Canadian Wireless Telecommunications Association

Submission to Innovation, Science and Economic Development Canada consultation -

"Strengthening Privacy for the Digital Age:

Proposals to modernize the *Personal Information Protection and Electronic Documents Act*"

September 10, 2019

EXECUTIVE SUMMARY

Canada's current legal framework for balancing the protection of privacy with the economic and social potential of the digital age, of which the *Personal Information Protection and Electronics Documents Act* (PIPEDA) forms a part, is sound and does not require significant changes. While some changes to address the risks for "consent fatigue" and to update or clarify specific provisions are warranted, we do not think that all of the proposals made by the Government are necessary.

Most importantly, it is our view that the current privacy legal framework already contains sufficient incentives and deterrents for organizations. This is evidenced by the fact that the number of complaints received by the Office of the Privacy Commissioner (OPC) is declining and the vast majority of them are resolved through early resolution processes. For example, when comparing the statistics for 2013 and 2018, the number of complaints accepted by the OPC dropped from 426 to 297, a decrease of 30.3%. Over that same period, the number of complaints resolved through early resolution has increased from 133 to 205, an increase of 54.1%.

Rather than focusing primarily on enforcement, we recommend that more emphasis be placed on enhancing collaboration between the OPC and organizations so that privacy-related issues can be dealt with proactively, rather than waiting for investigations to be initiated. If new deterrents and enforcement tools are introduced, they should be carefully targeted, proportionate, and accompanied by appropriate procedural safeguards.

For convenience, a summary of CWTA's submissions is listed below. Please refer to the main body of this document for our full explanation of our submissions.

Submission #1: We agree with the Government's proposal that consent should not be required for "standard business practices."

Submission #2: We support the proposed requirement for plain-language on the intended use of collected information but we do not agree that organizations should be required to use "specific" or "standardized" language.

Submission #3: We support the Government's proposal that PIPEDA be amended to include an exemption to consent for the use and disclosure of de-identified information.

Submission #4: We agree that the consent exemption for publicly available information should be preserved, but that the regulations specifying publicly available information should be amended.

Submission #5: While we understand that data mobility, or portability, may be appropriate for some industries, we have concerns with introducing a portability right within PIPEDA and applying the corresponding obligations to all industry sectors.

Submission #6: With respect to online reputation and source takedown/deletion, PIPEDA already provides rights and obligations such as withdrawal of consent, correction of inaccurate information, and

deletion. The additional measures proposed by the Government are not necessary and, in some cases, impractical.

Submission #7: We disagree with the Government's conclusion that the ombudsman model and enforcement tools of PIPEDA are outdated and do not incentivize compliance. The Government offers little evidence to support this claim, while the Office of the Privacy Commissioner's (OPC) annual reports show the opposite. Rather than focusing primarily on enforcement, the Government should consider ways in which the ombudsman model can be enhanced, such as improving education and increasing collaboration between the OPC and organizations.

Submission #8: We support retaining the OPC's education and awareness mandate. We also support extending the Minister's existing authority to include the authority to direct the OPC to undertake research on themes relevant to the Minister's mandate. We also think that the Minister should have the authority to direct the educational focus of the OPC.

Submission #9: We support providing increased discretion to the Privacy Commissioner on whether to investigate complaints. We do not support increased flexibility for auditing or reviewing organizations for compliance with PIPEDA. Additional procedural safeguards for organizations in relation to the conduct of audits should be introduced.

Submission #10: Any discussion of increasing cooperation and information sharing between the OPC and other enforcement agencies should be subject to a separate consultation so that stakeholders can adequately consider specific proposals and their potential impact.

Submission #11: We do not think the OPC requires additional order-making powers. If additional powers are introduced they should be restricted to those set out in the consultation document and should be subject to sufficient procedural safeguards, including the right of appeal.

Submission #12: If the current fine regime is extended to include other key provisions of the Act, the current requirement that an organization "knowingly" contravened the provision in question must also apply. Similarly, the decision to seek fines should reside with the Attorney General and the organization must be able to appeal any decision that it contravened the Act.

Submission #13: We do not agree that fines need to be "substantially" increased. If fines are increased they should include a range of fines that are proportionate to the seriousness of the wrongdoing and its impact. Fines should only be applied after other tools, such as warning letters, have been used and failed.

