand decisions made about them and facilitate the exercise of other rights such as to correct erroneous personal information, including inferences. At least that is the goal of Article 15(1)(h) of the GDPR (General Data Protection Regulation), which requires data controllers to provide individuals with “meaningful information about the logic involved” in decisions.

However, the current obligation under section 63(3) does not provide consumers with the right to a meaningful explanation. It provides the right to know the prediction or decision, and the provenance of the information upon which this was based, but not the relationship between the personal information and the decision, nor even the elements of personal information relevant to the decision. Without the latter two elements, or at least the nature and elements of the decision to which they are being subject, or the rules that define the processing and the decision’s principal characteristics, the explanation cannot be meaningful.

The explanations concerning automated decisions must take into account organizations’ intellectual property and commercial secrets. On the other hand, it must also be remembered that one of the objectives of the right to an explanation is to address potential scenarios where black box algorithms and unknown personal information is used to automatically determine an individual’s fate. It provides an avenue of recourse and respects basic human dignity by ensuring that the organization is able to explain the reasoning for the decision in understandable terms. While in this context, trade secrets may limit the explanations provided, some form of meaningful explanation will always be possible without compromising intellectual property. While some (perhaps substantial) information may need to be omitted, an individual should not be denied their right to a meaningful explanation on the grounds of proprietary information or trade secrets.

In scenarios where trade secrets may prevent explanations from being provided using the standard described above, organizations could use the following three factors, based on suggestions made by the UK (United Kingdom) Information Commissioner’s Office (https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/automated-decision-making-and-profiling/what-else-do-we-need-to-consider-if-article-22-applies/) (ICO), to provide an adequate explanation:

- the type of information collected or used in creating the profile or making the automated decision;

- why the information is relevant; and
- what the likely impact is going to be.

Recommendation 27: That a standard for the level of explanation required under subsection 63(3) be enhanced to allow individuals to understand: (i) the nature of the decision they are subject to and the relevant personal information relied upon, and (ii) the rules that define the processing and the decision's principal characteristics.

Where trade secrets prevent such an explanation from being provided, that at least the following be disclosed: (i) the type of personal information collected or used, (ii) why the information is relevant, and (iii) its likely impact on the individual.

Additionally, individuals should be provided with a right to contest automated decisions. Technology is not perfect, and individuals should not be bound by automated decisions without a way to seek human intervention, particularly when such decisions can be based on inaccurate data, reflect bias, or otherwise result in a decision that a human would deem inappropriate. This right would apply both to those scenarios where an individual has provided consent for the processing of their personal information as well as those where an exception to consent was used by the organization. It serves as a complement to the right to explanation.

Such a right would be consistent with the approach taken in other jurisdictions, including Europe under the GDPR (General Data Protection Regulation) and Quebec under Bill 64, where a human could be required to take a second look at the decision upon request. The right to contest would be in addition to the ability to withdraw consent currently provided for in the CPPA (Consumer Privacy Protection Act). It is necessary to have both rights, as withdrawal of consent is an all-or-nothing decision, whereas contestation provides individuals with recourse even when they choose to continue to participate in the activity for which automated decision-making was employed.

Recommendation 28: That a right to contest automated decisions be included in the CPPA (Consumer Privacy Protection Act).

Right to reputation

In our 2018 Draft Position on Online Reputation (/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/pos_or_201801/), we set out our preliminary views on matters related to online reputation, including the right to be forgotten.

In this paper, we found that under certain circumstances, PIPEDA (Personal Information Protection and Electronic Documents Act) already provided for a right to de-indexing, stemming from the right that individuals have to challenge the accuracy or completeness of information about them, and to have that information amended (corrected or deleted). We also recognized that this is an important issue given the significant impacts that information posted online can have on individuals and the close connection of online reputation to other rights, such as freedom of expression. Because of the importance of the values and rights involved, we have recommended that elected Members of Parliament expressly study the question of de-indexing and the removal of information from online sources.

Certain of the issues raised in that paper have been addressed, in part, by the CPPA (Consumer Privacy Protection Act). For instance, the express ability for individuals to request the deletion of personal information provides more

certainty with respect to an individual's ability to obtain removal of information about them. However, it appears to be unnecessarily limited in scope, given subsection 55(1)'s reference only to information collected from the individual.

By way of example, this would mean that the ability to request deletion would likely not apply to information held by organizations such as data brokers, which would seldom (if ever) receive information directly from an individual. In fact, as in addition to the exception to consent under paragraph 18(2)(e), this measure would remove an additional privacy obligation from those organizations without a direct relationship to individuals.

To address this gap, we recommend that the right to deletion be expanded, to include any personal data concerning the individual, in line with the approach adopted in the GDPR (General Data Protection Regulation). We agree with the exceptions set out at paragraphs 55(1)(a) and (b) where organizations should be able to refuse a deletion request.

Recommendation 29: That section 55 be expanded to include *all* personal information held by an organization about the individual, subject to consideration of additional reasons for refusal.

However, of greater concern to us is to ensure that individuals have the ability to assert appropriate control over the information available about them online – to protect their online reputation.

Such protection is recognized internationally in both the Universal Declaration of Human Rights, and the International Covenant on Civil and Political Rights (ICCPR), of which Canada is a signatory. They provide that all persons have a right to be free from "arbitrary interference" with their privacy, and "unlawful attacks on [their] honour and reputation." [13](#fn13) While freedom from interference has traditionally been used to refer to protection from the state, the UN (United Nations) Human Rights Committee has said the ICCPR (International Covenant on Civil and Political Rights) requires states to protect individuals from acts committed by private persons or entities. [14](#fn14)

The right to request deletion found in section 55 only applies to information collected from the individual. As a result, the CPPA (Consumer Privacy Protection Act) provides no new solutions with respect to issues such as search engine de-indexing or the right for individuals to request deletion of harmful information posted by others. Our recent investigation concerning RateMDs (/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-002/), a website where reviews are posted about medical professionals, highlighted the shortcomings of PIPEDA (Personal Information Protection and Electronic Documents Act) in addressing such reputational issues, which continue to be reflected in the CPPA (Consumer Privacy Protection Act). It also does not address recommendations that the Office had made in this respect in 2018.

The matter of the existence or not of a right to de-indexing is currently before the courts as a matter of interpretation of the current law. However, we strongly believe that, because constitutional rights are at stake (the right to privacy and freedom of expression), and because they risk coming into conflict, Parliament should consider the question, arbitrate as necessary and enact the mechanisms and criteria that would be most fair and effective in enabling individuals to protect their reputation while preserving freedom of expression.

The approach taken by Quebec's Bill 64 may provide a useful model in this regard. In particular, proposed section 28.1 of the Bill sets out the following criteria for the de-indexing or removal of information from online sources, which we believe are reasonable:

1. the dissemination of the information causes the person concerned serious injury in relation to his right to the respect of his reputation or privacy;
2. the injury is clearly greater than the interest of the public in knowing the information or the interest of any person in expressing himself freely; and

3. the cessation of dissemination, re-indexation or de-indexation requested does not exceed what is necessary for preventing the perpetuation of the injury.

In assessing the criteria set out in the second paragraph, the following, in particular, must be taken into account:

a. the fact that the person concerned is a public figure;
b. the fact that the person concerned is a minor;
c. the fact that the information is up to date and accurate;
d. the sensitivity of the information;
e. the context in which the information is disseminated;
f. the time elapsed between the dissemination of the information and the request made under this section; and
g. where the information concerns a criminal or penal procedure, the obtaining of a pardon or the application of a restriction on the accessibility of records of the courts of justice.

Recommendation 30: That Parliament enact a clear and explicit right with respect to the de-indexing and/or removal of personal information from search results and other online sources, considering the OPC (Office of the Privacy Commissioner of Canada)'s recommendations in its 2018 Draft Position on Reputation and the approach proposed under Bill 64.

Data mobility

The data mobility provisions in C-11 provide individuals with a form of control over their personal information that is not present in PIPEDA (Personal Information Protection and Electronic Documents Act) – namely, the ability to require organizations to transfer some of their personal information to another organization, under certain circumstances. Overall, the OPC (Office of the Privacy Commissioner of Canada) supports the introduction of data mobility provisions in the CPPA (Consumer Privacy Protection Act); however, we recommend certain amendments to better align the Bill with international models.

First, it is notable that section 72 would only apply to information collected from an individual. As discussed previously with respect to a right to reputation, this may represent only a small subset of the overall information held about a person by an organization. To the extent to which this provision is intended to increase consumer control over their information, and promote consumer choice, it will be important to include all personal information about an individual, including that which is derived or inferred by the organization.

Similar to what is proposed in the CPPA (Consumer Privacy Protection Act), the Australian *Consumer Data Right Act* (CDR) sets out a process by which the government designates sectors which are subject to the CDR (Australian Consumer Data Right Act) Act (and thus required to transfer personal information to other organizations, at the request of the individual). It also creates the rules under which data is shared for each designated sector. Notably, this includes specifying the classes of information that must be shared between organizations within the sector, clarifying that derived information within each identified class is included.

Recommendation 31: That section 72 of the CPPA (Consumer Privacy Protection Act) be expanded to include all personal information about an individual, including derived or inferred information.

The Australian CDR (Australian Consumer Data Right Act) Act also sets out clear roles and responsibilities for the three government stakeholders involved in the development of data mobility frameworks – the relevant minister, the Australian Competition and Consumer Commission, and the OAIC (Office of the Australian Information

Commissioner). This includes explicit requirements for the Information Commissioner to be consulted on both the designation of, and design of rules for, sectors, as well as the ability to recommend sectors for designation. Under the CPPA (Consumer Privacy Protection Act), however, s. (section) 120 specifies that data mobility frameworks are to be established through regulations, without specifying any role in that process for the Privacy Commissioner. We believe that the OPC (Office of the Privacy Commissioner of Canada) should have a consultative, advisory, and/or approval role for data mobility frameworks. However, this can be done administratively and does not require amendment to the Act.

Recommendation 32: That a clear consultative, advisory or approval role be established for the OPC (Office of the Privacy Commissioner of Canada) with respect to data mobility frameworks.

Theme three: Quick and effective remedies and the role of the OPC (Office of the Privacy Commissioner of Canada)

The stated third pillar for Bill C-11 is a strong enforcement and oversight mechanism. Such a mechanism should include, in our view, access to quick and effective remedies for individuals, and should provide the regulator the legal tools required to fulfill its mandate to protect Canadians effectively, including the discretion to allocate its resources to areas of greatest impact and risk. We address each of these in turn.

Remedies

As mentioned in the Commissioner's foreword, we believe that due to the severe restrictions imposed on the monetary penalty regime and the addition of an administrative appeal tribunal between the OPC (Office of the Privacy Commissioner of Canada) and the courts, consumers would not have access to quick and effective remedies. We will come to these fundamental flaws later, but for now let us explain the procedural rules that would generally apply to investigations and inquiries.

Rules of procedure and evidence in investigations and inquiries and relevant to orders

Most of the CPPA (Consumer Privacy Protection Act)'s procedural rules regarding the conduct of investigations and inquiries are relatively straightforward. Despite this, we have a number of recommendations that we believe will enhance our effectiveness and the efficiency of investigations, inquiries and order making measures under the CPPA (Consumer Privacy Protection Act). Our recommendations are informed in part by our investigative experience under PIPEDA (Personal Information Protection and Electronic Documents Act) as well as consultations held with our provincial counterparts in Alberta and British Columbia, both of which have similar measures in their provincial statutes.

First, we suggest reducing the threshold by which the OPC (Office of the Privacy Commissioner of Canada) can compel evidence under s. (section) 98(1)(a). Currently, this provision requires that the evidence requested be "necessary" for the proceedings being conducted, while comparable legislation (as in Alberta and British Columbia), have no such threshold. We recommend replacing "necessary" with "relevant to the investigation, inquiry or audit." This would avoid unnecessary court proceedings that could cause delays. We also recommend this power be reframed as the power to order appearance or production of records, and to amend subsection 103(2) (and s. (section) 104 consequentially) to make orders under 98(1)(a) and 98(1)(e) enforceable in the same manner as an order of the Federal Court. This would avoid us having to go to court to apply for a new order if someone did not comply with our subpoenas. Again, this is to avoid unnecessary delays.

