

CMA Response to Government of Canada's Proposals to Modernize the Personal Information Protection and Electronic Documents Act

December 19, 2019

Executive Summary

As the voice of the marketing profession, the Canadian Marketing Association (CMA) is pleased to respond to the May 2019 proposals by Innovation, Science and Economic Development Canada (ISED) to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA).

PIPEDA, now and into the future, is based on a balance between embracing the enormous social and economic benefits of data use for Canadians while protecting their individual right to privacy. The CMA is providing recommendations to preserve this important balance under a reformed law, in six key areas:

1. PIPEDA – General Structure: A reformed law must preserve PIPEDA’s strengths as principles-based, technology neutral and not overly prescriptive. The nuances – the respect for context, individuals’ expectations and overall emphasis on reasonableness, must remain. In considering the adoption of certain aspects of other international frameworks like GDPR, each aspect should be assessed based on its merit in a Canadian context. As we await a reformed law, we should act now to make better use of existing options under the current law.

2. Consent and Transparency: The Canadian model of express and implied consent is a central underpinning of PIPEDA that should be preserved. However, we must do more to focus consent on situations that are not reasonably expected, and where individuals have a meaningful choice. To do so, ISED must further develop and implement exemptions to consent for standard business practices, publicly available information and de-identified data.

3. Third-Party Processing: The CMA recommends ISED preserve the current model, which provides adequate privacy protection in the context of third-party data flows, including across borders, as outlined in the August 2019 [CMA Response to the OPC’s Consultation on Transfers for Processing](#). Further clarity is required in the Act regarding the obligations of service providers processing personal information on behalf of clients, necessitated by a recent OPC [report of findings](#).

4. Codes and Certifications: A co-regulatory model in which government regulation and industry self-regulation work in tandem is important to ensure regulatory efficiency. A reformed law should acknowledge and incentivize self-regulated standards and codes, such as the CMA [Code of Ethics & Standards of Practice](#), as well as formally recognized certifications and codes involving the Standards Council of Canada and approved third-party accreditors.

5. Enforcement: To ensure an efficient Canadian enforcement model that permits collaboration and trust between the OPC and business, while cracking down on bad actors, we recommend the following:

- A. Clearer and more balanced policy direction for the OPC to ensure the Act is interpreted and applied by the OPC with a balanced view
- B. Broader stakeholder collaboration by the OPC to inform its initiatives, including a greater business voice on the External Advisory Committee

- C. New procedural safeguards regarding OPC guidance to ensure guidance contributes to the balanced environment intended by the legislation
- D. Limited sharing of sensitive information about businesses with other agencies such as the Competition Bureau, except for prescribed purposes
- E. Additional procedural safeguards for audit power based on the standard of reasonable grounds there is a contravention of PIPEDA
- F. Limited additional tools and fines to address offences and non-compliance, in order to better leverage existing mechanisms, and to ensure proportionality and fairness in punitive actions

6. Data Mobility: The proposed right to data mobility creates serious new privacy risks, and its wider impacts on Canada's unique economy are not well-understood. Data mobility should only be achieved through a phased-in approach that allows for the implementation of sector-specific frameworks developed in consultation with industry. The scope of ported data should be carefully limited, strong authentication should be in place, and organizations mandated to port data should have limited liability.

Contents

Executive Summary	1
Introduction and Context	4
1. PIPEDA – General Structure	5
2. Consent and Transparency	6
2.1 Exemptions to Consent.....	7
A. Standard business practices.....	7
B. Publicly available information.....	8
C. De-identified data	8
3. Third-Party Processing.....	9
4. Codes and Certifications	10
A. Self-regulated standards and codes	10
B. Formally recognized certifications and codes	11
5. Enforcement.....	12
A. Clearer and more balanced policy direction for the OPC	12
B. Broader stakeholder collaboration	12
C. New procedural safeguards regarding OPC guidance	13
D. Limited sharing with other agencies	13
E. Additional procedural safeguards for audit power.....	13
F. Limited additional tools to address offences and non-compliance	13
6. Data Mobility	14
A. The need to limit the scope of ported data.....	15
B. The importance of ensuring fair accountability	16

Introduction and Context

The Canadian Marketing Association (CMA) appreciates the opportunity to respond to the May 2019 proposals by Innovation, Science and Economic Development Canada (ISED) to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA).