Submission #14: Fines should not be based on the revenues of the organization. Focusing primarily on an organization's revenues can result in fines that are disproportionate to the level of wrongdoing and/or harm inflicted. In determining what level of fine to impose, if any, a court should be required to consider factors such as the degree of demonstrable harm to the consumer, the organization's history of compliance, whether the violation was negligent or intentional, due diligence exercised by the

organization, and the organization's reaction to the initial complaint (e.g. remedial action taken; cooperation with investigation).

Submission #15: We do not support the introduction of statutory damages. Courts are best placed to assess the degree of harm and any potential damages that should be awarded.

Submission #16: Any additional powers and enforcement tools for the OPC should come with additional responsibilities, including requiring the OPC to be more transparent in its methods, investigations, and determinations.

Submission #17: We do not agree with the Government's proposition that PIPEDA is difficult to understand and should be significantly rewritten. The principles-based framework of the Act remains sound.

INTRODUCTION

The Canadian Wireless Telecommunications Association (CWTA) is pleased to provide its comments to the Government of Canada's *Proposals to modernize the Personal Information Protection and Electronics Documents Act*. CWTA is the authority on wireless issues, developments and trends in Canada. Its membership is comprised of companies that provide services and products across the wireless industry, including wireless carriers and manufacturers of wireless equipment, who combine to deliver Canada's world-class wireless services, one of the key pillars on which Canada's digital and data-driven economy is built.

For our members, the protection of personal information is a key element of their business practices and corporate ethos. Their reputations and success are based on establishing a trusting relationship with their customers. It is why they invest significant resources into their privacy-related processes and security.

As set out in the Government's consultation document, the world is undergoing a digital and data-driven revolution in which the innovative combination of data and technology will enable Canadians to be more productive, generate economic growth, and deliver a higher quality of life. But with each new opportunity comes potential new risks, and that is why it is important to balance the legitimate and responsible use of data, including innovative uses of personal information, with the protection of privacy.

It is for that reason we welcome the Government's review of the *Personal Information Protection Electronic Documents Act* (PIPEDA) to ensure that it properly addresses technological and societal change. As we explain in our comments below, we think that Canada's current legal framework for balancing the protection of privacy with legitimate uses of individual's data, of which PIPEDA forms a part, is sound and does not require significant changes. Most importantly, it is our view that the current privacy legal framework already contains sufficient incentives and deterrents for organizations and that more emphasis should be placed on enhancing collaboration between the Office of the Privacy Commissioner (OPC) and organizations so that privacy-related issues can be dealt with proactively,

rather than waiting for investigations to be initiated. If new deterrents and enforcement tools are introduced, they should be carefully targeted, proportionate, accompanied by appropriate procedural safeguards and enable the exercise of discretion to ensure appropriate application.

Finally, in our submission we have not commented on every proposal contained in the consultation document. We have limited our response to those matters most relevant to our industry. Our decision not to provide a response to particular proposals in the consultation document is not an indication of CWTA's agreement with such proposals.

PIPEDA: Standing the Test of Time

When PIPEDA was developed nearly 20 years ago, it was hailed as a remarkable achievement built through consultation amongst consumer, business, and government representatives, and encompassing the ten commonly accepted fair information principles that reflect the concepts of openness and transparency, knowledge and consent, and sensitivity and harm. Equally important, it was drafted in technology-neutral language.

The technical advances and innovations that have occurred since PIPEDA's inception have introduced new ways for individuals to interact with other individuals, businesses and government, and in some cases the amount and type of personal information that they share with others. Notwithstanding these advances, PIPEDA and the privacy principles on which it is based have withstood the test of time, and continue to provide a sound framework that balances the right to privacy with the need for organizations to collect, use and disclose personal information for reasonable purposes and, when applicable, with informed consent.

Despite this, some argue that the PIPEDA model no longer meets the needs of a digital and data-driven economy and requires significant changes. In doing so, they point to more recent privacy regulations enacted in other countries, or argue that the principle of consent has outlived its useful purpose.

While there is opportunity to enhance and clarify the privacy protections in PIPEDA, we disagree with the notion that PIPEDA requires a substantial overhaul. PIPEDA has stood the test of time because it is based on strong principles that support both privacy and innovation. In most cases, these principles can be applied to new and innovative products and services and other new uses of personal data without the need for legislative change. As technology and the collection and use of personal information has evolved, so too have the concepts of transparency, informed consent and what individuals consider to be reasonable. This has resulted in investigations, findings and guidelines issued by the Privacy Commissioner that have introduced new ways and methods for organizations to ensure transparency and informed consent when collecting personal information. Privacy By Design guidelines, transparency reports, and the new consent guidelines are concrete examples of how PIPEDA and tools created to support it have successfully met the challenges of an evolving world of information sharing.