Next, interim orders under section 98(d) may often address time sensitive or urgent matters (for example, to prevent

the destruction of documents relevant to an investigation or to prevent a risk of harm to individuals). We therefore recommend that the appeal provisions at sections 103(2) and 104 relating to interim orders (and potentially to orders under ss. (sections) 98(1)(a) and (e) as suggested above) be considered for any necessary amendments to ensure that orders under section 98 are not unduly delayed or undermined pending any appeal. For example, the Act could confirm the legal obligation to comply with an urgent order, absent a stay sought by the organization pending any application for leave to appeal. Given the likely time sensitive nature of the issues involved, we recommend consideration also be given to shorter timeframes for requests for leave to appeal orders under section 98. For example, in *Canada's Anti-Spam Legislation*, reviews of preservation demands must be sought within five days of the demand (see sections 15 and 16).

As well, we recommend that s. (section) 98(1)(h) be amended to clarify that the records referred to in this provision are not limited to those physically located on the premises of the organization. We seek thus to avoid organizations arguing, as has already occurred, that records cannot be examined by the OPC (Office of the Privacy Commissioner of Canada) because the organization has stored them on an off-site server, for example, in the cloud.

Additionally, the OPC (Office of the Privacy Commissioner of Canada) recommends that, at least in the case of access complaints where privilege is being claimed, it be able to request and receive records protected by solicitor-client privilege in order to assess claims of statutory exemptions. It should be noted that similar powers are available under both the Alberta and British Columbia acts, as well as to the OPC (Office of the Privacy Commissioner of Canada) under the *Privacy Act*. A provision would clarify that the disclosure to the Commissioner of protected documents would not constitute a waiver of solicitor-client privilege.

Subsection 92(4) states that an investigation must be completed within one year, unless extended, which is also limited to one year. We recommend removing the limit provided for time extension, following the laws in force in Alberta and British Columbia. While the OPC (Office of the Privacy Commissioner of Canada) strives to resolve issues quickly (as evidenced by the fact that the majority of cases are closed without formal investigation) and we strongly believe that consumers are entitled to quick and effective remedies, delays beyond our control are sometimes caused by the parties. It would be unfair to the other party if an investigation could not be completed or had to be completed on the basis of an incomplete file because of a rule setting a peremptory maximum time limit.

Finally, in the context of order making, we recommend striking the phrase from section 92(2) which enacts that orders can only be taken “to the extent that it is reasonably necessary to ensure compliance with this Act.” This requirement of necessity does not exist in the comparable laws of Alberta, British Columbia and Quebec, nor is it included in the UK (United Kingdom)’s *Data Protection Act* 2018, New Zealand’s *Privacy Act* 2020, or Ireland’s *Data Protection Act 2018*. It risks giving rise to unnecessary court proceedings that would delay the conclusion of cases to the benefit of consumers.

Recommendation 33: That the following amendments be made with respect to the inquiries and investigations under the CPPA (Consumer Privacy Protection Act):

- 98(1)(a): Reduce the threshold by which the OPC (Office of the Privacy Commissioner of Canada) can compel the production of evidence, and rephrase this power as “order” rather than “compel”;
- 98(1)(h): Clarify that this provision also applies to information stored on remote servers, but accessible within the premises in question;
- 103(2): Make orders under 98(1)(a) and 98(1) enforceable in the same manner as an order of the court;
- 103(2) and 104: Appeal provisions relating to interim orders made pursuant to s. (section) 98(d) should be amended to ensure that such orders are not unduly delayed or undermined pending appeal;
- 90(2): Enact necessary amendment to allow the OPC (Office of the Privacy Commissioner of Canada) to request and receive information subject to solicitor-client privilege, for the purpose of assessing claims of statutory exemptions in the context of access-related complaints;
- 92(2): Strike the necessity test, which is not found in any comparable statute;

- 92(4): Remove the one-year maximum period for extensions to completion of an inquiry.

Special case of breaches – Access to full reparation for damages suffered

Order-making, like other enforcement mechanisms, is forward looking. Subsection 92(2) of the CPPA (Consumer Privacy Protection Act), for instance, sets out that the Commissioner can order an organization to take measures that comply with the Act or to stop doing something that is in contravention of the Act. This is normal, but creates challenges in defining an effective remedy when a breach has taken place. In such cases, compensation to victims for damages suffered may be necessary.

In the course of breach investigations, the OPC (Office of the Privacy Commissioner of Canada) will frequently engage in discussions with organizations with respect to offering remedial or mitigating measures following a breach. For instance, following a recent major breach, Desjardins (/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2020/pipeda-2020-005/) offered both risk mitigations (such as credit monitoring) as well as remediation, such as direct rehabilitation assistance (including access to lawyers and psychologists) and compensation for costs associated with identify theft. However, organizations will not always be willing to offer such measures.

We believe that in some cases, it would be reasonable and desirable for the OPC (Office of the Privacy Commissioner of Canada) to be able to order remedial or mitigating measures, as an exception to the general rule that enforcement actions should be forward looking.

Organizations derive significant commercial benefits from processing large volumes of personal information. However, where their security safeguards are deficient and lead to a breach, the consequences fall primarily on affected consumers. Other remedies are possible to compensate the individual, but we believe that in cases where the OPC (Office of the Privacy Commissioner of Canada) has investigated a breach and found a violation of the safeguards obligation, it would be efficient and fair that we have the authority to make an order that would provide consumers with reparations for damages suffered.

Recommendation 34: That a paragraph be added under section 92(2) which permits the OPC (Office of the Privacy Commissioner of Canada) to order an organization to “take measures which allow individuals to be compensated for damages suffered, financial or otherwise, stemming from a breach or violation of security safeguards required by law.”

Compliance agreements

The OPC (Office of the Privacy Commissioner of Canada) considers compliance agreements as an important means of efficiently resolving matters. As such, we are pleased that they remain available to us as an enforcement mechanism under the CPPA (Consumer Privacy Protection Act). However, we believe that their effectiveness could be improved through three principal amendments.

First, an amendment should be introduced to Bill C-11 to permit the resolution of inquiries with a compliance agreement. There is no reason why such agreements are no longer possible at this stage of the proceedings. It is in the interest of all - the parties to a complaints investigation, the OPC (Office of the Privacy Commissioner of Canada) and the courts - that cases can be resolved through a negotiated settlement at any point prior to the issuance of a compliance order or the recommendation of an administrative monetary penalty (AMP) to the Tribunal (under the current model of the CPPA (Consumer Privacy Protection Act)).

Second, we recommend that the OPC (Office of the Privacy Commissioner of Canada) be authorized to register compliance agreements with the Court, so that they take on the same force and effect as an order of the Court. Currently, the process established by C-11 for enforcing a contravened compliance agreement is complex (and likely lengthy), requiring the commencement and completion of an inquiry and issuance of a compliance order compelling the organization to comply with the agreement. Then, assuming it is not appealed, that compliance order can be filed with the Federal Court, at which point it would become a court order. We compare this to similar instruments such as the Commissioner of Competition's consent agreements or the US (United States) Federal Trade Commission's consent orders, both of which take on the same effect as a court order once registered or ratified by the courts.

Finally, we recommend that subsection 86(2) be amended to make it clear that compliance agreements can include the payment of AMPs (administrative monetary penalties) and other measures of compliance, whether or not they may be imposed by the Commissioner or the court. This recommendation is modeled on subsection 74.12(2) of the *Competition Act*, which states that the consent agreement referred to in that Act "shall be based on terms that could be the subject of a court order against that person, and ***may include other terms, whether or not they could be imposed by the court***" (emphasis added). We are advised that this provision has helped consent agreements become a cornerstone of the Commissioner of Competition's compliance program aimed at combatting misleading advertising. The predictability and certainty inherent in the consent agreements have enabled the Commissioner to negotiate settlements that are very effective for compliance purposes and therefore very beneficial to consumers. Similar tools may be used by our counterparts at the CRTC (Canadian Radio-television and Telecommunications Commission), the U.S. (United States) FTC (Federal Trade Commission) and in the United Kingdom.

Recommendation 35: That the CPPA (Consumer Privacy Protection Act) be amended, with respect to compliance agreements, to permit:

- The resolution of inquiries through compliance agreements;
- The registration of compliance agreements with the court, making them equivalent to an order of the court; and,
- The addition of the payment of AMPs (administrative monetary penalties) and all other negotiated measures as possible terms within compliance agreements.

The Personal Information and Data Protection Tribunal

Bill C-11 creates a check and balance for the OPC (Office of the Privacy Commissioner of Canada) in the form of the Personal Information and Data Protection Tribunal. According to the Government, this is meant to both ensure fairness to organizations and access to quick and effective remedies for consumers.

While the OPC (Office of the Privacy Commissioner of Canada) welcomes oversight and accountability for our actions, we respectfully suggest that the new Tribunal is both unnecessary to achieve greater accountability and fairness (the Federal Court already plays this role), and counter-productive in achieving quick and effective remedies. In fact, all objective indicators show overwhelmingly that the Tribunal would unnecessarily delay justice for consumers.

In his foreword, the Commissioner outlines the main reasons why the creation of such a structure between the OPC (Office of the Privacy Commissioner of Canada) and the courts is not a good idea. In summary, there is no need to add an administrative appeal to ensure fairness to business when the Federal Court already plays this role, and as, at any rate, the OPC (Office of the Privacy Commissioner of Canada) has an exemplary record in this regard. Moreover, adding a level of appeal can only delay the ultimate resolution of cases.

Why create a real delay to solve a theoretical but non-existent problem of fairness?

The central issue in this design is as follows. In order to enhance consumer confidence, we believe that the decision-making system for adjudicating complaints should be as fast and efficient as possible. In order for individuals to have confidence, they would expect there to be real and timely consequences when the law is violated. Of course, the system must also be fair to businesses. Over a 40-year period, the OPC (Office of the Privacy Commissioner of Canada)'s performance in this regard has been excellent, and we welcome making our procedures more transparent and consulting on ways to enhance them. We are also prepared, should Parliament grant us the power to impose monetary penalties, to have to take into account any relevant factors, beyond those set out in subsection 94(5), that Parliament may choose to enact.

In our opinion, the design of the decision-making system proposed in the CPPA (Consumer Privacy Protection Act) goes in the wrong direction. By adding an administrative appeals Tribunal and reserving the power to impose monetary penalties at that level, the CPPA (Consumer Privacy Protection Act) encourages organizations to use the appeal process rather than seek common ground with the OPC (Office of the Privacy Commissioner of Canada) when it is about to render an unfavorable decision. While the drafters of the legislation wanted to have informal resolution of cases, they removed an important persuasive tool from the OPC (Office of the Privacy Commissioner of Canada). Moreover, this design is outside the norm when compared with other jurisdictions.

Given these considerations, our primary and strong recommendation is to remove the provisions relating to Personal Information and Data Protection Tribunal from Bill C-11. Should Parliament disagree with this approach, as an alternative we would recommend that the Tribunal's composition be strengthened and that appeals from its decisions go directly to the Federal Court of Appeal.

We have identified several federal tribunals whose enabling statutes explicitly require tribunal members to have expertise or experience in their field. For example, the Canadian Agricultural Review Tribunal; the Canada Industrial Relations Board; the Federal Public Sector Labour Relations and Employment Board; the Canadian Human Rights Tribunal ("Persons appointed as members of the Tribunal must have experience, expertise and interest in, and sensitivity to, human rights"); and the Transportation Appeal Tribunal of Canada ("The Governor in Council shall appoint as members of the Tribunal persons who, in the opinion of the Governor in Council, collectively have expertise in the transportation sectors in respect of which the federal government has jurisdiction").

In order to reduce the delays in obtaining a final judgment, judicial reviews of decisions of the Tribunal could be performed by the Federal Court of Appeal, rather than the Federal Court. This would compensate for the delays caused by the added layer of the Tribunal. Based on existing precedents, some Tribunal members would be required to have experience as a judge. Five of the tribunals listed in s. (section) 28 of the *Federal Courts Act* are required by statute to be composed of judges, either sitting or retired, including the Copyright Board, the Public Servants Disclosure Protection Tribunal, the Assessors under the *Canada Deposit Insurance Corporation Act*, the Specific Claims Tribunal, and the Competition Tribunal.

Of the tribunals listed, the Competition Tribunal is procedurally the most similar to the Tribunal – for example, it does not investigate complaints; rather it hears applications from the Commissioner of Competition or, with leave, by private parties under the civil reviewable matters sections of the *Competition Act*. It is also made up of a maximum of six federal court judges and a maximum of eight lay people. This is a model that could be emulated under Bill C-11 to increase efficiencies.

Given the above, we would recommend – if the Tribunal is maintained – and based on the precedents cited, that it be composed of a majority of judges, either sitting or retired, with lay members who "collectively have experience" in privacy. Members who have other backgrounds and expertise could, of course, be appointed, including in the areas of business or of consumer protection, however there would be greater numbers of members with an expertise in law or privacy.