The CMA is the voice of the Canadian marketing profession. We represent more than 400 corporate, not-for-profit, public, and post-secondary members, including Canada's most prestigious brands. Our community also includes creative, media, and PR agencies, research firms, management consulting firms, technology companies and other suppliers to the marketing community. We are committed to helping Canadian organizations maintain high standards of conduct and transparency through our mandatory [Code of Ethics & Standards of Practice](#), and our privacy and data protection resources for marketers and consumers. As the recognized longstanding leader in marketing self-regulation, we strive to ensure an environment where consumers are protected and businesses can thrive.

We agree with ISED's goal of ensuring that PIPEDA supports the principles outlined in Canada's Digital Charter and provides the foundation for achieving a strong and vibrant digital economy for Canada. We agree that PIPEDA must support an inclusive digital economy that provides a level playing field, fairness of opportunity, enhanced security and privacy, predictability for business, and international competitiveness.

Canada's marketing community highly values its customers, whose loyalty and trust provides the foundation for business success. Most Canadian organizations recognize that strong privacy and data protection practices serve as a competitive advantage and customer retention strategy, and they work hard to protect the privacy interests of the individuals they serve.

In our modern digital economy, consumers increasingly expect organizations to deliver the intuitive products and services they want and need. In a recent survey by Ipsos Canada, 50% of consumers indicated a desire to see internet advertising that is relevant and targeted to them, despite having concerns about the security of their personal information. Similarly, a 2018 research study [Data Privacy – What the Canadian consumer really thinks](#) found that a strong majority of Canadian consumers (76%) are willing to share personal data in order to receive benefits, as long as the data is properly protected. Public policy must ensure a balanced privacy framework that supports these interests.

The spirit of PIPEDA, since its inception and into the future, is based on a balance between embracing the enormous social and economic benefits of data use for Canadians while protecting their individual right to privacy. We are encouraged that this important balance is prominently reflected in ISED's discussion paper.

The CMA's response to the discussion paper provides recommendations for a reformed law in six key areas.

- PIPEDA – General Structure
- Consent and Transparency
- Third-Party Processing
- Codes and Certifications
- Enforcement
- Data Mobility

1. PIPEDA – General Structure

The data economy provides significant benefits for individuals. Technological advancements have provided Canadian organizations with the agility to offer relevant, useful offerings to consumers who want them. Many of the online services Canadian consumers have come to rely on are supported, at least to some extent, by revenue that relies on interest-based advertising and data collection techniques.

The ability of organizations to collect, use and disclose personal information is key to providing value to consumers, and to ensuring Canadian innovation and competitiveness. In order to meet the government's commitment to support the middle class by growing the economy, PIPEDA needs to remain flexible in the face of rapidly evolving technologies, business models and consumer privacy expectations.

While some aspects of PIPEDA are due for an update, it is important to recognize that this law has many strengths that have stood the test of time. It is built on solid principles that provide flexibility for specific applications, and its framework is understandable and achievable for non-specialists. Many of its features are regarded to provide materially better privacy outcomes for individuals than newer and more prescriptive laws in other jurisdictions. This includes the EU's GDPR which in many respects remains unproven, and has created a staggering regulatory burden for government and business.

We appreciate that PIPEDA is being reformed with a view to ensuring reasonable interoperability with privacy frameworks in other jurisdictions. With regards to GDPR adequacy status, reducing friction in data transfers is a worthwhile objective. However, in considering the adoption of certain aspects of GDPR, we must assess each based on its merit in a Canadian context, with the goal being compatible privacy outcomes as opposed to compatible legislative requirements.