Where gaps in regulation have been identified, targeted changes have been introduced, such as those introduced in 2015 by *The Digital Privacy Act*. These changes included measures dealing with protecting

vulnerable Canadians, additional exceptions to the need for consent, and data breach notification obligations and associated additional powers for the Privacy Commissioner.

Not a Catch-All Solution

When considering potential changes to PIPEDA, we caution the Government against trying to address all potential issues or concerns about the use of personal information and data within PIPEDA. PIPEDA is but one element of Canada's privacy framework, which includes provincial legislation, sector specific regulations and common law claims brought through private litigation. As discussed below, some of these other mechanisms are better suited to address issues raised in this consultation.

Other Elements of Trust

It would also be short-sighted to think that regulation is always the best way to foster trust. The European Union Agency for Network and Information Security (ENISA), now the EU Cybersecurity Agency, identified trust as a function of (1) the user's knowledge of online privacy, (2) the technology design, (3) the practices of the providers, and (4) the institutions governing the system.[1] Yet, as many observers have noted,[2] when the EU developed its new General Data Protection Regulation it focused almost exclusively on the last two elements: regulatory compliance and enforcement. In doing so, the EU "clearly puts the thumb on the scale in favor of regulation over innovation".[3] The result has been a variety of unintended consequences, including no increase in consumer trust, the weakening of SMEs, high costs of compliance, increasing cybersecurity risks, and increasing market share for the dominant social media and on-line advertising platforms.[4]

Too heavy a reliance on regulation can have unintended consequences, including stifling innovation and impairing Canada's ability to benefit from the digital and data-driven economy. For example, unnecessary regulation would represent a barrier to entry for all businesses, but particularly small and medium-sized enterprises, which in turn slows economic growth. Excessive regulation also results in finite resources being shifted to ensuring compliance and away from innovative research and development. It also discourages investment in Canada and can result in innovative products and services not being made available to Canadians.

Rather than focusing on additional regulation, Canada should increase its attention to other elements of trust in order to expand consumer confidence in the manner in which their personal information is collected, used and disclosed. For example, attention should be paid to increasing Canadians' digital

[1] As referenced in "Understanding the GDPR and its Unintended Consequences", Strand Consult, strandreports.com

[2] Ibid., see also "How the GDPR compares to best practices for privacy, accountability and trust", Roslyn Layton and Simone Celant, https://bit.ly/2Q5fmm2

[3] See Strand Consult at p14.

[4] See "The 10 Problems of the GDPR", Statement before the Senate Judiciary Committee On the General Data Protection Regulation and California Consumer Privacy Act: Opt-ins, Consumer Control, and the Impact on Competition and Innovation, Roslyn Layton – at https://www.judiciary.senate.gov/imo/media/doc/Layton%20Testimony.pdf

literacy and knowledge of ways in which they can protect and control the sharing of their personal information. Armed with such knowledge, Canadians will be better equipped and more likely to engage in the digital and data economy.

Similarly, an emphasis on the development of systems that are designed to minimize or eliminate the sharing of personal information is preferable to, and more cost-effective than, increasing regulation. In fact, encouraging Canadian businesses and organizations to experiment with privacy enhancing technologies and systems, such as identity authentication, anonymization of personal information, and other limited disclosure techniques would, in combination with a stable and balanced regulatory environment, make Canada an attractive location for companies and other organizations to develop innovative uses of data and digital technologies that can help improve the quality of living, grow the Canadian economy and create jobs

RESPONSE TO THE GOVERNMENT'S PROPOSALS

PART 1: ENHANCING INDIVIDUALS' CONTROL

A. Consent & Transparency

i. Standard Business Practices

As mentioned in the consultation document, PIPEDA already requires organizations to inform and obtain the individual's consent for the collection, use and disclosure of their personal information. The OPC has also issued guidance which sets out further requirements and recommendations for how organizations can obtain meaningful consent. However, relying solely on lengthy privacy policies to obtain consent, even for uses that an individual would reasonably expect, has proven to be less than ideal. For this reason, CWTA agrees with the Government's proposal that consent should not be required for "standard business practices".