Recommendation 36: We strongly recommend that the Personal Information and Data Protection Tribunal not

be created and that the Privacy Commissioner be granted the authority to impose administrative monetary penalties at the conclusion of inquiries. If the Tribunal is created, we recommend in the alternative that its composition be amended to include a majority of judges, either sitting or retired, with lay members who "collectively have experience" in privacy.

Should it remain in place, we would also raise the issue of the OPC (Office of the Privacy Commissioner of Canada)'s standing before the tribunal. Currently, PIPEDA (Personal Information Protection and Electronic Documents Act), the *Privacy Act*, and the *Access to Information Act* each contain provisions that grant the OPC (Office of the Privacy Commissioner of Canada) standing before the Federal Court. Under the CPPA (Consumer Privacy Protection Act), though, the OPC (Office of the Privacy Commissioner of Canada)'s standing before the Tribunal can at best be inferred from section 94(1)(b), which is limited to situations where the OPC (Office of the Privacy Commissioner of Canada) has recommended a penalty be imposed.

This is potentially problematic, as without standing the OPC (Office of the Privacy Commissioner of Canada) would be unable to make submissions in appeals of its orders or bring judicial review applications of decisions of the Tribunal, where appropriate. One of our concerns, among others, in such a situation is that it could exacerbate access to justice issues for complainants, who may not have the means or capacity to contest appeals brought by organizations or to seek redress where the tribunal has committed a reviewable error. Several federal statutes provide express standing rights before courts and tribunals in similar circumstances. In addition to those cited above, we note that the Canadian Human Rights Commission has the express right to participate in proceedings before the Canadian Human Rights Tribunal.

Recommendation 37: That, should the tribunal remain in place, the CPPA (Consumer Privacy Protection Act) be amended to explicitly grant the OPC (Office of the Privacy Commissioner of Canada) standing before the tribunal.

Administrative monetary penalties (AMPs)

Section 93(1) of the CPPA (Consumer Privacy Protection Act) specifies that, in completing an inquiry, if the Commissioner finds an organization has contravened one or more of a narrow list of enumerated provisions, the Commissioner must decide whether to recommend to the Tribunal that a penalty be imposed. It is not evident why the recommendation of a penalty is limited to such a narrow list of contraventions. This list does not include obligations related to the form of consent, nor the numerous exceptions to consent. It also does not include violations of the accountability provisions. In our view, this makes the proposed AMP (administrative monetary penalty) regime completely ineffective.

Our research – which examined the AMP (administrative monetary penalty) regimes in the United Kingdom, Australia, Singapore, Quebec (under Bill 64), Ontario (under the *Personal Health Information Protection Act*), and California – found that this is an unusual approach as compared to these other jurisdictions, in which the recent legislative trend has been to give data protection authorities the ability to issue AMPs (administrative monetary penalties) for almost any violation connected to the collection, use or disclosure of personal information. We have found no other instance in which only violations of such a narrow list of legal requirements are subject to penalties.

We have also found no specific legal impediment that would prevent a more expansive range of contraventions to be added under s. (section) 93(1). In particular, we do not believe that the "doctrine of vagueness" – which may render a law or legislative provision unconstitutional if it is too vague – would apply here. If a provision is sufficiently precise to be constitutionally valid, we would argue that it is sufficiently precise to allow for an AMP (administrative monetary

penalty) to be imposed on an organization that contravenes it.

Similarly, there is no limitation to the range of provisions for which the Commissioner may issue a compliance order under subsection 92(2). As we understand it, the government intends financial penalties to be possible for violations other than those listed in s. (section) 93(1), but through the following very circuitous route.

First, an investigation would be conducted by the OPC (Office of the Privacy Commissioner of Canada) and then, in order to produce an order, an inquiry. Then an appeal to the new Tribunal. Some organizations would then bring the matter to the Federal Court. Assuming the OPC (Office of the Privacy Commissioner of Canada) order is upheld, the organization would then be given some time to comply. Only in the case of non-compliance with an OPC (Office of the Privacy Commissioner of Canada) order would a criminal process be commenced potentially leading to a fine. This process would involve the preparation of evidence by the OPC (Office of the Privacy Commissioner of Canada) or some other investigative body. The evidence would then be forwarded to the Public Prosecution Service of Canada, which would analyze it to determine whether a prosecution would be in the public interest. Then a criminal trial would take place, and a fine potentially imposed at its conclusion.

As illustrated in Figure 1 of Annex C (#toc6), we estimate that this process would take approximately seven and a half years. If the OPC (Office of the Privacy Commissioner of Canada) was authorized to impose AMPs (administrative monetary penalties) and there was no administrative appeal to the Tribunal, but instead there was judicial review, the process would take approximately three and a half years (see Figure 3 of Annex C (#toc6)). If, as previously recommended, the OPC (Office of the Privacy Commissioner of Canada) was authorized to reach a compliance agreement with AMPs (administrative monetary penalties), there would be no judicial review, since the penalty would be the result of a mutual agreement, and the process would take approximately two years (per Figure 2 of Annex C (#toc6)).

The UK (United Kingdom) *Data Protection Act* includes an interesting solution to the potential concern that penalties might be imposed for violations of “vague” provisions. There, the AMP (administrative monetary penalty) scheme includes an optional two-step process. Where the UK (United Kingdom) Information Commissioner is “satisfied that a person has failed” (that is, that a violation has occurred), they may immediately issue a “payment notice,” requiring payment of a specified amount (s. (section) 155). However, the Commissioner can also issue an “enforcement notice” which requires that an organization either takes, or refrains from taking, steps set out in the notice (s. (section) 149). Failure to meet the conditions of the enforcement notice could then lead to the issuance of a payment notice. In the context of the CPPA (Consumer Privacy Protection Act), a scheme such as this would allow for the potential that, where requirements for compliance with a particular provision may be considered “vague,” the Commissioner would be empowered to first issue a notice that clarifies compliance requirements, followed by an AMP (administrative monetary penalty) if these clarified requirements are not met.

Recommendation 38: That subsection 93(1) of the CPPA (Consumer Privacy Protection Act) be amended to make the range of violations for which AMPs (administrative monetary penalties) may be imposed much broader, potentially encompassing all violations under Part 1 of the CPPA (Consumer Privacy Protection Act).

The CPPA (Consumer Privacy Protection Act) should also be amended to include provisions similar to the UK (United Kingdom) *Data Protection Act* whereby, when appropriate, the Commissioner could give an organization an enforcement notice, clarifying the nature of a violation, before proceeding to the recommendation or the imposition of a penalty.

Of course, for transparency, we are open to having criteria that would guide us and which we would need to take into consideration before recommending an AMP. This has been partially accomplished by subsection 93(2), though we would recommend the following amendments to that section:

- Given that (per subsection 94(6)) an AMP (administrative monetary penalty) is not meant to be punitive, but to promote compliance with the legislation, it is unclear why 93(2)(b) – whether the organization has voluntarily paid compensation – would be an applicable factor.
- It is challenging to assess an organization's history of compliance with the Act. We suggest that 93(2)(c) should be re-phrased as "history of non-compliance."
- It is unclear why the Tribunal would consider additional factors (per subsection 94(5)) in determining the amount of a penalty beyond those considered by the Commissioner in recommending an AMP. As the OPC (Office of the Privacy Commissioner of Canada) is not precluded from considering these factors, we see no reason why they should not be expressly added to the list under subsection 93(2), all the more so since the OPC (Office of the Privacy Commissioner of Canada) will be called upon to make its recommendations to the Tribunal.

Recommendation 39: That section 93(2) be amended by:

- Removing paragraph 93(2)(b);
- Rephrasing paragraph 93(2)(c) to focus on history of *non*-compliance; and
- Incorporating paragraphs 94(5)(b) and (c).

Lastly, we are unclear about the purpose of subsection 93(3), which (in short) prohibits the OPC (Office of the Privacy Commissioner of Canada) from recommending a penalty in the case that an organization is in compliance with the requirements of an approved certification program.

Under section 76(2), an approved code of practice would provide for "substantially the same or greater protection of personal information" as some or all of the CPPA (Consumer Privacy Protection Act). On the other hand, by definition a penalty would only be recommended when a violation of the CPPA (Consumer Privacy Protection Act) has occurred. Thus, subsection 93(3) would seem to contemplate situations in which an organization simultaneously met the requirements of the Act (by compliance with an approved code) and did not meet the requirements of the Act (and was thus potentially subject to a penalty).

Subsection 93(3) therefore seems to contemplate that, in at least some scenarios, an organization's compliance with an approved code would not be sufficient for compliance with the CPPA (Consumer Privacy Protection Act). In our opinion, such scenarios would be unacceptable – a code of practice should be intended to provide organizations with clarity on how to comply with the Act, not to establish a lesser compliance standard.

Recommendation 40: That subsection 93(3) be removed from the CPPA (Consumer Privacy Protection Act).

Private right of action

One of the OPC (Office of the Privacy Commissioner of Canada)'s roles is to offer a relatively quick and inexpensive remedy to individual consumers who file complaints alleging violations of the Act. On the other hand, it is not our only role and, as noted, in order to be an effective regulator, we must be able to be strategic in our enforcement and advisory activities, applying a risk-based approach. Because our resources are not unlimited, we cannot be the only gateway to all consumer remedies. Where we cannot do so, consumers need to have access to the courts.

The recommendation to supplement the discretion not to investigate certain complaints with a private right of action (PRA) is consistent with the procedure in several countries. For example, several jurisdictions, including the U.K. (United Kingdom), the EU (European Union) and California, allow consumers to exercise a PRA (private right of

action) in privacy matters. As well, during consultations on Australia's *Privacy Act*, the Australian Information Commissioner's Office recently made a recommendation similar to our position.

While the introduction of a PRA (private right of action) in the CPPA (Consumer Privacy Protection Act) is a positive step, we are of the view that this measure is too restrictive, in that the right would only apply in cases where the OPC (Office of the Privacy Commissioner of Canada) has made a final finding of a contravention of the CPPA (Consumer Privacy Protection Act), which could take several years in the event of an appeal.

Furthermore, a PRA (private right of action) as framed in the CPPA (Consumer Privacy Protection Act) would likely increase the number of complaints filed with the OPC (Office of the Privacy Commissioner of Canada) since a final decision from us would be the gateway to access this right. Complainants may also be more likely to seek judicial review of findings that are not in their favour. This would result in us having to defend ourselves in court rather than focusing on compliance or advisory work.

To avoid these unfortunate consequences, we recommend the adoption of a scheme similar to that found in the *Official Languages Act* (OLA). Section 77 of the OLA (Official Languages Act) provides for recourse to the Federal Court, which may grant an appropriate remedy in three circumstances, after a person has made a complaint to the Commissioner:

1. Where the complainant has received the results of an investigation.
2. Where the complainant has been informed of the Commissioner's decision to refuse or cease to investigate the complaint.
3. Where he or she has not been informed of the result of the investigation or of a decision within six months after the complaint is made.

In 2015, the Federal Court affirmed (https://www.clo-ocol.gc.ca/en/language-rights/court-decisions/dionne-v-canada) the Commissioner of Official Language's position that Parliament's intention for this section was to "give complainants the right to go to court to obtain a fair and just remedy after the Commissioner has had the opportunity to resolve the complaint".

This scheme could be considered a middle ground between an unrestricted PRA (private right of action), as exists in other jurisdictions, and the highly constrained PRA (private right of action) currently proposed in the CPPA (Consumer Privacy Protection Act). A PRA (private right of action) still dependent on a complaint to the Commissioner, but not on the finding of a violation of the Act would provide a greater number of individuals the ability to pursue a civil action under the Act. At the same time, it would allow the OPC (Office of the Privacy Commissioner of Canada) to maintain discretion over allocation of its resources, exercise its powers under sections 83 (refusal to investigate), 85 (discontinuance of an investigation), 86 (entering into a compliance agreement), and 88 (discretion not to conduct an inquiry) without restricting individuals' access to justice.

Recommendation 41: That section 106 of the CPPA (Consumer Privacy Protection Act) be amended to expand the private right of action, by replacing paragraphs 106(1)(a) and 106(1)(b) with requirements similar to section 77 of the *Official Languages Act*.