A reformed law must preserve PIPEDA's strengths as principles-based, technology neutral and not overly prescriptive. The nuances – the respect for context, individuals' expectations and overall emphasis on reasonableness, must remain.

As a reform process of this magnitude takes time, we have an opportunity to make better use of existing options under the current law, which provides the necessary tools to address many of the challenges that new technology poses to privacy. This includes the opportunity for ISED and the OPC to collaborate with industry on new guidelines and standards on topics such as de-identification and standard business practices.

2. Consent and Transparency

We welcome the opportunity that this review provides to tweak PIPEDA's consent model to better serve Canadian consumers. As business models evolve in step with technological advancement, including big data analytics and IoT, it is more important than ever to ensure we are obtaining meaningful consent. An overreliance on consent does not provide consumers with meaningful privacy protection, rather it contributes to "consent fatigue", causing consumers to be less likely to carefully review notices and make informed decisions. It is imperative that the requirement for consent be better focussed on the things that matter most.

A strength of the Canadian consent model is that organizations have the operational choice of whether to seek express or implied consent. This ensures the appropriate form of consent is dependant on the context and the reasonable expectations of the individual. And although we have learned not to place too much emphasis on consent alone, it is a central underpinning of PIPEDA. Paired with other PIPEDA obligations, including fundamental openness and accountability obligations, obtaining meaningful consent helps empower individuals.

Meaningful consent cannot be achieved without transparency. By being open and transparent, organizations breathe life into the consent requirement, enabling Canadians to make more informed choices about their personal information. Building on the OPC's Guidelines for Meaningful Consent, the [CMA Guide to Transparency for Consumers](#) helps organizations provide clear, user-friendly information to consumers about how their personal information is collected, used and shared.

The CMA supports ISED's proposal to require organizations to provide individuals with the information they need to make informed decisions, including on the intended use of the information and the nature of third parties with which information will be shared. However, disclosure requirements that are too prescriptive, such as in the proposed requirement for organizations to include specific and standardized information or language in their privacy notices, will not result in better consumer understanding. Given the great variety of business models and data uses, organizations need the flexibility to determine how best to communicate with individuals in an understandable way, taking into account the context, target audience and actual risks.

To assist individuals in better understanding how decisions are made about them, we support the requirement for organizations to share summary information with individuals about the use of automated decision-making, the factors involved in the decision and where the decision is impactful, as long as it does not require organizations to reveal any confidential or proprietary commercial information, algorithms or procedures.

The Act should not have a specific definition of, and protections for, "sensitive information". Under PIPEDA, a contextual analysis is required prior to making a determination about sensitivity of data, as well as a determination of the scope of harm. These determinations must be based on the facts of the circumstances, so organizations avoid broad statements of acceptable or unacceptable use in their privacy policies or notices.

While certain types of data, such as financial or health information, may at first glance seem to be sensitive, this data could be used in a way that could make it not as sensitive as initially envisioned. In the same way, fairly routine personal information could be sensitive in certain contexts.

We note that the mandate letter that the Prime Minister sent to the Minister of Innovation, Science and Industry this month refers to the development of a National Advertising Registry where companies would have to report with whom individuals' data is being shared or sold, with the ability to withdraw consent at any time. We are interested in learning more about the intent and scope of this initiative, the additional value that it would provide beyond existing transparency and consent obligations, and how it could be implemented efficiently through existing platforms, such as the Digital Advertising Alliance of Canada's AdChoices program. The CMA looks forward to being involved in further discussions on this initiative.

2.1 Exemptions to Consent

The current over-reliance on consent does a disservice to individuals and potentially exposes them to harm. We must do more to focus consent on situations that are not reasonably expected, and where individuals have a meaningful choice. To do so, ISED must consider areas for which consent may not be necessary or even appropriate, such as in the below areas.

A. Standard business practices

The processing of data for standard business practices can already be done through the "legitimate purpose" section in 4.3.3 and the "reasonable expectations" section in 4.3.5 of PIPEDA, relying on express or implied consent. To achieve the goal of focussing consent on things that matter most, we support the proposed exemption to consent for processing personal information for standard business practices.