This approach would benefit both organizations and individuals. Organizations would benefit by having greater certainty as to when consent must be obtained, and being able to provide potential customers with streamlined consent notices that focus on what individuals really want to know; namely, collection and uses of information that would not reasonably be expected or where potential risk of harm is the greatest. Individuals would benefit by not receiving consent notices for collections and use of information that should reasonably be expected. This would reduce "consent fatigue" as individuals would know that if they receive a request for consent it is because the information or use in question may be outside their reasonable expectations or pose a potentially greater risk of harm. This would make consent notices more meaningful to individuals.

As noted above, one of the strengths of PIPEDA is that it is principles-based, which enables its application to adjust to changes in technology and business practices. The same principles-based approach should be applied when defining "standard business practices". By using a principles-based definition, what is regarded as a standard business practice can evolve with time and be further refined by future guidance and decisions by the OPC or the courts.

A standard business practice should include any practice that is customary to the business in question and for which it is reasonable to expect that the individual would consent to the collection, use and/or disclosure of the personal information in question. Examples of standard business practices would include those mentioned in the consultation document; namely, fulfilling a service, using information for authentication purposes, sharing information with third-party processors, risk management, or meeting regulatory and legal requirements.

ii. **Specific, Standardized, Plain-Language**

While CWTA supports the use of plain-language when describing the intended use of personal information, we do not support the consultation document proposal that organization be required to use specific and/or standardized language. Requiring specific and standardized language ignores the fact that the type of information collected from individuals and the uses of that information has evolved, and will continue to evolve, over time. Even if it were possible to create standardized language that captures all of today's potential uses of personal information, new uses of information will be developed that will likely fall outside of the standardized language. Moreover, the concepts of standardization and specificity are contradictory. If organizations are unable to tailor the language used in their consent notices to accurately describe new uses, or tailor the language to best suit the intended audience, individuals may not be sufficiently informed of the intended use of their information.

Instead, organizations should remain responsible for developing consent notices that are user-friendly and understandable, and to adapt their practices to maintain and enhance meaningful consent. This approach is supported by the OPC's "Guidelines for obtaining meaningful consent", which state that "[c]onsent processes must take into account the consumer's perspective to ensure that they are user-friendly and that the information provided is generally understandable from the point of view of the organization's target audience(s)." Importantly, the OPC has stated that it does not see itself as having a role to play in drafting privacy policy templates.[5] Our members spend significant time and resources to make their consent processes understandable and accessible to their customers, and to update these processes and consent language as their business models evolve. Requiring that they, or any other organization, use specific and standardized language would not enhance the goal of meaningful consent.

iii. De-identified Information

De-identification of personal information is an important privacy protection tool. It is also a valuable way to safely enable the use and sharing of information for legitimate and innovative purposes, both commercial and non-commercial, such as policy making, quality assurance testing, business planning, research, security and threat assessment, evaluating trends and diagnosing issues, and understanding aggregated use patterns and behaviours.

[5] Towards Privacy of Design: Review of the *Personal Information Protection and Electronic Documents Act*, Report by the Standing Committee on Access to Information, Privacy and Ethics. February 2018. Page 21.

CWTA supports the consultation document proposal that PIPEDA be amended to include an exemption to consent for the use and disclosure of de-identified information. De-identified information should consist of information that is not linked or reasonably linkable to an individual or device. The reasonableness standard is in recognition that, just as with other security processes, one cannot guarantee that re-identification is always impossible.

To protect against the risk of re-identification, the Government can consider sanctions, such as fines, against any person or organization that intentionally attempts to re-identify information. It may also wish to consider requiring organizations to include contractual prohibitions on recipients of the de-identified information from attempting to re-identify it. An exemption to the contractual requirement could be included for de-identified information that is so highly abstracted that a reasonable person with data science expertise would not consider it possible to re-identify such information.

iv. Publicly Available Information

CWTA agrees that the consent exemption for publicly available information should be preserved, but that the regulations specifying publicly available information should be amended. The current regulations set out types of information and formats that were prevalent at the time and are now outdated. As technology has evolved, so too has the way in which individuals make their information publicly available and their expectations regarding how that information may be used. In addition to making the exemption technology-neutral, an exemption should be added for information about an individual that is voluntarily put into the public domain by that individual with the reasonable expectation that it may be used by others.

B. Data Mobility

In the consultation document the Government proposes an "explicit right for individuals to direct that their personal information be moved from one organization to another in a standardized digital format, where such a format exists." The reason cited by the Government for proposing such a right is that it "has the potential to enhance consumer choice" by fostering innovative alternative services and "encouraging competition".