Role of the regulator

In addition to maintaining all existing functions, Bill C-11 imposes several new mandatory responsibilities on the OPC (Office of the Privacy Commissioner of Canada), including the obligation to review codes of practice and certification programs and to provide advice to individual organizations on their privacy management programs. We welcome new opportunities to work with businesses to help ensure their activities comply with the law. This is consistent with our philosophy that the preferred strategy of an effective regulator is to assist entities in complying with the law, rather

than moving too quickly to using enforcement powers. However, adding new responsibilities of this nature to an already overflowing plate means the OPC (Office of the Privacy Commissioner of Canada) would not be able to prioritize its activities, based on its expert knowledge of evolving privacy risks, to focus on what is likely most harmful to consumers.

No regulator has enough resources to handle all the requests it receives from citizens and regulated entities. Adding new non-discretionary responsibilities for the OPC (Office of the Privacy Commissioner of Canada) risks exhausting our finite resources, leaving no room for us to pursue discretionary activities to address activities of high risk to Canadians. While these new responsibilities will obviously have to be appropriately resourced, the OPC (Office of the Privacy Commissioner of Canada) should have the legal discretion to manage our caseload, and to respond to requests from organizations and complaints from consumers in the most effective and efficient way possible. We should also have the ability to reserve a portion of our time for activities we choose to initiate, based on our assessment of risks for Canadians.

In this section, we make a number of recommendations that would help to ensure the OPC (Office of the Privacy Commissioner of Canada) can be responsive to requests from complainants and organizations, to the extent our resources allow, as well as an effective regulator for all Canadians.

Discretion to investigate

Over the past number of years, the Office has often raised issues with the inability of PIPEDA (Personal Information Protection and Electronic Documents Act)'s complaints-based model to effectively address privacy issues on its own, given the complex and opaque business processes and data flows that characterize the modern economy. Individuals are unlikely to file complaints about activities of which they are unaware. In this light, it is essential that a regulator be able to act proactively, including having the ability to rely on its expertise with respect to business practices to target enforcement actions against those activities that pose the highest risk and inflict the greatest harm to the privacy rights of individuals.

To be an effective regulator, providing protection to the maximum number of people from the greatest harms, the OPC (Office of the Privacy Commissioner of Canada) must be strategic in its enforcement and advisory activities, applying a risk-based approach. Unfortunately, the CPPA (Consumer Privacy Protection Act) provides no such discretion to the OPC (Office of the Privacy Commissioner of Canada) that would allow it to manage its workload to this end. The Bill's non-discretionary approach means that the OPC (Office of the Privacy Commissioner of Canada)'s limited capacity would likely be fully occupied investigating complaints by consumers, giving advice to individual organizations on their privacy management programs, and approving codes of practice – all activities that the Commissioner would have the obligation to undertake on demand. The Commissioner should be able to leverage the expertise and knowledge of employees and have the ability to invest a portion of resources to matters identified as priorities to undertake, including proactive inspections and the development of public guidance to promote compliance.

The CPPA (Consumer Privacy Protection Act) does not generally align with other jurisdictions in respect of discretion to investigate complaints. For instance, the Alberta PIPA (Personal Information Protection Act) (s. (section) 36), British Columbia FIPPA (Freedom of Information and Protection of Privacy Act) (s. (section) 42) and PIPA (Personal Information Protection Act) (s. (section) 36) all specify that the Commissioner "may" investigate complaints rather than "shall" or "must." As well, the New Zealand *Privacy Act* requires that the Commissioner "consider" all complaints and decide on the appropriate course of action (including investigating it, not investigating it, referring it to another authority, or exploring the possibility of a settlement).

Aside from the manner in which the duty to investigate is characterized, most statutes also include a provision for declining and/or discontinuing, which may have narrow or broad grounds. Examples of statutes that contains broad grounds include:

- Alberta PIPA (Personal Information Protection Act)'s paragraph 49.1(1)(b): "the circumstances warrant refusing

to conduct or to continue an investigation or review."
- New Zealand *Privacy Act*'s subsection 74(2), "the Commissioner may … decide not to investigate a complaint if it appears … that, having regard to all the circumstances of the case, an investigation is unnecessary."
- Australia *Privacy Act* paragraph 41(1)(da), "the Commissioner is satisfied that an investigation, or further investigation, of the act or practice is not warranted having regard to all the circumstances."

As discussed, in order to ensure the OPC (Office of the Privacy Commissioner of Canada) uses its resources as efficiently and effectively as possible, we propose that the CPPA (Consumer Privacy Protection Act) be amended to provide discretion:

- to address matters with the means we deem best and most effective in the circumstances,
- to allocate resources to the matters of greatest impact on Canadians, and
- to provide explicit discretion as to the procedure to be followed in the conduct of investigations as is the case for inquiries.

Thus, taking the above-described precedents into account, we would recommend the following scheme to amend and merge the current sections 83, 84 and 85:

83(1) The Commissioner may attempt to resolve a complaint by means of a dispute resolution mechanism such as mediation and conciliation.
(2) Where dispute resolution would not be appropriate or is unsuccessful, the Commissioner may conduct an investigation into all such matters as the Commissioner considers necessary to decide questions of fact and law arising from the complaint.
(3) The Commissioner may, in the Commissioner's discretion, decide not to investigate a complaint or to discontinue investigation of a complaint if the Commissioner is of the opinion that:
(a – d) [Current text of paragraphs 83(1)(a-d)]
(e - j) [Current text of paragraphs 85(1)(a-e, h)
(k) having regard to all the circumstances of the case, conducting or continuing an investigation is not warranted.
(4 – 5) [Current text of subsections 83(3) and 83(4).

Recommendation 42: That sections 83 to 85 of the CPPA (Consumer Privacy Protection Act) be amended to provide the Commissioner greater discretion with respect to the conduct of investigations under the Act.

Advice to organizations on their privacy management programs

Subsection 109(e) would require the OPC (Office of the Privacy Commissioner of Canada), on request by an organization, to provide advice on its privacy management program. We expect that seeking advice on privacy management programs will be very popular, since it would give organizations relative certainty that their programs comply with the Act. There are significant advantages to this activity, both for organization and consumers, but we are concerned it may overwhelm our limited resources.

We recommend that the OPC (Office of the Privacy Commissioner of Canada) be authorized, but not required, to provide advice to organizations that may make these requests. This is essentially the model we created a few years ago with our new Business Advisory Directorate.

Recommendation 43: That s. (section) 109(e) of the CPPA (Consumer Privacy Protection Act) be amended so that the Commissioner is authorized, but not required, to give advice to organizations, on request, in relation to their privacy management programs.

Codes of practice and certification programs

Codes of practice are an excellent means of bringing the Act's privacy principles to a more concrete level, adding certainty for both organizations and consumers. Overall, we are supportive of their inclusion in the CPPA (Consumer Privacy Protection Act), though we have a number of concerns about the potential impact of the proposed approach on our resources.

We are seeking greater discretion in relation to investigations and advice to individual organizations on their privacy management programs. We would not find it desirable, nor do we think the government would find it acceptable, that we have the discretion to refuse, as exceeding our capacity, an application by an industry sector or other entity for approval of a code of practice or certification program. Contrary to investigations and advice, which primarily concern individual consumers or organizations, codes of practice and certification programs are of a more general application, potentially affecting millions of Canadians.

For these reasons, we are of the opinion that the approval of codes of practice and certification programs should include an element of cost recovery. The approval process for codes and certification programs would most directly benefit the particular entities and their members, likely industry sectors, suggesting this approach would be reasonable. In fact, entities would likely see the payment of a small service fee as an investment in the certainty that the regulator would approve a code or program as providing for "substantially the same or greater protection" than the CPPA (Consumer Privacy Protection Act) (s. (section) 76(3)). For the OPC (Office of the Privacy Commissioner of Canada), cost recovery would ensure we would have the capacity both to review codes and certification programs, and other priorities that might otherwise be displaced by the mandatory nature of the approval process.

While we anticipate that, in general, applications for codes would be brought by industry associations, a cost recovery model should be designed in such a way so as to not discourage application by groups such as not-for-profits. This might be achieved, for instance, by providing the OPC (Office of the Privacy Commissioner of Canada) the flexibility to reduce or waive the fee.

Thus, we recommend an amendment to the CPPA (Consumer Privacy Protection Act) which would read: "Prior to examination of a code of practice or certification program by the OPC (Office of the Privacy Commissioner of Canada), the applicant shall pay such fees as may be prescribed."

Recommendation 44: That the Commissioner's obligation to review an application for approval of a code of practice or certification program be conditional on the payment of a cost recovery fee.

As mentioned, the CPPA (Consumer Privacy Protection Act) imposes a number of checks and balances on the OPC (Office of the Privacy Commissioner of Canada), including in relation to codes of practice and certification programs.

We have reviewed provisions related to codes in recently updated privacy legislation, such as the EU (European Union) GDPR (General Data Protection Regulation) and New Zealand's *Privacy Act* 2020. This review showed that while the scheme proposed in the CPPA (Consumer Privacy Protection Act) has similarities to its international counterparts, there are also a number of dissimilarities, generally relating to the lack of flexibility provided to the regulator with respect to procedures for approving codes and certification programs. Rather than allowing the OPC

(Office of the Privacy Commissioner of Canada) to set procedures, timelines and application criteria for implementing the general standard set out in the law, the Bill provides that almost all aspects of the codes and certification regime will be prescribed by regulations. In reviewing other models, we found that it is unusual for a regulator's role and required procedures with respect to the approval of codes to be specified in regulations in this fashion. No other comparable regime we examined provides for such lack of deference to the regulator.

We find it absolutely appropriate, of course, that the approval of codes and certification programs be subject to objective standards, prescribed at a certain level of generality, such as those set out at ss. (sections) 76(2) and 77(1) of the CPPA (Consumer Privacy Protection Act). Once these general standards are set, however, we believe that an appropriate way to proceed would be, as in the countries mentioned, to let the regulator define the procedures and detailed rules for how the law should apply.

The OPC (Office of the Privacy Commissioner of Canada), as the federal privacy regulator in Canada, has a very challenging role, enforcing the law and promoting compliance with the law in a digital economy that evolves at lightning speed. We are up to the task, but we need Parliament to give us the tools, including the legal tools, to manage our workloads and processes, define our priorities according to our assessment of risks, and carry out our mandate and responsibilities in the most efficient and effective ways possible. The imposition of detailed procedural rules through regulations, and consequently the removal of our discretion to define the processes we will adopt to fulfil our legal mandate, are unhelpful. We recommend that the CPPA (Consumer Privacy Protection Act) provisions on codes of practice and certification programs give the OPC (Office of the Privacy Commissioner of Canada) the same discretion as our colleagues internationally, to define and apply fair procedures for the application of the general standards found in ss. (sections) 76(2) and 77(1) of the Act.

Recommendation 45: That all references to regulations in sections 76, 77, 78, 81 and 122 (a)-(j) of the CPPA (Consumer Privacy Protection Act) be removed, leaving to the Commissioner the authority, as is the norm in other jurisdictions, to adopt fair procedures to approve codes of practice and certification programs pursuant to the standards found at subsections 76(2) and 77(1) of the Act.

Section 108

Section 108 of the CPPA (Consumer Privacy Protection Act) outlines that the Commissioner must, in the exercise of his powers and the performance of his duties and functions under the Act, take into account the size and revenue of organizations, the volume and sensitivity of the personal information under their control and matters of general public interest.

We understand the objective of this section since, in our application of the current law, PIPEDA (Personal Information Protection and Electronic Documents Act), we always carefully consider the realities and circumstances of organizations, including SMEs (small and medium enterprises), a subset of organizations for which section 108 seems tailor-made.

However, the mandatory and broad nature of section 108 as currently drafted could create challenges in its implementation. In particular, section 108 would appear to require the OPC (Office of the Privacy Commissioner of Canada) to consider the factors noted in any exercise of powers and the performance of all of its duties and functions under the Act. We are concerned that this may lead to unnecessary litigation, not only as to how the OPC (Office of the Privacy Commissioner of Canada) interpreted the law in a given situation and whether it gave due consideration to the context, including the size of the organization, but also as to whether it was appropriate to take action against an organization on the basis of the same factors. We could be prevented from acting, or our procedures delayed on frivolous grounds, for example, because we did not give due consideration to the context.

Due to these concerns, we recommend that s. (section) 108 be limited to encouraging the Commissioner to consider

the same factors.

Alternatively, a new section could be added after s. (section) 5 of the CPPA (Consumer Privacy Protection Act), stipulating that a purpose of the Act is that it applies contextually, including with regard to the factors mentioned in s. (section) 108. Including these factors in a purpose clause would be helpful in its interpretation but would not expose the OPC (Office of the Privacy Commissioner of Canada) to litigation that would seek to prevent us from acting.

Note that our Recommendation 21 takes into account the size of organizations in the application of accountability and record-keeping obligations.