Standard business practices should be limited to reasonable and legitimate activities that are necessary to deliver the products and services the consumer requests. Seeking consent in these cases is not meaningful because individuals interested in a product or service would not have a real option to opt out of these practices. Organizations relying on this exemption must be transparent about their standard business practices by outlining them in a privacy policy that is readily available to individuals.

The activities captured by such a provision must not be too prescribed given the varying nature of products and services requested by consumers, and to leave room for innovation. For example, location tracking is essential to the delivery of wireless services but may not be critical to the delivery of another service.

This exemption could be bolstered with accompanying guidance on the scope of standard business activities, developed in collaboration with industry.

This recommendation is not to be confused with the ‘legitimate interests’ grounds for processing under GDPR, which permits processing for purposes (even outside the original purposes) subject to a balancing test that indicates that the interests and fundamental rights and freedoms of the individual are not overridden. The GDPR approach has proven to be challenging because it is impossible for individual organizations to balance their own well-defined legitimate interests against the diffuse and varied interests of individuals.

B. Publicly available information

Consumers should be the ones to decide whether or not their personal information can be used publicly, even if it appears to be openly available in the public domain.

The PIPEDA regime includes the Regulations Specifying Publicly Available Information, which are outside of the knowledge and consent requirements. “Publicly available” information is defined as information appearing in telephone directories, professional or business directories, government registry information, and records of quasi-judicial bodies that are available to the public, as well as information published in a magazine, book or newspaper that is available to the public and where the individual has provided the information. Generally speaking, no consent is required as long as the collection, use and disclosure of such information relates directly to the purposes for which it was made publicly available. All personal information that is not “publicly available” as defined above, or which is not covered by the other exceptions, requires consent.

The term “publicly available information” has led to some confusion because the definition did not foresee the way information would be shared in the online environment.

The decision about what information is public should reside with individuals. The best way to achieve this is by enabling information to be used on the condition that the individual has provided his/her consent or other authority for the information to be shared and consumed publicly, i.e. online records where individuals have provided the information and made a clear choice that it should be consumed publicly. This is a more reasonable and effective approach than prescribing a list as was done in the past.

The Act should include some restrictions on use, for example to ensure the purpose is compatible with those reasons that justify its presence in the source, and to ensure its use is not clearly against the interest of the individual. Organizations using publicly available information without consent will continue to be subject to all other PIPEDA obligations, including the reasonable person test.

C. De-identified data

Data de-identification provides a significant opportunity for organizations to protect individual privacy, while permitting the smart use of data. The CMA supports the proposal to add a definition of de-identified information to the Act.

Given the critical importance of de-identification to security safeguarding efforts and to innovation more broadly, and in order to remove any legal uncertainty, the Act should clarify that consent is not required to de-identify data, or for its collection, use and disclosure, as long as de-identification standards are met.

These standards should be acknowledged in the Act, and should include benchmarks for technical and administrative procedures and monitoring, as well as proper risk assessments and protocols. Accountability chains are also important to guard against the technical risk of re-identification. The Act should clarify parameters of accountability around the onward transfers of de-identified data, and should emphasize the need for contractual provisions between organizations to be in place to address re-identification.

At present, the meaning and methodology of de-identification varies across organizations. To ensure a level playing field and provide clarity, it is important for organizations to have a set of common standards by which they can demonstrate whether they took all reasonable steps at the time to de-identify personal information and mitigate the risk of re-identification. Consistent with the reasonable safeguards principle, the standard of de-identification and ongoing monitoring should fit the purpose/activity. The context and data-use activity is more relevant than the type of data.

Robust de-identification, in and of itself, poses no risk of harm and has no negative impact on the individual to whom the PI originally related. Not only is this a useful safeguarding technique, but de-identification is also one of the most privacy-protective mechanisms available for organizations to engage in data analytics and innovation in the digital economy.