While we recognize that the concept of data portability is useful in the context of voluntary participation in data trusts and other data management schemes, CWTA has concerns with introducing a portability right within PIPEDA and applying the corresponding obligations to all industry sectors.

First, while the inability to easily transfer personal information to an alternate service, such as some social media platforms or online data storage services, may present a barrier to switching service providers, such is not the case with every industry, including mobile wireless services. Wireless subscribers can easily switch to another wireless service provider, including being able to use the same phone number with the new service provider.

Requiring the mobile wireless industry, and similarly situated sectors, to engineer technical solutions and procedures to enable personal data transfers that will provide little, if any, benefit to consumers is an unnecessary burden that will only make the provision of services more costly. It also gives rise to potential security risks as fraudsters could attempt to impersonate consumers and use the portability right to illegally obtain consumer's personal information.[6] In fact, it may require organizations to collect even more personal information from individuals for the sole purpose of being able to authenticate the individual in case a data request transfer is made.

Secondly, in sectors where the inability to easily transfer personal information presents a potential barrier to competition, the matter is better dealt with under competition law.

Notwithstanding the above, should a right of portability be implemented within PIPEDA it should include several restrictions. First, data portability should not cover all personal data, as portability is different than a right to access. Portability should only apply to information that was provided by the data subject as well as observed data that is indirectly provided by the data subject when using the service (e.g. location data, activity logs, etc.). It should not include data and information that is derived from such information. Derived information is the work product of the organization and in many cases will comprise of intellectual property rights or commercially sensitive or confidential information of the organizations.

Exceptions should also include instances in which transferring information would: be contrary to law; prejudice an investigation; reveal proprietary processes or technologies; or be technically unfeasible. In addition, where an individual has provided information that includes third-party information (e.g. photos uploaded to cloud storage or a social media account) it is not reasonable to expect transferring organizations to separate third-party information from that which pertains solely to the customer. Transferring organizations should also be permitted to decline to transfer such information if the individual refuses to first provide reasonable assurances that he or she has the right to provide such information, includes third-party information, to the transferee organization. Organizations should also be shielded from liability for transferring such information where they receive such assurances.

C. On-line Reputation

When considering online reputation and PIPEDA, one must recognize the issue of online reputation goes beyond the scope of PIPEDA and federal jurisdiction. Much, if not most, of the harm that occurs to online reputation takes place outside of commercial transactions and instead occurs within the realm of personal relationships. As such, some provincial governments have introduced legislation that permits an individual to sue another for invasion of privacy,[7] while the federal government has introduced the

[6] See https://www.theregister.co.uk/2019/08/09/gdpr_identity_thief/ for examples of how fraudsters have used new individual rights under the GDPR to illegally obtain information.
[7] See the *Privacy Act* of each of British Columbia, Saskatchewan, Manitoba and Newfoundland & Labrador, as well as Article 35 of Quebec's Civil Code.

Protecting Canadians from Online Crime Act which criminalizes the online dissemination of intimate images without consent.

In the context of commercial transactions, two of the most commonly mentioned potential solutions are de-indexing and source takedown/deletion. As mentioned in the consultation document, de-indexing is the removal or suppression of links in online search engines, but does not result in the removal of the material in question from the source web page. De-indexing just makes it much harder for the public to find the original source. As the issue of de-indexing is currently before the courts in Canada and is not part of this consultation, our comments will focus on the issue of source takedown/deletion.

PIPEDA already provides that an individual can withdraw consent for the use of any personal information, subject to contractual and legal restrictions, allowing individuals to correct inaccurate information, and a requirement that organizations delete or dispose of personal information when it is no longer required. In the consultation document the Government suggests that, despite these rights and obligations, additional measures may be required.

First, the consultation document proposes that all individuals be given "the explicit right to request deletion of information about them that they provided, with some caveats". As mentioned above, individuals already have a right to withdraw consent to the use of information they have provided, subject to contractual and legal restrictions. Presumably the proposed additional right to request deletion is meant to be a companion to the right to withdraw consent, and to clarify that where consent is withdrawn, such information should be deleted. If enacted, the right to request deletion of information provided by the individual should be subject to the same contractual and legal restrictions that qualify the right to withdraw consent.

A second proposal is to inform minors of their rights to delete or de-identify their personal information that they provided and how to do so. While we do not oppose additional controls or protections for minors, a distinction should be made between organizations that target their goods and services to minors and those that do not. For example, organizations that do not knowingly collect personal information from minors should not be required to establish costly new processes for dealing with requests for the deletion or de-identification of personal information provided by minors. Any such requirement should be targeted to organizations that market or sell their products or services to minors.