Recommendation 46: That section 108 of the CPPA (Consumer Privacy Protection Act) be amended to encourage the Commissioner, in the exercise of his powers and duties, to consider the size of the organization and other factors mentioned. Alternatively, include these factors in a purpose clause.

Subsection 82(2) – Demonstrable accountability and proactive inspections

In the second part of this submission, we spoke to the importance of demonstrable accountability.

To reiterate, proactive audits and investigations, without grounds of a violation of the Act, are essential components of the concept of demonstrable accountability, which itself is an increasingly important element of modern privacy laws in an era where technologies and business models are complex, and where organizations seek greater authority to process personal information without consent. Consumers need to know that the regulator will “have their back” and ensure that they can safely participate in the digital economy without fear that their rights will be violated. Review of policies alone is not sufficient to achieve this. Consumers must also know that the regulator has the ability to meaningfully scrutinize personal information handling practices, including proactively.

Section 10 of the CPPA (Consumer Privacy Protection Act) goes some way towards achieving these goals, by requiring organizations – on request of the Commissioner – to provide access to the policies, practices, and procedures included in their privacy management program. However, s. (section) 110 negates the effect of s. (section) 10 by prohibiting the Commissioner from using that information as grounds to initiate a complaint, or to carry out an audit. Further, the grounds for initiating a complaint or audit (pursuant to subsection 82(2) and s. (section) 96, respectively) are more stringent than commonly seen in other jurisdictions.

To promote demonstrable accountability, and properly empower the OPC (Office of the Privacy Commissioner of Canada) to proactively verify compliance, we recommend amendments to subsection 82(2), s. (section) 96, and s. (section) 110, which will be discussed in turn in the following sections.

We strongly recommend that the OPC (Office of the Privacy Commissioner of Canada) be granted the authority to proactively initiate complaints to “ensure compliance” with the law rather than s. (section) 82(2)’s current “if…there are reasonable grounds to investigate a matter”. This is the threshold set out in, for instance, s. (section) 36(1)(a) of the Alberta *Personal Information Protection Act*. S. (Section) 81 of Quebec’s private-sector privacy law similarly allows the Commissioner to investigate, on his or her own initiative, “any matter relating to the protection of personal information”. Legislation in common law countries such as the United Kingdom, Ireland, and Australia contain similar thresholds.

As is the case with our colleagues in other jurisdictions, this would not lead to the arbitrary exercise of powers. Rather, it would permit the OPC (Office of the Privacy Commissioner of Canada) to undertake an assessment of the risks of a practice for Canadians, and to act accordingly. As a model for this, we would refer to the UK (United Kingdom) ICO (Information Commissioner’s Office)’s Regulatory Action Policy (https://ico.org.uk/media/about-the-ico/documents/2259467/regulatory-action-policy.pdf) (RAP) and the OAIC (Office

of the Australian Information Commissioner)'s Privacy Regulatory Action Policy (https://www.oaic.gov.au/about-us/our-regulatory-approach/privacy-regulatory-action-policy/). The ICO (Information Commissioner's Office)'s RAP (Regulatory Action Policy) is clear that organizations should be able to predict how the ICO (Information Commissioner's Office) will carry out its regulatory activity and that those who are subject to ICO (Information Commissioner's Office) regulatory action should be in no doubt that failures under the law will be pursued in a way that is transparent, consistent and proportionate. Per the RAP (Regulatory Action Policy), the ICO (Information Commissioner's Office) will select the most suitable regulatory tool in the circumstances by assessing the nature and seriousness of a failure, the sensitivity of the subject matter, whether and how individuals have been affected, the novelty and duration of the concerns, the public interest, and whether other regulatory authorities are already taking action on the matter.

Similarly, the OAIC (Office of the Australian Information Commissioner)'s policy outlines that where the OAIC (Office of the Australian Information Commissioner) has discretion as to whether to take regulatory action, it must prioritize matters for privacy regulatory action and select the most appropriate power in the circumstances. Factors the OAIC (Office of the Australian Information Commissioner) will take into account in deciding when to take privacy regulatory action, and what action to take, include: the seriousness of the incident or conduct to be investigated, the number of persons potentially affected, whether the matter involves sensitive information, whether conduct was deliberate or reckless, and the level of public interest or concern relating to the conduct, proposal or activity.

As noted at the outset, Canadians should be confident that the OPC (Office of the Privacy Commissioner of Canada) is able to effectively carry out its mandate of ensuring organizations' compliance with privacy law. A key element of this is to ensure that when the OPC (Office of the Privacy Commissioner of Canada) sees the need to act proactively in the interests of Canadians, it is able to do so. This includes the potential for proactive compliance activities to lead to meaningful enforcement action.

Recommendation 47: Section 82(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows:

~~If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act, t~~**T**he Commissioner may initiate a complaint **to ensure compliance with this Act.** ~~in respect of the matter.~~

Section 96 – Proactive compliance audits

Under Section 96 of the CPPA (Consumer Privacy Protection Act), to initiate an audit of the personal information management practices of an organization, the Commissioner must have "reasonable grounds to believe that the organization has contravened Part 1." The OPC (Office of the Privacy Commissioner of Canada) recommends that this threshold be amended, and that the OPC (Office of the Privacy Commissioner of Canada) be able to initiate an audit on reasonable notice.

Per section 97(1), the outcome of an audit is a report that contains the Commissioner's findings and a set of non-binding recommendations. This is a far less severe potential consequence than is possible through investigation of a complaint, as unlike an investigation:

- Audits cannot be the basis for a compliance order (though an interim order may be possible under 98(1)(d))
- Audits cannot lead to the recommendation of a penalty
- Audits cannot proceed to an inquiry
- Audits cannot trigger the private right of action (as currently drafted).

The threshold to initiate an audit also differs significantly from the standard proposed by the Department of Justice in its *Privacy Act* modernization consultation paper (https://www.justice.gc.ca/eng/csj-sjc/pa-lprp/dp-dd/raa-rar.html), which states:

> Currently, section 37 of the [Privacy Act] gives the Privacy Commissioner the power to review compliance with [the Act]. The Act could replace this with the power to audit the personal information management practices of a federal public body on reasonable notice.

In comparable jurisdictions, audits (or similar investigative tools) are generally available without the need to establish reasonable grounds – this includes Alberta (PIPA (Personal Information Protection Act) s. (section) 36(1)), Quebec (CQLR (Compilation of Quebec Laws and Regulations) c P-39.1, s. (section) 81), the GDPR (General Data Protection Regulation) (Article 58), Ireland (*Data Protection Act 2018*, s. (section) 136), United Kingdom (*Data Protection Act 2018*, s. 146), and Australia (*Privacy Act*, 1988, s. (section) 33C(2)).

The audit provisions in the CPPA (Consumer Privacy Protection Act) are described as a tool to "ensure compliance." However, they are limited in their ability to **proactively** ensure compliance, being available only after establishing reasonable grounds to believe non-compliance has already occurred. The increased flexibility provided to organizations under the CPPA (Consumer Privacy Protection Act) – and in particular, the increase in situations in which they are permitted to collect and use information without the knowledge or consent of the individual – suggests a need for proactivity from the regulator. As previously discussed in the context of accountability, in order for accountability to be demonstrable, it is fundamental that the regulator have the ability to proactively review records.

Similar to the investigative context, it would be important that audits be conducted in a manner that is risk based, proportionate and targeted. [14](#fn14)

Removing the reasonable grounds threshold from s. (section) 96 would align the CPPA (Consumer Privacy Protection Act) with the Department of Justice's audit-related suggestions for the *Privacy Act*, as well as bring the CPPA (Consumer Privacy Protection Act) closer to other domestic and international jurisdictions. More importantly, it would provide the Commissioner with a tool to support the proactive verification of compliance, which is recognized as an integral aspect of an effective data protection scheme.

Recommendation 48: That the condition "if the Commissioner has reasonable grounds to believe that the organization has contravened Part 1" be removed from s. (section) 96.

Section 110 – Prohibition on use of information provided by an organization

Section 110 of the CPPA (Consumer Privacy Protection Act) prohibits the Commissioner from using information requested or submitted on privacy management programs under sections 10 and/or 109(e) as grounds to initiate a complaint or to carry out an audit.

The OPC (Office of the Privacy Commissioner of Canada) is of the opinion that the prohibition against the use of information received in through section 10 or paragraph 109(e) is overly restrictive, and should be removed or amended.

Outside the context of an investigation or audit, an organization's privacy management program (or its associated policies, practices and procedures) can be reviewed in one of two ways: on request of the Commissioner under section 10, or on request of the organization under paragraph 109(e). Aside from the mandatory nature of the review under 109(e), this latter provision is very similar to the OPC (Office of the Privacy Commissioner of Canada)'s existing business advisory program.

In creating that program, the OPC (Office of the Privacy Commissioner of Canada) was seized with the question: "what balance needs to be struck between encouraging organizations to voluntarily engage with our advisors and

maintaining the OPC (Office of the Privacy Commissioner of Canada)'s ability to appropriately protect the privacy of Canadians?" To address this, a terms of engagement document was created, noting among other things that if the Business Advisory Directorate learns of willful, serious or systemic non-compliance during the course of an advisory activity, the activity would be terminated and the organization referred to the OPC (Office of the Privacy Commissioner of Canada)'s Compliance Sector. In that case, information obtained by the Directorate may be shared, to the extent necessary, and assessed as relevant evidence.

The organizations engaging with our Business Advisory Directorate have been satisfied with these terms and, up to this point, no organization has needed to be referred for investigation. Given this, an absolute prohibition on the initiation of an investigation based on information obtained through a voluntary engagement under 109(e) is both unnecessary and, in the case of evidence of willful, serious or systemic non-compliance, inappropriate.

This line of thinking is equally valid for information collected under section 10, particularly if that section is intended as a basis for demonstrable accountability. Granting the OPC (Office of the Privacy Commissioner of Canada) visibility into the practices of an organization but preventing it from taking any action to correct non-compliant practices (with the potential exception of making non-binding recommendations) would be detrimental to our role in protecting the privacy rights of individuals.

The way in which information provided under section 10 or paragraph 109(e) will be treated by the OPC (Office of the Privacy Commissioner of Canada) should certainly be clear to organizations, a principle that is ensured by section 111.

Lastly, removal of this section would also be consistent with analogous statutes in which a Commissioner or tribunal exercises overlapping functions. For example, the PIPA (Personal Information Protection Act) in both BC and Alberta grant the Commissioner the discretionary authority to comment on the privacy implications of an organization's existing or proposed programs, but neither law contains a prohibition against use of information gained through such an activity to commence an investigation.

Recommendation 49: That section 110 of the CPPA (Consumer Privacy Protection Act) be removed. Alternatively, that section 110 of the CPPA (Consumer Privacy Protection Act) be amended such that:

- There is no restriction to the use of information obtained under s. (section) 10.
- Any restriction on the use of information obtained under s. (section) 109(e) is not absolute, but rather subject to a policy drafted by the OPC (Office of the Privacy Commissioner of Canada) and made public per s. (section) 111.

Confidentiality and cooperation with other organizations

The OPC (Office of the Privacy Commissioner of Canada) recommends amendments to sections 115 to 117, which would enhance our ability to cooperate with domestic and international authorities. Here, our end goal is not strictly efficiency, but also efficacy. The ability to work and/or share information with other government authorities is essential given the cross-border and cross-sectoral nature of illegal uses of personal information. The OPC (Office of the Privacy Commissioner of Canada)'s long history of cooperation with domestic and foreign data protection authorities has shown the overall value of cooperation, and proven that it is possible to coordinate activities even where parties are applying different laws. Extending this potential for cooperation will create efficiencies for the OPC (Office of the Privacy Commissioner of Canada), but more importantly can lead to better outcomes for Canadians.

To achieve the desired level of cooperation, we make the following recommendations.

First, subsection 115(1) provides the Commissioner the authority to enter into agreements and arrangements with the

CRTC (Canadian Radio-television and Telecommunications Commission) and Competition Bureau in order to undertake and publish research and to develop procedures for disclosing information. However, there is no explicit provision to allow the OPC (Office of the Privacy Commissioner of Canada) to also enter into agreements in order to collaborate with the CRTC (Canadian Radio-television and Telecommunications Commission) and Competition Bureau on investigations, inquiries, or other formal compliance matters. We recommend addressing this gap, which would allow us to collaborate with our Canadian colleagues in the same way we currently collaborate with international data protection authorities.