As technology evolves, the requirements for robust de-identification must also evolve to keep up with the times. This may mean an 'evergreen' approach to OPC guidance, and other formalized standards around deidentification. These standards should be developed in consultation with industry, and could result in a formal certification involving a third-party accreditor approved by the Standards Council of Canada (see section on Codes and Certifications).

3. Third-Party Processing

The CMA recommends ISED preserve the current model, which provides adequate privacy protection in the context of third-party data flows, including across borders, as outlined in the August 2019 [CMA Response to the OPC's Consultation on Transfers for Processing](#).

Any requirement for additional consent would contribute to consumer consent fatigue, disruptions in service for consumers, significant operational consequences for organizations relying on third-party data processing (including non-profits and others providing critical services to Canadians), and a lack of interoperability with other privacy frameworks. Given the nature of data flows, consent is not the most effective form of responsible data governance and it offers no meaningful additional privacy protection. In many cases, consent would be illusory as the requirement would not mean individuals have any choice at all but to walk away. A customer who is very interested in a product or service is not likely to make that choice. In fact, it works against our common goal of obtaining meaningful consent to the benefit of consumers.

PIPEDA's openness and accountability requirements, including providing notice and using contractual or other means to provide a comparable level of privacy protection when data is transferred, are sufficiently strong in the context of transfers for processing. A future law need not require demonstrable accountability by giving a public authority, such as the OPC, additional powers to approve standard contractual clauses before they are implemented and, once they are adopted, proactively reviews their implementation. Issues should be reviewed only upon complaint to the OPC. The proposed drafting of such clauses, similar to the GDPR's standard contractual clauses, would depart from PIPEDA's balanced approach.

Further clarity is required in the Act regarding the obligations of service providers processing personal information on behalf of clients. In a recent [report of findings](#), the OPC diverges from the common working assumption that Canadian companies that collect, use and disclose personal information on behalf of clients are subject to the laws that govern their clients' activities. The recent decision creates an obligation on Canadian processors to ascertain whether data controllers obtained valid consent under PIPEDA even when those controllers are located outside of Canada dealing with the information of non-Canadians (and in this case used a legitimate grounds for processing besides consent under the GDPR). Such an obligation would create significant barriers for Canadian businesses to compete at home and abroad. There is no express legal basis for this decision under the current law, and clarification under a new law is critical.

4. Codes and Certifications

All sectors have a role to play to protect the privacy of Canadians. A co-regulatory model in which government regulation and industry self-regulation work in tandem is important to ensure regulatory efficiency. There is no one-size-fits all approach to privacy compliance; much depends on each sector and the types of information being collected, used and shared. Now and into the future, codes, certifications and other standards will play an important role in supplementing privacy legislation.

Standards could be either self-regulated or formally recognized by government, as outlined below. All schemes should be voluntary, recognizing the varying degrees of data processing operations among organizations, and ensuring organizations with limited resources are not unduly impacted.

A. Self-regulated standards and codes

Self-regulated standards and codes should be referenced in the Act as tools that can help organizations ensure compliance with PIPEDA and help demonstrate accountability in the event of an investigation by the OPC. Industry should be encouraged to develop and follow these standards and codes.

Industry and professional self-regulated codes of practice are practical and efficient tools to steer privacy compliance. For example, the CMA [Code of Ethics & Standards of Practice](#) is a comprehensive code that establishes and promotes high standards for the conduct of marketing in Canada and strengthens marketers' knowledge of compliance requirements.

Section J of the Code addresses the protection of personal privacy. The Code is reviewed and updated regularly. Upon joining the CMA and upon membership renewal each year, all CMA members agree to comply with the Code.

These instruments operate in a legal environment that includes consumer, competition, health and safety, labour and environmental legislation and regulations, and contract and tort law. For example, if an organization purported to be in compliance with a code but was not, it could be subject to the Competition Act for misleading advertising. Failure to adhere also has a reputational impact.

The OPC should investigate and audit only where complaints occur that haven't been resolved internally, or where there isn't an adequate internal complaints process in place. When an organization cannot demonstrate compliance, it would risk falling under general compliance rules enforced by the OPC.