The third proposal would require organizations to "ensure the accuracy and integrity of information about an individual throughout the chain of custody by requiring organizations to communicate changes or deletion of information to any other organization to which it has been disclosed." Such a requirement would create a significant burden on organizations and does not recognize the reality of how information is disclosed to, and used by, third parties.

For example, an organization may disclose information to a third party for a specific purpose, and as part of that transaction, require the third party to delete the information once it is no longer required for the specified purpose. Under the Government's proposal, if the data subject later corrects or has their information deleted by the organization, the organization must communicate that correction or deletion to all third parties who have been given that information, whether or not the third-party is still

using or possesses the information provided to it.[8] This would make no sense. Add to this the fact that many large organizations will use hundreds or even thousands of third-party service providers, many of whom process some customer information, and the proposed requirement would be exceedingly difficult, if not impossible, to implement. Finally, in many cases, if not most, the information transferred to third parties has no impact on an individual's online reputation; either in subject matter or the manner in which it used.

PART 3: ENHANCING ENFORCEMENT & OVERSIGHT

In its consultation document the Government concludes that the ombudsman model and enforcement tools of PIPEDA are outdated and do not incentivize compliance but, with the exception of one example, offers no evidence that PIPEDA is ineffective in incentivizing compliance. In fact, the number of complaints received by the OPC is declining and the vast majority of them are resolved. For example, when comparing the statistics for 2013 and 2018, the number of complaints accepted by the OPC dropped from 426 to 297, a decrease of 30.3%. Over that same period, the number of complaints resolved through early resolution has increased from 133 to 205, an increase of 54.1%.

These statistics show that the existing powers, including the ability to launch investigations and issue formal findings, to name names when in the public interest, audit the privacy practices of organizations and to take organizations to Federal Court if they fail to uphold their obligations under PIPEDA, have proven to be effective in incentivizing organizations of all sizes to update and continually monitor their privacy practices. New protections and powers, such as mandatory breach notifications and the ability of the OPC to enter into compliance agreements and coordinate enforcement with international counterparts have further enhanced the effectiveness of PIPEDA. No organization wants to be regarded as being inattentive to the privacy rights of its customers. Certainly that is the case for our members, who have made privacy and consumer trust high priorities and continually invest significant resources in their privacy compliance programs.

It is also important to recognize that other enforcement mechanisms and deterrents exist outside of PIPEDA. In addition to the OPC's right to refer a matter to Federal Court, an increasing number of cases are brought directly to the courts by individuals, and through class actions, through claims under tort, breach of contract, negligence, and other courses of action. These claims cover not just commercial uses of personal information, but all matters of uses in both the private and public sector.

When one looks at the downward trend in complaints to the OPC, the early and successful resolution of most of complaints, and the existing toolkit of incentives and deterrents found both inside and outside of PIPEDA, it is not clear that there is an enforcement or incentive problem. And if there is no problem, there is no need to vest the OPC with additional enforcement powers. If there is a problem, it appears to be limited to a narrow set of cases, and as such, any new enforcement powers should be specifically

[8] The transferring organization typically does not track when the intended use is complete and when the information is deleted by the transferee organization.

tailored to address those outlier situations without harming the collaborative and proportionate approach that has been an effective feature of Canada's privacy framework.

The Importance of the Ombudsperson Model

PIPEDA was intentionally based on core principles so that it could adapt to new technologies, processes and society's expectations. This remains one of PIPEDA's core strengths. But there will always be some uncertainty when it comes to applying the principles of PIPEDA to new technologies and processes. The ombudsperson model promotes collaboration between the OPC and organizations that is crucial to ensuring that organizations receive guidance on how to apply PIPEDA's principles to their offerings. As illustrated above, this approach has effectively incentivized compliance with PIPEDA, supported effective complaint resolution, and delivered positive outcomes for consumers.

Providing the OPC with more direct enforcement powers would undermine the collaborative model and cause organizations to be more reluctant to develop and market innovative products and services in Canada. Significant investments must be made in developing and marketing a new product or service with no guarantee that it will be embraced by consumers. If there is uncertainty as to how the principles of PIPEDA apply to the new offering, both organizations and consumers would benefit from a greater focus on helping organizations comply, not on penalizing them.