Recommendation 50: That section 115(1) be amended to provide that the OPC (Office of the Privacy Commissioner of Canada) can enter into agreements with the CRTC (Canadian Radio-television and Telecommunications Commission) and Competition Bureau in order to collaborate on investigations, inquiries or other formal compliance matters.

Next, we note that there is a difference in scope between sections 116 (related to domestic collaborations) and 117 (international collaborations). In particular, section 116 makes reference to “any person who … has powers, duties and functions similar to those of the Commissioner with respect to the protection of personal information.” On the other hand, section 117 includes both the language of section 116 and a reference to “any person or body who … has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.” It is unclear why the scope for cooperation would be broader internationally than domestically, and so at a minimum we would recommend that the added language of section 117 be incorporated into section 116.

However, preferably, the OPC (Office of the Privacy Commissioner of Canada) would be able to cooperate on a wider scale. For instance, we have encountered situations in which collaboration with non-data protection authorities such as provincial human rights commissions, credit reporting regulators, or the Office of the Superintendent of Financial Institutions would have benefitted an OPC (Office of the Privacy Commissioner of Canada) investigation. As such, we recommend that section 116 also be expanded to include the ability to collaborate and share information with institutions responsible for the enforcement or administration of federal or provincial law. To be clear, this recommendation is not intended to expand the scope of the matters that can be investigated by the OPC (Office of the Privacy Commissioner of Canada), but rather to ensure the ability to work with other bodies in areas of overlap to promote effectiveness and efficiency.

Recommendation 51: That section 116 of the CPPA (Consumer Privacy Protection Act) be amended such to permit the OPC (Office of the Privacy Commissioner of Canada) to:

- (Preferred) Collaborate and share information with institutions responsible for the enforcement or administration of federal or provincial law.
- (Alternative) As per section 117, collaborate and share information with any person or body who has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.

Offences

The CPPA (Consumer Privacy Protection Act) introduces new offences and increased amounts for fines. These changes have prompted our consideration of the process for prosecutions.

As with the model under PIPEDA (Personal Information Protection and Electronic Documents Act), the CPPA

(Consumer Privacy Protection Act) provides that the OPC (Office of the Privacy Commissioner of Canada) can disclose information relating to the commission of an offence to the Attorney General of Canada (AGC) if, in the Commissioner's opinion, there is evidence of an offence. However, a discussion with the Public Prosecution Service (PPSC), which fulfills the responsibilities of the AGC (Attorney General of Canada) in prosecuting offences under federal statutes, confirms that this is not the most useful and effective route to a prosecution. The PPSC (Public Prosecution Service) does not investigate offences. The initial steps of evidence gathering and laying charges rests with either a law enforcement or other investigative agency who must be able to gather evidence that is both relevant and admissible to support a prosecution. In particular, an investigation aimed at obtaining evidence for purposes of a prosecution of an offence would require appropriate Charter protections.

In the context of offences under PIPEDA (Personal Information Protection and Electronic Documents Act) or the CPPA (Consumer Privacy Protection Act), the Royal Canadian Mounted Police (RCMP) could undertake these activities. However, the RCMP (Royal Canadian Mounted Police) may not always have dedicated resources to deal with offences under privacy law and may be faced with more pressing priorities. In our view, the more effective and efficient route would be for the OPC (Office of the Privacy Commissioner of Canada) to assume the primary responsibility for investigating offences and laying charges (in consultation with the PPSC (Public Prosecution Service) as appropriate) to support the prosecution of offences under the CPPA (Consumer Privacy Protection Act). In this regard, as the expert in privacy and the underlying statutory scheme, we are of the view that the OPC (Office of the Privacy Commissioner of Canada) is best placed to understand and assist in advancing the policy objectives behind the offence provisions.

Our discussion with the PPSC (Public Prosecution Service) confirms that the OPC (Office of the Privacy Commissioner of Canada) could not use investigation powers contemplated for the purposes of investigations and inquiries under the CPPA (Consumer Privacy Protection Act) to compel the production of evidence of an offence. Investigation tools with enhanced procedural safeguards such as search warrants and/or production orders with prior judicial authorization may at times be required. Accordingly, we recommend consideration be given to amendments to the CPPA (Consumer Privacy Protection Act) to ensure the OPC (Office of the Privacy Commissioner of Canada) explicitly has the appropriate authorities and tools necessary to support prosecutions, such as a scheme for offence investigations that includes authorities that permit the use of existing search and seizure provisions in the *Criminal Code*, or builds such authorities directly in the Act. While some federal models exist to draw from, we further recommend that any amendments be developed in consultation with the PPSC (Public Prosecution Service) to ensure the best approach is adopted to support prosecution of offences by the PPSC (Public Prosecution Service) and ultimately the policy objectives behind the offence provision in the CPPA (Consumer Privacy Protection Act).

Recommendation 52: Consider amendments to the CPPA (Consumer Privacy Protection Act) to ensure the appropriate structure and tools are available to effectively support the prosecution of offences under the Act.

Annex A – Full list of recommendations

No.	Recommendation
1	That the CPPA (Consumer Privacy Protection Act) be amended to introduce the proposed preamble.

No.	Recommendation
2	That section 5 of the CPPA (Consumer Privacy Protection Act) be amended as follow: **In an era in which significant economic activity relies on the analysis, circulation and exchange of personal information and its movement across interprovincial and international borders,** the purpose of this Act is ~~to establish rules to govern the protection of personal information~~ **to promote confidence and therefore the sustainability of information-based commerce by establishing rules** ~~to govern the protection~~ **for the lawful, fair, proportional, transparent and accountable collection, use and disclosure** of personal information ~~in a manner~~ that recognize a. the **fundamental** right of privacy of individuals, b. ~~with respect to their personal information~~ the need of organizations to collect, use or disclose personal information for purposes **and in a manner** that a reasonable person would consider appropriate in the circumstances, and c. **where personal information moves outside Canada, that the level of protection guaranteed under Canadian law should not be undermined.**
3	That subsection 12(1) of the CPPA (Consumer Privacy Protection Act) be amended as follows: An organization may collect, use or disclose personal information only for the purposes **and in a manner** that a reasonable person would consider appropriate in the circumstances.
4	That subsection 12(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows: The ~~following~~ factors ~~must~~ **to** be taken into account in determining whether the purposes **and manner** referred to in subsection (1) are appropriate **include**: … **(g) any other relevant factors in the circumstances**
5	That the factors set out in subsection 12(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows: a. the sensitivity of the information; **[delete if the proposed amendment make to subsection 12(2) non-exhaustive is not adopted]** b. whether the purposes represent legitimate business needs of the organization; c. the effectiveness of the collection, use or disclosure in meeting the organization's legitimate business needs; d. whether there are less intrusive means of achieving those purposes ~~at a comparable cost and with comparable benefits~~; ~~and~~ e. whether the individual's loss of privacy **or other fundamental rights and interests** is proportionate to the benefits ~~in light of any measures, technical or otherwise, implemented by the organization to mitigate the impacts of the loss of privacy on the individual~~; [Alternatively, the clause could be amended as: "whether the individual's loss of privacy, **dignity, autonomy and self-determination** is proportionate to the benefits."] f. **[if subsections 12(1) and 12(2) are amended as proposed to refer to means] whether the personal information is collected, used or disclosed in a fair, lawful and transparent manner; and** g. **any other relevant factor(s) in the circumstances.**

No.	Recommendation
6	That subsection 13 of the CPPA (Consumer Privacy Protection Act) be amended as follows: The organization may collect only the personal information that is necessary for the **specific, explicit, and legitimate** purposes determined and recorded under subsection 12(3).
7	That the definition of personal information be amended to expressly include inferred information.
8	That a definition of sensitive information be included in the CPPA (Consumer Privacy Protection Act), that would establish a general principle for sensitivity followed by an open-ended list of examples.
9	That the definition of commercial activity be clarified as follows: **Commercial activity** means: a. any particular transaction, act or conduct ~~or any regular course of conduct~~ that is of a commercial character, **whether or not it is committed by an organization whose general objectives are of a commercial character**; or b. any regular course of conduct that is of a commercial character, **including any activity that is part of a regular course of conduct that is of a commercial character** taking into account an organization's objectives ~~for carrying out the transaction, act or conduct~~ **and** the context in which it takes place~~, the persons involved and its outcome~~.
10	Subject federal political parties to the CPPA (Consumer Privacy Protection Act), for example by registering them in the schedule pursuant to subsection 6(3) and paragraph 119(2)(c).
11	That subsection 15(3) of the CPPA (Consumer Privacy Protection Act) be amended as follows: The individual's consent is valid only if, at or before the time that the organization seeks the individual's consent, it provides the individual with **the following information, in a manner such that it is reasonable to expect that the individual would understand the nature, purpose and consequences of the intended collection, use or disclosure. This** information **must be presented in an intelligible and easily accessible format, using clear and** ~~in~~ plain language.
12	That subsection 15(4) of the CPPA (Consumer Privacy Protection Act) be amended as follows: Consent must be expressly obtained unless ~~the organization establishes that~~ it is appropriate to rely on an individual's implied consent, taking into account the reasonable expectations of the individual and the sensitivity of the personal information that is to be collected, used or disclosed.
13	That the scope of the "commercial risk" exception be limited.
14	That paragraph 18(2)(e) be repealed, and that either: i. Any legitimate commercial interests which would have been enabled by paragraph 18(2)(e) be authorized via an explicit and knowable exception to consent; or, ii. A legitimate commercial interests exception to consent be introduced if accompanied by the introduction of a rights-based regime and pre-conditions such as the conduct of a PIA (Privacy Impact Assessment) and a balancing test, and if monitoring of its application was possible through proactive compliance checks by the OPC (Office of the Privacy Commissioner of Canada).

No.	Recommendation
15	That s. (section) 39 of the CPPA (Consumer Privacy Protection Act) be amended to require: • A written request be made prior to information being disclosed to ensure that the use is of societal benefit as defined in the CPPA (Consumer Privacy Protection Act); • An information sharing agreement be entered into, which would prohibit the recipient from re-identifying the information as well as from using the information for secondary purposes which are not of a societal benefit; and • The definition of "socially beneficial purposes" should be amended to include a limit on regulatory power, for example by indicating that they must be “purposes that are beneficial to society and not simply of individual or commercial interest or profit.”
16	That s. (section) 51 of the CPPA (Consumer Privacy Protection Act) be amended to provide, in addition to the conditions already present, that the personal information is such that the individual would have no reasonable expectation of privacy.
17	That the CPPA (Consumer Privacy Protection Act) maintains its current balance of providing organizations flexibility with respect to use of de-identified personal information while maintaining necessary controls and oversight by including de-identified information within the scope of the law. That the Act be amended to be explicit that it applies to de-identified information to address any potential ambiguity in this interpretation.
18	That record-keeping and reporting requirements be established with respect to disclosures of personal information to government organizations, especially with respect to disclosures to law enforcement.
19	That a definition clarifying the meaning of “lawful authority” for the purposes of section 44 be introduced.
20	That s. (section) 9 of the CPPA (Consumer Privacy Protection Act) be amended to prescribe an objective standard for accountability, as follows: 9(1) Every accountable organization must implement a privacy management program to ensure compliance with its obligations under the Act. (2) A privacy management program includes the organization’s policies, practices and procedures that serve to ensure compliance with the Act, and includes policies, practices and procedures respecting …
21	That accountability be strengthened in the CPPA (Consumer Privacy Protection Act), by: • Introducing a provision requiring organizations to maintain adequate records to demonstrate compliance with their privacy obligations under the Act, including an explicit traceability requirement in the context of automated decision-making; • Amending s. (section) 9(2) so that the scaling of accountability and record-keeping obligations be dependent on the nature and importance of the personal information under an organization’s control, the size and revenue of the organization, as well as relevant risks and threats.
22	That accountability provisions include two important proactive practices that will improve privacy compliance and respect for rights: • Requiring that organizations practice privacy by design; and • Requiring that PIAs (Privacy Impact Assessments) be undertaken for high risk activities

No.	Recommendation
23	That organizational requirements with respect to trans-border data flows be set out explicitly and separately, in a manner consistent with the recommendations set out in Annex B (#toc5).
24	That subsection 57(2) of the CPPA (Consumer Privacy Protection Act) be replaced by: In addition to the sensitivity of the information, the organization must, in establishing its security safeguards, take into account the risks to consumers, in the event of a breach, associated with the nature, scope, and context of its use of personal information, in light of the organization's business activities.
25	That subsection 58(2) of the CPPA (Consumer Privacy Protection Act) be amended as: The report must contain the prescribed information and must be made in the prescribed form and manner ~~as soon as feasible~~ **without unreasonable delay, but no more than 7 calendar days,** after the organization **becomes aware of the breach** ~~determines that the breach has occurred~~. and that subsection 58(6) of the CPPA (Consumer Privacy Protection Act) be amended as: The notification must be given ~~as soon as feasible~~ **without unreasonable delay** after the organization determines that the breach has occurred.
26	That recommendations 3, 4, 5, and 7 of Annex B (#toc5) also be applied in the context of domestic service providers.
27	That a standard for the level of explanation required under subsection 63(3) be enhanced to allow individuals to understand: (i) the nature of the decision they are subject to and the relevant personal information relied upon, and (ii) the rules that define the processing and the decision's principal characteristics. Where trade secrets prevent such an explanation from being provided, that at least the following be disclosed: (i) the type of personal information collected or used, (ii) why the information is relevant, and (iii) its likely impact on the individual.
28	That a right to contest automated decisions be included in the CPPA (Consumer Privacy Protection Act).
29	That section 55 be expanded to include *all* personal information held by an organization about the individual, subject to consideration of additional reasons for refusal.
30	That Parliament enact a clear and explicit right with respect to the de-indexing and/or removal of personal information from search results and other online sources, considering the OPC (Office of the Privacy Commissioner of Canada)'s recommendations in its 2018 Draft Position on Reputation and the approach proposed under Bill 64.
31	That section 72 of the CPPA (Consumer Privacy Protection Act) be expanded to include all personal information about an individual, including derived or inferred information.
32	That a clear consultative, advisory or approval role be established for the OPC (Office of the Privacy Commissioner of Canada) with respect to data mobility frameworks.

