Innovation Science and Economic Development

Strengthening Privacy for the Digital Age: Proposals to modernize the Personal Information Protection and Electronic Documents Act

Submission from Cybera Inc

CYBERA
Calgary Office: Suite 200, 3512 - 33 St NW, Calgary, AB T2N 2A6 T: 403-210-5333
Edmonton Office: Suite 10065 Jasper Ave NW, Edmonton AB T5J 2A6
@cybera info@cybera.ca www.cybera.ca

Introduction

Cybera is the not-for-profit, technology-neutral organization responsible for driving Alberta's economic growth through the use of digital technology.. One of its core roles is the operation of Alberta's Research and Education Network, called CyberaNet. This is the dedicated network for unmetered, not-for-profit traffic used by Alberta's schools, post-secondary institutions, and business incubators to enable research, innovation, and enterprise.

Cybera is guided by a strategic leadership team and is home to some of the world's top cloud and networking experts, who work with the public sector to build cloud infrastructure, data storage, and advanced networking solutions. In addition, the organization is committed to robust advocacy for the rights of all Canadians to engage in the modern digital economy, unencumbered by any and all barriers, including those that are social, financial or geographic in nature.

Cybera welcomes the invitation from Innovation, Science and Economic Development (ISED) to provide comments on its proposed measures to modernize the Personal Information Protection and Electronic Documents Act (PIPEDA). The free flow of data between individuals, organizations, and processors brings significant benefits to the fields of commerce, research, education, and innovation. This significance will only grow with time. However, as ISED is aware, the increasing reliance on individuals' personal data for commercial activity requires new legal, legislative, and regulatory measures to ensure the protection of personal information.

A robust legislative regime, coupled with effective exercise of regulatory authority, is essential to address modern challenges with respect to personal data protection. In the discussion paper provided by ISED to which this document is a response, ISED has proposed a number of key approaches that provide a solid overarching framework to the relevant issues. Cybera supports ISED's overarching intention to strike a balance between implied and meaningful consent, to avoid cumbersome consent requirements that will result in "consent fatigue", and to further investigate innovative approaches to modernize privacy protection. Furthermore, Cybera commends ISED for prioritizing privacy issues that pertain to new technologies, such as, artificial intelligence and machine learning.

Part 1 - Enhancing Individuals' Control

A. Possible Options - Consent and Transparency

1. Cybera is of the view that the current notice and consent regime — and the fundamental legislative and regulatory principles underpinning modern privacy protection — have become redundant and in need of significant change. In the current context, purpose specification, use limitation, and even the meaning of 'privacy' as defined in PIPEDA, are in need of re-examination, among other issues.

2. It is important to note, however, that understanding “data protection” and “data use” as equally important yet contradictory interests is an important overarching framework that should not be abandoned. However, the volume and complexity of modern data uses will complicate this balance. As such, this submission will make the argument that modern privacy law will need to be based on a risk-management — rather than a harm reduction — approach.

3. The quantity of data, and the complexity of the uses of that data, necesitate a new framework to manage this dynamic in a manner that both allows for novel and beneficial uses of data, while meaningfully protecting the privacy of data subjects. The efficacy of GDPR has been questioned on these grounds, and Cybera is of the view that the European approach to data protection may not be appropriate in the Canadian context.[1] For example, there is an indication that the consent requirements of GDPR have led some tech companies to withdraw from the European market altogether, and that data subjects have become increasingly overwhelmed by consent requirements.[2] In addition, an International Association of Privacy Professionals survey found that 20% of European companies deemed it “impossible” for them to become fully GDPR compliant.[3]

4. As such, Cybera supports ISED’s balanced approach to dealing with matters of consent and transparency as they pertain to collections, uses, and disclosures of personal information. “Consent fatigue” should be considered a serious concern, as should the possibility that overbearing consent requirements may erode consumer vigilance in the long-term. A 2008 study in the USA found that an individual would need roughly 244 hours — roughly 30 working days — to fully read the privacy policies stemming from the websites they visit.[4] It is almost certain that this number is higher today, considering the growth in internet usage. As such, it is simply not possible for an individual to read and comprehend this much technical information, thereby calling into question the relevance of an “opt-in” regulatory regime in the modern context.

5. Consent, as it pertains to personal information, can only be understood in relation to the totality of an individual’s data usages, which, for the majority of people, means that meaningful consent cannot be secured in all circumstances. This will instead necesitate a contextual approach to requiring consent for data uses. It will also require a regulatory approach that can allow regulators to determine the degree of sensitivity of different types of data, and how much consent and/or transparency should therefore be required.

---

[1] https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html
[2] https://martechtoday.com/drawbridge-pulls-ad-business-europe-ahead-gdpr-212175
[3] https://www.exonar.com/2018/12/04/the-era-of-the-technology-enabled-dpo-has-begun/
[4] https://heinonline.org/HOL/LandingPage?handle=hein.journals/isjlpsoc4&div=27&id=&page=

6. With respect to de-identification of data, opinions are divided as to its effectiveness. While there has been much media attention given to several large linkage attacks, a more holistic understanding of the effectiveness of de-identified information shows that it *can* be successful. For example, in a US Department of Health and Human Services study, data analysts were only able to re-identify two data subjects from a dataset of 15,000, or 0.013%.[5]

7. In addition, PIPEDA is currently far behind similar legislation in other developed jurisdictions in having no clear framework with which to understand de-identified data. Instead, the definition of "de-identified" must be implied through the definition of "personal information" as "information about an identifiable individual".[6] This definition requires further clarification as to the proper meaning of "about" and "identifiable."