Enhancing Collaboration

Rather than focusing primarily on enforcement, the Government should be considering ways in which education and collaboration can be improved. For example, PIPEDA should be amended to allow organizations, on a voluntary basis, to reach out to the OPC for an interpretation around new emerging privacy-impacting issues or initiatives, understanding that these opinions would be non-binding on both sides. Opinions would offer comments and recommendations from the OPC that the organization could then consider before launching its new service or other offering. Providing such guidance would also give the OPC visibility into new technologies and business models, which would support and potentially accelerate the OPC's proactive agenda, including the timely issuance of OPC advisories on such emerging issues.

While the organization would not be required to follow all of the recommendations provided by the OPC, an organization's reliance on an OPC opinion should be a factor that must be taken into consideration as part of any future investigation.

Response to Specific Government Enforcement Proposals

Notwithstanding the foregoing, if the Government introduces new enforcement tools, it should ensure that it does so in a fair and balanced manner. For example, any new investigative or enforcement tools must be accompanied by appropriate procedural safeguards that protect the rights of organizations, including transparency with respect to the OPC's decision making process and the right of appeal.

(a) Education/Outreach

We support retaining the OPC's education and awareness mandate. However, as mentioned above, we think the guidance role of the OPC should include the power to issue non-binding advance opinions. In addition, while we support extending the Minister's existing authority to include requesting that the OPC undertake research on themes relevant to the Minister's mandate, we also think that the Minister should have the authority to direct the educational focus of the OPC. Digital literacy is a key element in the protection of personal information and the OPC should play a greater role in educating Canadians about how they can take control of their personal information.

(b) Investigation and Audit

We support providing increased discretion to the Privacy Commissioner on whether to investigate complaints. The early resolution process that currently exists is an example of successful use of discretion.

We do not support increased flexibility for auditing or reviewing organizations for compliance with PIPEDA. The current standard that requires reasonable grounds of there being a contravention should remain. An audit of personal information management practices can be very disruptive to an organization and subjecting an organization to an audit or review where there are no reasonable grounds for conducting one places an unfair burden on organizations.

In addition to preserving the reasonable grounds standard, additional procedural safeguards for the conducting of audits should be introduced. For example, longer notice periods should be prescribed and the OPC should be required to provide a clear indication of the scope of the audit. The scope of the audit should be restricted to the activities for which there are reasonable grounds to think there has been a contravention of the Act, and should not be used as a means to conduct a "fishing expedition". In addition, while the Act currently states that investigations are to be concluded within twelve months, this time limit is not always followed. Prolonged investigations place additional burdens on organizations who must continue to allocate resources to the matter and operate with ongoing uncertainty regarding the OPC's view of practices under review. The Act requires some level of accountability, or relief for the organization, if this time limit is not adhered to.

With respect to exploring options and mechanisms for enabling increased cooperation and information sharing with other enforcement agencies, it is difficult to provide meaningful comments without a specific proposal to consider. Any further exploration of new options and mechanisms should be subject to a separate consultation so that stakeholders can adequately consider specific proposals and their potential impact. Notwithstanding the foregoing, it is clear that any such information sharing arrangements must exclude information that is provided by an organization to an enforcement agency on a confidential basis.

(c) Tools to address non-compliance or offences

i. Order-Making Powers:

While we do not think the OPC requires additional order-making powers, if such additional powers are provided to the OPC they should be limited to those outlined in the consultation document. With respect to cessation orders, such orders should only be made after the conclusion of an investigation and when the Privacy Commissioner's findings are issued. As proposed in the consultation document, cessation orders should only be available where the non-compliance has caused or is likely to cause a risk of harm or significant distress to an individual. All orders must be subject to appeal to a court of competence jurisdiction.

ii. Fines:

As mentioned above, it is our position that when one considers the privacy protections that exist both within PIPEDA and outside PIPEDA, the need for additional deterrence, at least for the vast majority of organizations who are already doing their best to protect consumers' privacy, is questionable. If the current regime for fines is to be extended to include other key provisions of the Act, the requirement under the existing regime that the organization "knowingly" contravened the provision must be preserved. Similarly, the decision to seek fines should be a matter that resides with the Attorney General and the organization must be able to appeal any decision that it contravened the Act.

We also do not agree that the range of fines needs to be "substantially" increased. Increasing fines will only stifle innovation as organizations may be hesitant to innovate for fear that they could inadvertently contravene PIPEDA. A proactive and collaborative approach, such as enabling non-binding advance opinions would be much more efficient and better protect Canadians' personal information. It is also important to note that potential harm to reputation will often act as a greater deterrent than a monetary penalty.