B. Formally recognized certifications and codes

The Act should further incentivize the use of certifications and codes as tools for privacy compliance and accountability through an allowance in the Act for the formal recognition of some certifications and codes by ISED and/or the OPC, with oversight from select third-party accrediting bodies approved by the Standards Council of Canada.

The Act should not prescribe a list of areas that warrant standards but rather a framework to allow existing bodies to develop schemes for approval in response to market needs. They could be in relation to certain provisions of the Act only or a broad assessment of privacy (for example for a sector or industry).

Borrowing from the UK model, proposals submitted for approval could identify the data processing operations covered, the categories of organizations that it applies to, and the privacy issues are that it intends to address. Proposals should be informed by adequate consultation and could be ranked against standard admissibility criteria. Once an organization is deemed to be in compliance with a certification or code by a third-party accreditor, it could be considered to meet the requirements for a set time period (e.g., three years), after which its adherence could be renewed if the conditions and requirements are still met. The Standards Council of Canada has a thorough development and review process for accreditation standards; its role should be leveraged and maximized.

The OPC could have a general obligation to consider adherence to formally recognized codes and certifications in making decisions about whether to investigate. Compliance should also be a factor in determining due diligence in the context of an OPC investigation, prosecution by the Auditor General or court action. The OPC should not have authority to periodically review an organization's adherence to a scheme, and this would properly fall with the third-party accrediting body. The accrediting body could have a duty to report incidences where an organization's compliance is revoked for non-compliance.

5. Enforcement

Despite a few high-profile cases, the OPC has seen a high level of voluntary compliance from Canadian organizations. It is important to ensure that changes to the Canadian enforcement and oversight model translate to better privacy outcomes for individuals. The current Canadian enforcement model, which is a combination of PIPEDA, provincial laws and common law/civil code, has unique strengths that make it effective.

Through PIPEDA, the Commissioner as Ombudsman can constructively engage with businesses to address privacy issues. The focus on resolving complaints through negotiation and persuasion continues to work very well and is bolstered by mediation and conciliation if appropriate. If voluntary co-operation is not forthcoming, the OPC has the power to summon witnesses, administer oaths and compel the production of evidence. Further, the OPC has the power to enter into compliance agreements if necessary, or to take matters to the Federal Court and seek a court order to rectify situations that remain unresolved.

Additionally, the ombudsman model permits the OPC to protect and promote the privacy rights of individuals through positive and proactive engagement with industry associations and organizations seeking guidance on compliance and emerging privacy issues. Organizations are more cautious and less likely to consult in a cooperative way with a regulator that has the direct power to impose monetary penalties or issue orders against them.

There is an inevitable degree of uncertainty when applying privacy principles to new technologies. A flexible and collaborative model is required to create conditions under which OPC and organizations can work together to find the right solutions.

To ensure a balanced and efficient Canadian enforcement model, we recommend the following:

A. Clearer and more balanced policy direction for the OPC

PIPEDA has the dual objective of supporting both economic and privacy interests. The revised legislation must explicitly state this objective as a lens for application and interpretation of the Act, including by the OPC. As an agent of Parliament without policymaking authority, the OPC has a duty to take into account the wider policy objectives of government to encourage innovation and economic development. On an ongoing basis, ISED should have the ability to issue specific policy directions that require the OPC to consider the above objective as it fulfills its duties.

B. Broader stakeholder collaboration

Most Canadian businesses and other organizations vigorously pursue all reasonable steps to serve consumers well, including protecting their privacy. Canadians are best served when the private and public sectors work collaboratively to achieve PIPEDA's dual objective.

To ensure this collaboration, the OPC should deepen its consultation with stakeholders to inform guidance, potential codes and certification schemes, research needs and other initiatives. A greater business voice at the OPC, including through more diverse business representation on the External Advisory Committee, will contribute to a balanced environment that serves businesses and their customers.