No.	Recommendation
33	That the following amendments be made with respect to the inquiries and investigations under the CPPA (Consumer Privacy Protection Act): • 98(1)(a): Reduce the threshold by which the OPC (Office of the Privacy Commissioner of Canada) can compel the production of evidence, and rephrase this power as “order” rather than “compel”; • 98(1)(h): Clarify that this provision also applies to information stored on remote servers, but accessible within the premises in question; • 103(2): Make orders under 98(1)(a) and 98(1) enforceable in the same manner as an order of the court; • 103(2) and 104: Appeal provisions relating to interim orders made pursuant to s. (section) 98(d) should be amended to ensure that such orders are not unduly delayed or undermined pending appeal; • 90(2): Enact necessary amendment to allow the OPC (Office of the Privacy Commissioner of Canada) to request and receive information subject to solicitor-client privilege, for the purpose of assessing claims of statutory exemptions in the context of access-related complaints; • 92(2): Strike the necessity test, which is not found in any comparable statute; • 92(4): Remove the one-year maximum period for extensions to completion of an inquiry.
34	That a paragraph be added under section 92(2) which permits the OPC (Office of the Privacy Commissioner of Canada) to order an organization to “take measures which allow individuals to be compensated for damages suffered, financial or otherwise, stemming from a breach or violation of security safeguards required by law.”
35	That the CPPA (Consumer Privacy Protection Act) be amended, with respect to compliance agreements, to permit: • The resolution of inquiries through compliance agreements; • The registration of compliance agreements with the court, making them equivalent to an order of the court; and, • The addition of the payment of AMPs (administrative monetary penalties) and all other negotiated measures as possible terms within compliance agreements.
36	We strongly recommend that the Personal Information and Data Protection Tribunal not be created and that the Privacy Commissioner be granted the authority to impose administrative monetary penalties at the conclusion of inquiries. If the Tribunal is created, we recommend in the alternative that its composition be amended to include a majority of judges, either sitting or retired, with lay members who “collectively have experience” in privacy.
37	That, should the tribunal remain in place, the CPPA (Consumer Privacy Protection Act) be amended to explicitly grant the OPC (Office of the Privacy Commissioner of Canada) standing before the tribunal.

No.	Recommendation
38	That subsection 93(1) of the CPPA (Consumer Privacy Protection Act) be amended to make the range of violations for which AMPs (administrative monetary penalties) may be imposed much broader, potentially encompassing all violations under Part 1 of the CPPA (Consumer Privacy Protection Act). The CPPA (Consumer Privacy Protection Act) should also be amended to include provisions similar to the UK (United Kingdom) *Data Protection Act* whereby, when appropriate, the Commissioner could give an organization an enforcement notice, clarifying the nature of a violation, before proceeding to the recommendation or the imposition of a penalty.
39	That section 93(2) be amended by: • Removing paragraph 93(2)(b); • Rephrasing paragraph 93(2)(c) to focus on history of *non*-compliance; and • Incorporating paragraphs 94(5)(b) and (c).
40	That subsection 93(3) be removed from the CPPA (Consumer Privacy Protection Act).
41	That section 106 of the CPPA (Consumer Privacy Protection Act) be amended to expand the private right of action, by replacing paragraphs 106(1)(a) and 106(1)(b) with requirements similar to section 77 of the *Official Languages Act*.
42	That sections 83 to 85 of the CPPA (Consumer Privacy Protection Act) be amended to provide the Commissioner greater discretion with respect to the conduct of investigations under the Act.
43	That s. (section) 109(e) of the CPPA (Consumer Privacy Protection Act) be amended so that the Commissioner is authorized, but not required, to give advice to organizations, on request, in relation to their privacy management programs.
44	That the Commissioner's obligation to review an application for approval of a code of practice or certification program be conditional on the payment of a cost recovery fee.
45	That all references to regulations in sections 76, 77, 78, 81 and 122 (a)-(j) of the CPPA (Consumer Privacy Protection Act) be removed, leaving to the Commissioner the authority, as is the norm in other jurisdictions, to adopt fair procedures to approve codes of practice and certification programs pursuant to the standards found at subsections 76(2) and 77(1) of the Act.
46	That section 108 of the CPPA (Consumer Privacy Protection Act) be amended to encourage the Commissioner, in the exercise of his powers and duties, to consider the size of the organization and other factors mentioned. Alternatively, include these factors in a purpose clause.
47	Section 82(2) of the CPPA (Consumer Privacy Protection Act) be amended as follows:<br ~~If the Commissioner is satisfied that there are reasonable grounds to investigate a matter under this Act,~~ ~~t~~**T**he Commissioner may initiate a complaint **to ensure compliance with this Act.** ~~in respect of the matter.~~
48	That the condition "if the Commissioner has reasonable grounds to believe that the organization has contravened Part 1" be removed from s. (section) 96.

No.	Recommendation
49	That section 110 of the CPPA (Consumer Privacy Protection Act) be removed. Alternatively, that section 110 of the CPPA (Consumer Privacy Protection Act) be amended such that: • There is no restriction to the use of information obtained under s. (section) 10. • Any restriction on the use of information obtained under s. (section) 109(e) is not absolute, but rather subject to a policy drafted by the OPC (Office of the Privacy Commissioner of Canada) and made public per s. (section) 111.
50	That section 115(1) be amended to provide that the OPC (Office of the Privacy Commissioner of Canada) can enter into agreements with the CRTC (Canadian Radio-television and Telecommunications Commission) and Competition Bureau in order to collaborate on investigations, inquiries or other formal compliance matters.
51	That section 116 of the CPPA (Consumer Privacy Protection Act) be amended such to permit the OPC (Office of the Privacy Commissioner of Canada) to: • (Preferred) Collaborate and share information with institutions responsible for the enforcement or administration of federal or provincial law. • (Alternative) As per section 117, collaborate and share information with any person or body who has responsibilities that relate to conduct that is substantially similar to conduct that would be in contravention of this Act.
52	Consider amendments to the CPPA (Consumer Privacy Protection Act) to ensure the appropriate structure and tools are available to effectively support the prosecution of offences under the Act.

Annex B – Recommendations relating to trans-border data flows

The following recommendations are largely extracted from the paper, *Bill C-11's treatment of cross-border transfers of personal information*, by Dr. Teresa Scassa. The OPC (Office of the Privacy Commissioner of Canada) has made two additional recommendations (13 and 14) to address other issues that we believe should be addressed in the context of trans-border data flows.

Recommendation 1:
The significance and complexity of cross-border data flows and the growing involvement of small and medium sized enterprises is such that they must be addressed in a specific dedicated section of the statute so that rights and obligations are clear and accessible. This will also serve to make express the fact that the law applies to cross-border data flows. Such a section should contain a version of s. (section) 11 of CPPA (Consumer Privacy Protection Act) reworked to specifically address the context of cross-border transfers.

Recommendation 2:
The changing nature of cross border data flows requires language that clearly reflects these changes. It is therefore recommended that the terms used to describe the actors in cross-border data flows be clear and distinct, and that they be directly related to roles/responsibilities with respect to personal data. This approach will inherently recognize that, for example, an organization may be a processor for some functions and a controller for others.

Recommendation 3:
The CPPA (Consumer Privacy Protection Act) is meant to apply to a broad range of actions (collection, use and

disclosure) with respect to data by both organizations and service providers. Some provisions, however, use the terms “transfer” and “transferred data” which do not adequately reflect this broad scope. As a result, there is uncertainty as to the application of these provisions in some circumstances. These provisions should be reviewed and reworded. See, in particular: s. (section) 7(2), s. (section) 11(1), s. (section) 11(2), s. (section) 19, s. (section) 62(2)(d).

Recommendation 4:
The definition of “service provider” expressly contemplates sub-contracting. The law should make it clear that in a sub-contracting situation, the organization/controller remains ultimately accountable for the personal data.

If organizations are meant to be accountable for what happens to personal data in the hands of a subcontractor, the CPPA (Consumer Privacy Protection Act) should provide that a contractor cannot subcontract personal data services without the consent of the organization/controller.

Recommendation 5:
Offshore service providers should not be able to avail themselves of the “business activities” exception to notice and consent in paragraph 18(2)(*e*) when they engage in the collection and use of data on their own behalf.

Recommendation 6:
Currently, s. (section) 11(1) of the CPPA (Consumer Privacy Protection Act) places an onus on organizations transferring data to service providers to ensure appropriate protection “by contract or otherwise.” Specific tools should be enumerated in the legislation to enable organizations to ensure that “substantially the same protection of personal information” is provided for in contracts involving cross-border transfers of data. These should include standard contractual clauses prescribed by regulations, or non-mandatory contractual clauses developed by the OPC (Office of the Privacy Commissioner of Canada) in consultation with stakeholders. Another option is a list of considerations that must be taken into account in drafting contractual clauses.

Nothing in the CPPA (Consumer Privacy Protection Act) is specific as to what “or otherwise” in s. (section) 11(1) might entail. The CPPA (Consumer Privacy Protection Act) should be amended to clearly state that the Codes of Practice and Certification Program provisions can be used to establish “substantially the same protection of personal information” in the context of cross-border data flows. In addition, the law should include options that respond to the reference to “or otherwise,” such as binding corporate rules or schemes.

Recommendation 7:
Currently subsection 11(2) provides that service providers are directly accountable under the CPPA (Consumer Privacy Protection Act) for any of the *transferred* personal information that the service provider collects, uses, or discloses for its own purposes. This accountability should not be limited to information that is transferred to it, but should also include information that it collects, uses and discloses on its own account in relation to the customers of the organization.

Section 11 should be amended to make it clear that service providers must provide substantially the same protection as the organization is required to provide for *all* personal information under their control, whether it is transferred to the service provider by the organization or whether the service provider collects, uses or discloses it on behalf of the organization.

Recommendation 8:
The CPPA (Consumer Privacy Protection Act) contemplates that a service provider may collect personal information on behalf of an organization. It should be amended to clarify that where service providers provide information to organizations that may have been collected by the service provider prior to the particular relationship, the organization must ensure that the information was collected in a manner consistent with Canadian data protection law.

Recommendation 9:
Section 61 imposes an obligation on service providers to give notice of data breaches to organization-controllers. In

the case of offshore service providers, it is not clear how this obligation is enforceable. The CPPA (Consumer Privacy Protection Act) should be amended to provide that in the case of offshore providers, the obligation to provide notice to the organization/controller must be part of their contractual arrangements.

Recommendation 10:
The 'transparency' requirement in paragraph 62(2)(d) is currently inadequate. It should be amended to achieve the following:

a. The ambiguity around the phrase "whether or not" should be corrected, as well as the uncertainty around what acts have "reasonably foreseeable privacy implications."
b. Organizations should be required to provide information about whether they carry out any international transfer or disclosure of personal information, and to provide sufficient details about these activities to enable individuals to understand the implications for their rights and to hold organizations and/or service providers to account. This should include the country or countries in which service providers are located.
c. Organizations should be required to provide specific notice of any risks regarding access to personal data by the authorities of the service provider's country.
d. Where service providers collect and use data for their own purposes, organizations should be required to disclose the identity of the service provider as well as the fact that the service provider, and not the organization, is accountable for this personal data.