Notwithstanding the foregoing, if fines are increased, they should include a range of fines, from nominal to higher fines that are proportionate to the seriousness of the wrongdoing and its impact. Fines should have specific dollar amounts, or dollar ranges, with the maximum fine only being imposed for the most serious cases; namely intentional contravention that causes significant and demonstrable harm to the consumer. Fines should also not be considered the first and only enforcement tool available. The OPC should first be required to consider warning letters or citations, especially for well-intended companies making genuine attempts to comply with the Act. Similar enforcement models and tools are used by other regulatory bodies in Canada and elsewhere.

Fines should not be based on the revenues of the organization. A contravention by an organization with large revenues may have very little impact or risk of harm to the individual, while a contravention by an organization with little revenue may have significant

impact and the potential to cause significant harm. As we have seen with Canada's anti-spam legislation, commonly referred to as CASL, focusing primarily on an organization's ability to pay can result in fines that are disproportionate to the level of wrongdoing and/or harm inflicted.

In determining what level of fine to impose, if any, the court should be required to consider factors such as the degree of demonstrable harm to the consumer, the organization's history of compliance, whether the violation was negligent or intentional, due diligence exercised by the organization, and the organization's reaction to the initial complaint (e.g. remedial action taken; cooperation with investigation).

iii. Statutory Damages

Statutory damages are typically established for situations where harm is presumed, but may be difficult to assess. Such is not the case with contraventions of PIPEDA, where an organization can breach a provision of the Act without any harm being caused. For example, even in cases where personal information is improperly disclosed, there may be no harm to the data subject if that data is encrypted and indecipherable to the recipient.

It is our view that the courts are best placed to assess the degree of harm and any potential damages that should be awarded. This is currently the case under Section 16 of PIPEDA, as well under the private sector privacy legislation of British Columbia[9] and Alberta.[10]

If, notwithstanding the above, the Government elects to establish statutory damages as a remedy for a breach of PIPEDA, such damages should be limited to violations related to unauthorized disclosure, and fall within a capped dollar range. Moreover, statutory damages should be available only to individuals who can show they were harmed by the non-compliant action or activity (e.g. personal information at issue must be unencrypted or non-redacted). The court should also be required to consider all relevant factors, such as those set out in the discussion of fines above, in determining statutory damages within the specified range and, indeed, should retain the discretion to deny the application of statutory damages where it deems that the circumstances do not warrant their imposition.

iv. Greater Transparency and Right of Appeal

Any additional powers and enforcement tools for the OPC should come with additional responsibilities. First, it is vital that the OPC be made more transparent in its methods, investigations, and determinations. For example, the OPC should be required to publish all of its findings of investigations, in a timely manner, so that organizations have a full understanding of OPC's decisions. The OPC should also be required to publish a yearly report summarizing in sufficient detail the frequency in which it has exercised each of its

[9] *Personal Information Protection Act*, s.57
[10] *Personal Information Protection Act*, s.60

order making and enforcement powers. As well, it is important that the length of time for the OPC to conclude an investigation be restricted and the OPC be held accountable to that timeline. Finally, organizations should have the right to appeal OPC orders and findings to the Federal Court.

(d) Advance/Proactive Advice

As discussed in "Enhancing Collaboration" above, we strongly recommend that PIPEDA be amended to authorize the OPC to provide non-binding advance opinions.

PART 4: AREAS OF ONGOING ASSESSMENT

Clarity of Obligations

The consultation document states that PIPEDA is difficult to understand and that the Government is proposing to redraft the law in a manner that is easier for all to understand. We urge the Government to exercise caution with respect to rewriting PIPEDA. First, we are not aware of any evidence that PIPEDA is more difficult to understand than any other legislation in Canada. Any uncertainty in its application is due to it being principles-based and not prescriptive, which as discussed, is a key intended feature of the Act. These uncertainties are clarified over time through findings and guidance issued by the Privacy Commissioner and decisions by the courts.

Organizations have spent considerable time and expense developing their policies and processes to comply with the requirements of PIPEDA as it is written. Even if the intent of the rewrite is not to change any rights or obligations, any change in language or structure will inevitability result in questions of interpretation and meaning. This will create new and unnecessary uncertainty for organizations and individuals, and result in precious resources of the OPC and all other stakeholders being spent on trying to resolve these questions.

[End of Document]