C. New procedural safeguards regarding OPC guidance

Reformed legislation should include new procedural safeguards for OPC guidance to ensure it contributes to the balanced environment intended by the legislation, and that no unintended consequences will result from the guidance. One option is an amendment to the Federal Court Act to create a statutory ability to appeal to the Court a legal interpretation in a non-binding guidance document (e.g. transfer for processing is a disclosure not a use, s. 9 of CASL). There could also be an ability for ISED to review OPC guidance through a right for parties to seek Cabinet appeal.

More transparency would also contribute to a better understanding of decisions being made. The OPC should publish all findings and other evidence used to provide guidance to business for greater certainty and understanding.

D. Limited sharing with other agencies

Any additional authority for the OPC to share information with other regulators (e.g. the Competition Bureau) should be limited to a set of specific prescribed purposes, similar to the requirement in CASL s. 58.

E. Additional procedural safeguards for audit power

The OPC currently has broad audit rights. It is essential for PIPEDA to include additional procedural safeguards for existing audit powers. There must be appropriate notice for audits and a clear indication of the focus of the audit. All audits must be undertaken based on the current standard of reasonable grounds that there is a contravention of PIPEDA. Any proposal to expand grounds for investigation should include expanded grounds for not investigating, or for discontinuing the investigation of complaints, such as in the above example of adherence to a formally recognized code or certification.

F. Limited additional tools to address offences and non-compliance

Most Canadian organizations want to protect the trust and privacy interests of the consumers they serve. We support enhanced enforcement measures to crack down on bad actors. This can be achieved by strengthening and leveraging the current enforcement model.

Any new cessation or records preservation orders for the OPC must be limited to egregious cases with a risk of imminent harm, for example the ongoing posting of personal data online after a data breach, and not applied in situations where there are differences of interpretation carried out in good faith.

The OPC's enforcement response should be triggered at the conclusion of an investigation, and should follow a staged approach, issuing warnings before orders, in order to give well-intentioned companies an opportunity to rectify the issues at hand. Severe enforcement tools should be used only when lesser tools have been ineffective or the potential harm is too great. In all cases, there must be an appeal process.

We do not support a model in which AMPs are issued by the OPC, as this would further undermine the collaborative model described above. Any new offences should be carefully considered for prosecution by the Auditor General, not the OPC, making best use of existing provisions and infrastructure. To date, the OPC has not yet utilized its ability to refer a matter to the Auditor General for prosecution. There should be consideration of a greater range of offences for the Auditor General to prosecute. If more general non-compliance issues are included in the list of offences, they should be limited to more egregious cases with intent and gross negligence, such as in the case of intentionally insufficient safeguards or deliberate re-identification.

ISED should take a cautionary approach when considering extending the current fine amount of \$100K "per contravention" of PIPEDA, which serves as a real deterrent to Canadian businesses. Fines levied on a "per individual" basis or on a "% of global revenues" basis could lead to a significant aggregate dollar amount out of touch with the actual impact of the offence. The courts must have specific factors to consider when applying fines, using a proportionate approach that considers the nature of the violation and the size and data processing activities of the organization that committed the violation. We must also recognize the impact of additional deterrents outside of PIPEDA through private claims in tort and contract law.

We oppose the introduction of statutory damages, as they are usually reserved for situations where harm is presumed but difficult to assess, and would create conditions that promote potentially opportunistic class actions. With PIPEDA, there can be breaches without harm, for example if personal information that is encrypted is breached. Courts are best placed to assess damages, as they have been doing.

Penalties should serve as a sufficient incentive to deter businesses that might not otherwise comply but they should also be designed so as not to create a litigious environment that doesn't serve to improve the privacy of consumers.

6. Data Mobility

The proposed right to data mobility would provide 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 primary objective of data mobility is two-pronged: to provide greater individual control over data and to encourage competition in the marketplace. Although data mobility is intended to enhance consumer control and choice, it creates serious new risks for consumers with regards

to cybersecurity, privacy and confidentiality. In addition, its wider impacts on Canada's unique economy are not well-understood, and more research must be done to understand its effects.