Recommendation 11:
Bill C-11 should include a provision that requires organizations to assess whether a contract with a service provider will maintain substantially the same protection as afforded by the CPPA (Consumer Privacy Protection Act), taking into account the legal data protection regime in place in the country of a service provider that will be collecting, using or disclosing personal data on their behalf.

Recommendation 12:
To enhance the protection of the rights of Canadians in the context of cross border data flows, to ensure that Canada meets the standards set in Convention 108+, and to permit Canada to accede to Convention 108+, the CPPA (Consumer Privacy Protection Act) should be amended to provide that

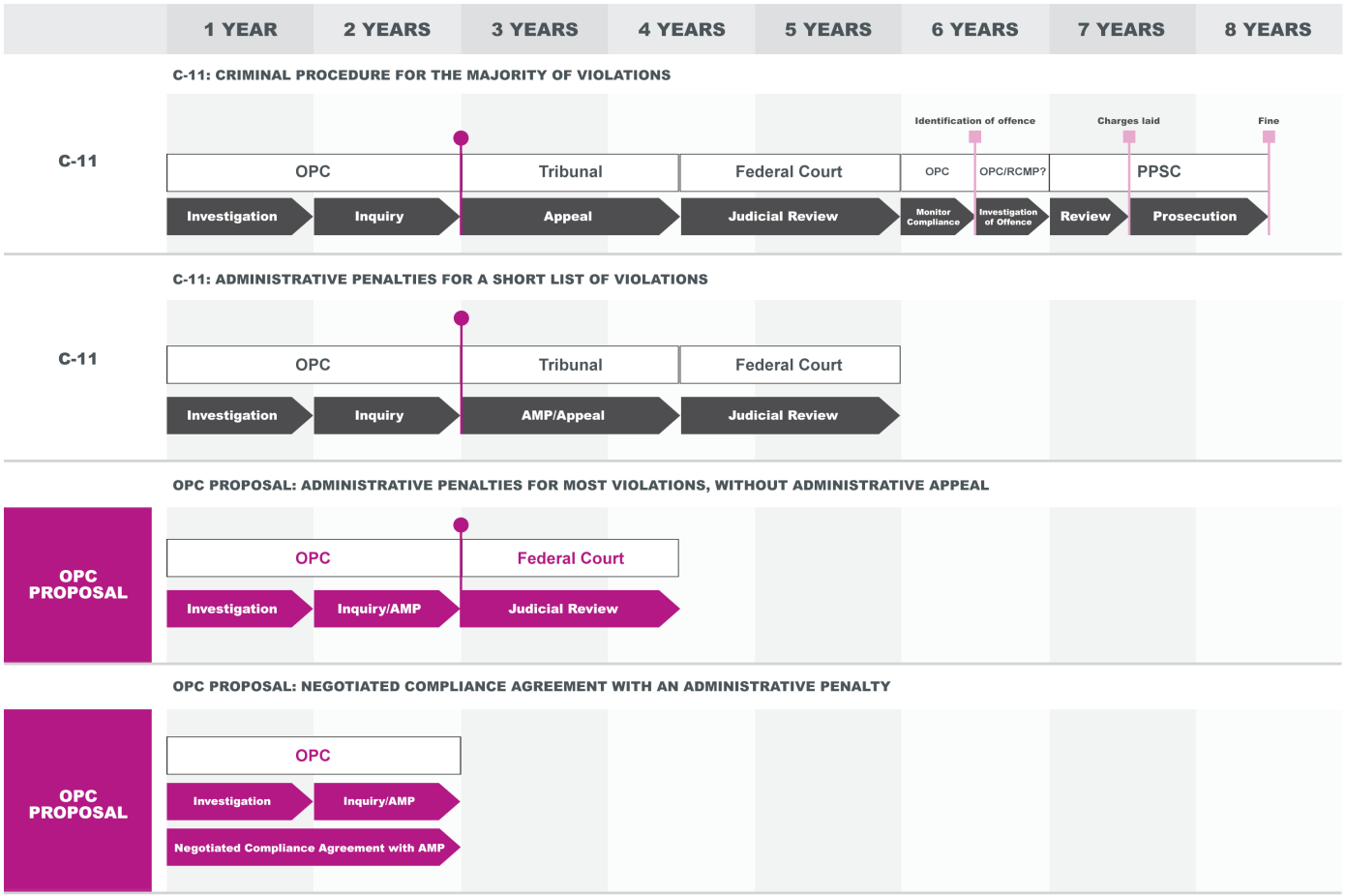
a. The Commissioner may request an organization to demonstrate the effectiveness of any safeguards put in place to govern data transfers;
b. The Commissioner be specifically empowered to prohibit, suspend, or place conditions on, offshore transfers of data where substantially similar protection is not in place.

In addition, we would propose the following two recommendations to ensure that the CPPA (Consumer Privacy Protection Act)'s protections adequately encompass all manner of cross-border data flows and avoid unwarranted asymmetries:

Recommendation 13:
The CPPA (Consumer Privacy Protection Act)'s protections should be expanded to include not only cross-border "transfers" to service providers but also "disclosures" to entities outside of the country, consistent with the approach taken by Canada's peers. In particular, organizations should be required to ensure that appropriate protections are in place prior to disclosing personal information to an organization outside of the country.

Recommendation 14:
The CPPA (Consumer Privacy Protection Act)'s transparency obligation (s. (section) 62(2)(d)) should be expanded to encompass cross border data flows other than transfers or disclosures. In particular, it should apply to organizations with a real and substantial connection to Canada that collect personal information in Canada but store or process the information in another country.

Annex C – Complaint timelines under various C-11 scenarios



7.5 YEARS

C-11: CRIMINAL PROCEDURE FOR THE MAJORITY OF VIOLATIONS

Under C-11, only a few contraventions of the law can lead to the imposition of an administrative monetary penalty ("AMP") as set out in section 93 of the Consumer Privacy Protection Act (CPPA). Others, including those relating to meaningful consent or exceptions to consent, would only be subject to orders. In these cases, it is only in the event that an order is knowingly contravened that an organization could be subject to a fine, and even then only following criminal proceedings. In these cases the timeline would be as follows: the Commissioner conducts an investigation into the complaint, and then an inquiry, leading to an order (estimated at two years). The organization appeals the order to the Tribunal (another year and a half). Where unsuccessful, the organization can bring the matter to Federal Court for judicial review (another year and a half). Assuming the OPC's order is upheld, the organization would then be given some time to comply (estimated here to six months). Should the organization knowingly contravene the OPC order, this constitutes an offence and a criminal investigation would begin (six months). After investigation, the file is sent to the Public Prosecution Service Canada (PPSC) for a determination of whether a prosecution is in the public interest (six months). If so, charges are laid and prosecution begins (one year). If successful, only then could the organization be fined. The matter is concluded, following a very circuitous route, 7.5 years after a complaint was first filed with the OPC.

5 YEARS

C-11: ADMINISTRATIVE PENALTIES FOR A SHORT LIST OF VIOLATIONS

For the few violations subject to AMPs, the timeline would be as follows: the Commissioner conducts an investigation into the complaint, and then commences an inquiry. At the conclusion of the inquiry, the Commissioner issues an order to bring the organization into compliance with the law, and recommends an AMP (estimated at two years). Since the organization has to appear at the Tribunal for an AMP hearing, the organization concurrently appeals the order (another year and a half). Assuming the appeal is unsuccessful and the Tribunal imposes an AMP, the organization would then file an application for judicial review. This can take another year and a half. The matter is concluded five years after the complaint was initially filed.

3.5 YEARS

OPC PROPOSAL: ADMINISTRATIVE PENALTIES FOR MOST VIOLATIONS, WITHOUT ADMINISTRATIVE APPEAL

To have trust in the law, consumers expect that violations will lead to meaningful and timely consequences. To our knowledge, no other jurisdiction limits the imposition of an AMP to such a narrow list of contraventions as found in s.93 of the CPPA. Most contraventions must be subject to AMPs for the regime to be effective. Should the OPC be authorized to impose AMPs, with the availability of judicial review to ensure accountability and fairness, consumers would have greater access to timely and effective remedies. This scenario would proceed as follows: the Commissioner conducts an investigation into the complaint, and then an inquiry, which produces an order and an AMP against the organization (estimated at two years). As with all OPC decisions, the organization retains the right to file an application for judicial review (estimated at one and a half years). Here, the matter is concluded approximately 3.5 years after the complaint was first filed with the Commissioner. A further reduction to the timeline is also possible through the negotiation of a settlement between the organization and the OPC, as illustrated in the following scenario.

2

OPC PROPOSAL: NEGOTIATED COMPLIANCE AGREEMENT WITH AN ADMINISTRATIVE PENALTY

Under C-11, a negotiated settlement in the form of a compliance agreement is no longer possible once an inquiry has begun. The CPPA then dictates that the process becomes entirely adversarial and may result in an AMP only through decision of the Tribunal. However, it is in the interest of all parties that cases can be resolved through a negotiated settlement at any point. To prohibit such settlements is not in the interest of justice and may actually result in unnecessary costs for everyone. To further

strengthen effectiveness, OPC recommends that the payment of AMPs be added as a possible negotiated term in a compliance agreement. For example, the scenario could be as follows: the Commissioner closes the investigation and/or an inquiry through the negotiation of a compliance agreement, which can include payment of an AMP. The compliance agreement would be registered with the Federal Court and take on the same force and effect as a court order. There is no judicial review because the AMP was negotiated. The matter is closed within two years of the complaint being filed.

► Text version of the C-11 Timelines and Scenarios

Footnotes

1 Towards Privacy by Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report of the Standing Committee on Access to Information, Privacy and Ethics, February 2018.

2 The paper produced by Dr. Scassa during this engagement is unpublished. However, another paper published by Dr. Scassa draws from her original work for the OPC (Office of the Privacy Commissioner of Canada): A Human Rights-Based Approach to Data Protection in Canada, in Dubois, E. and Martin-Bariteau, F. (eds.), Citizenship in a Connected Canada: A Research and Policy Agenda, Ottawa, ON: University of Ottawa Press (2020).

3 *Nammo v. (versus) Transunion of Canada Inc.*, 2010 FC 1284, at paragraphs 74 and 75.

4 See for example: Alberta (Information and Privacy Commissioner) v. (versus) United Food and Commercial Workers, Local 401, 2013 SCC 62 (CanLII), [2013] 3 S.C.R. 733 at paras. 19 & 22.

5 Sehgal, Pragya. "Microsoft CEO (Chief Executive Officer) says privacy is a human right, and businesses should treat it as such" IT World Canada, Jan 25 2020. Quote also available in this interview: Satya Nadella, Microsoft CEO (Chief Executive Officer): An Insight, An Idea | DAVOS 2020.

6 Hodge, Neil. "Microsoft president: Tech companies must embrace privacy regs" *Complianceweek*, Oct 23 2019.

7 Schiff, Allison. "Apple Says IDFA Changes Will Go Live 'In Early Spring' As Tim Cook Denounces The 'Data Industrial Complex'" *AdExchanger*, Jan 28 2021.

8 *Reference re Greenhouse Gas Pollution Pricing Act* , 2021 SCC 11 at paras. 59-61.

9 *Reference re Genetic Non-Discrimination Act*, 2020 SCC 17 at para. 170, per Kasirer J. (dissenting, but not on this point).

10 *Turner* 2005 FC 1601 (CanLII), affd by the FCA in *Wansink v. (versus) TELUS Communications Inc.*, 2007 FCA 21 (CanLII), at para. 15.

11 *R v (versus) Spencer*, 2014 SCC 43; *R v (versus) Kang-Brown*, 2008 SCC 18; *R v (versus) Gomboc*, 2010 SCC 55.

12 Ignacio Cofone, "Policy Proposals for PIPEDA (Personal Information Protection and Electronic Documents Act) Reform to Address Artificial Intelligence Report" *Office of the Privacy Commissioner of Canada*, Nov 2020.

13 Article 12 of the Universal Declaration of Human Rights, and Article 17 of the International Covenant on Civil and Political Rights.

14 United Nations Human Rights Committee, "International Covenant on Civil and Political Rights" *United Nations*, March 29 2004, at paragraph 8.

15 For example, see criteria used by the UK (United Kingdom) ICO (Information Commissioner's Office) as outlined in its Guide to ICO (Information Commissioner's Office) Audits.

Date modified:

2021-05-11