To ensure that this new right does not create unintended consequences that hamper Canada's economic well-being, other bodies, such as the Competition Bureau, should have a significant role in the research and development of this concept in a Canadian context. This is more than a privacy issue, and the corresponding reform of other statutes may be warranted.

For the right to data mobility to be effective, it must be meaningful for consumers and not overly burdensome or costly for organizations (and by extension consumers). If the right to data mobility is ultimately pursued, it could only be achieved through a phased-in approach that allows for the development and implementation of sector-specific frameworks. We have learned from the GDPR model, which creates a sweeping data portability right but provides little clarity on implementation, that a more practical approach is required.

Sector-specific frameworks would need to be developed in consultation with industry to reflect the current practicalities and risks in each affected industry, and could be implemented through regulation. These frameworks must consider important economic, technical, authentication, security and operational issues. Other regulators beyond the OPC should be involved in the enforcement of such frameworks, with the OPC overseeing issues related only to privacy compliance.

Other important considerations include:

A. The need to limit the scope of ported data

When it comes to providing data directly to an individual, this is an extension of the current right to access under PIPEDA, which in its current form goes a long way to support consumer control. Individuals already have a right to access the personal information that an organization holds about them, to challenge its accuracy and completeness, and to have that information amended as appropriate. For organization-to-organization transfers, the right to data mobility must be considered separately from the right to access, and the scope of data should not necessarily include all that is afforded under a typical access request.

Ported data must be limited to personal information provided by the individual. Other types of data should generally be excluded, such as data that may be proprietary, about a third party (e.g. an individual's contact list), or not considered personal information. This includes derived data (insights, observed data) and de-identified data. Some of the exempted data would continue to be subject to the normal access request process, such as, for example, call notes and complaints. Sector frameworks could provide clarity on the scope of data appropriate for the objective of data mobility, including limited data related to commercial transactions. With respect to higher risk or more sensitive data, it would be advisable to limit the data fields that can be ported and strengthen authentication requirements.

To avoid unnecessary disruption to standard business practices, the right to data mobility should not automatically include an onus on an organization to delete ported data. Organizations must be permitted to follow standard policies and procedures around retention.

In terms of format, ported data must be limited to digital data in technology neutral formats, in other words, a “standardized digital format, where such a format exists,” and not physical records to which normal access rights may apply. The Act must allow for solutions to emerge in each sector, and to evolve over time. Regulatory frameworks will need to be reviewed on a periodic basis to reflect technological and other advancements. As advancements occur, the scope of ported data could evolve accordingly.

Consideration should be given to ensuring that these rules do not create barriers for SMEs, working against the original intent of greater competition.

B. The importance of ensuring fair accountability

When organizations are obligated to respond to individuals’ requests for their own data, strong authentication must be in place to guard against fraudulent requests. Organization-to-organization mobility must be conditional on the request being made by the individual (and not just the third-party organization), and on there being an adequate sector-specific regulatory framework in place. Bulk requests from third parties must be prohibited. In particular, the Act should ensure organizations cannot automate requests, or attempt to bury consent for the sharing or obtaining of ported information in contracts.

The introduction of the right to data mobility will attract third-party providers that must be properly assessed, especially if they operate internationally and can more easily attempt to evade OPC enforcement. Parties receiving ported information must be accountable to consumers, and should be prepared to adequately protect their personal information.

An exclusion of liability must be in place when an organization is mandated to port data to a third party that it wouldn’t choose to port to. The responsibilities of the originating organization must be limited to confirming that the request is from the individual (i.e. not fraudulent) and the safe transfer of the data. The originating organization must not be held responsible if the recipient organization falls short of its safeguarding obligations and other requirements under a sector-specific framework, leading to misuse of the data. Additionally, organizations transferring ported data should not be responsible for educating recipients on their responsibilities.

For questions or comments regarding this submission, please contact:

Sara Clodman
VP, Public Affairs and Thought Leadership
sclodman@theCMA.ca

Fiona Wilson
Director, Government Relations
fwilson@theCMA.ca