8. While this problem is seemingly mitigated by the current legal interpretation of "personal information" as not encompassing de-identified and non-identifiable data, this instead invites an overly broad definition of "re-identifiable," which may not be appropriate for modern and emerging data uses.

9. In Cybera's view, PIPEDA should explicitly outline a definition of "de-identified," and the Office of the Privacy Commissioner (OPC) should release comprehensive guidelines to assist stakeholders in understanding and utilizing anonymization. One example from a developed jurisdiction is Australia's 1988 Privacy Act, which has the following definition of de-identifiable: "personal information is de-identified if the information is no longer about an identifiable individual or an individual who is reasonably identifiable."[7]

10. The UK's "Anonymization Code" is a good example of a regulatory guideline that is risk-tolerant in approach. It states: "although it may not be possible to determine with absolute certainty that no individual will ever be identified as a result of the disclosure of anonymised data, this does not mean that personal data has been disclosed."[8] The UK's Digital Privacy Act also specifically criminalizes unauthorized re-identification of data.

11. In light of the above considerations, Cybera addresses the following questions and concerns posed by ISED:

    Will the additions we are proposing be enough to increase meaningful consent for individuals?

[5] http://www.ehcca.com/presentations/HIPAAWest4/lafky_2.pdf
[6] https://laws-lois.justice.gc.ca/pdf/P-8.6.pdf
[7] https://www.legislation.gov.au/Details/C2019C00241
[8] https://ico.org.uk/media/1061/anonymisation-code.pdf

12. In Cybera's view, the proposals put forward by ISED in this regard do not represent a significant departure from the existing legislative framework of PIPEDA, or its legal interpretation. However, as it is also our view that the existing framework is sufficient to ensure meaningful consent of individuals in the proper context, the proposals as presented appear instead to be a clarification on the matter of implied consent.

13. As the matter of implied consent is already laid out in Sections 4.3.5 and 4.3.6 of Schedule 1 of PIPEDA, and as these provisions have been legally interpreted on several occasions to apply to matters closely resembling "standard business practices," it is not clear that this needs additional statutory clarification. The Supreme Court case *Royal Bank of Canada v Trang*, for example, found that, when determining reasonable expectations of consent surrounding a disclosure, avoiding the overarching context would "unduly prioritize privacy interests over the legitimate business concerns."[9]

14. As such, the existing contextual approach is quite successful in allowing for flexibility in the types of consent required for different use and disclosure situations, and avoids a cumbersome opt-in approach to all processing. In addition, the exemption to meaningful consent for "standard business activities" is sufficiently broad to cover most modern data processing for commercial purposes.

15. This, in conjunction with the continuation of the accountability principle and the additional transparency measures proposed, constitute a flexible regulatory framework that is well in keeping with international norms.

What are the benefits of removing the requirement to obtain consent to process personal information for purposes that are considered to be standard business practices?

16. As stated above, avoiding "consent fatigue" must be an important consideration for any future regulatory approach. Europe's experience with consent regulations for computer cookies demonstrates how ineffective and counterproductive an overreliance on consent can be. In addition, it calls into question whether consent can ever be meaningful if it is the condition on which a consumer is able to access a desired service in its optimal format. In the case of cookie consent regulations in Europe, the issue is paradoxically compounded for those users who are most concerned about their privacy, as those who delete cookies from a given website would be required to consent to each subsequent use every time they access that website.

[9] https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16242/index.do

17. While regulators clearly do not intend to create such results, in Cybera's view, they may result from an overly doctrinaire commitment to underlying principles and potentially as a response to public reactions to privacy breaches that may incentive overcorrection. For example, the OPC's earlier consultation regarding its proposed change to transfers for processing was launched in reaction to the Equifax breach. This led the OPC to reinterpret its 2009 guidelines whereby transfers for processing were determined to be a "disclosure" and not a "use," thereby requiring consent. While this consultation was revised in light of ISED's current initiative to modernize PIPEDA, it does provide an example of regulatory overcorrection as it is questionable whether the proposed change was relevant to the facts of the matter in the Equifax case. Additionally, the change would have resulted in a reliance on consent even more onerous than that found in GDPR.

18. However, as stated in a previous response, it is not clear to Cybera that the addition of a "standard business practice" exemption is a significant or necessary change to PIPEDA. As GDPR does not include any statutory concept of implied consent, its reference to "legitimate business interest" is a necessary measure to cover processing situations.

    What activities should be captured by such a provision?

19. PIPEDA's purpose statement, Section 3 of Part 1, implies the framework of the "reasonable person" test, which provides meaningful context on the matter of consent. As stated, this concept has been referenced in relevant case laws that have underscored appropriate uses of implied consent. This approach allows for a degree of flexibility that may be a better framework to approach matters of consent, rather than specifically defined exemptions.

B. Data Mobility

20. While Cybera generally supports the right to data mobility and is aware that, as a right, the international community is moving towards data portability as the norm, we question whether the principle of informational self-determination is the best framework with which to approach the issue of data mobility. In this respect, the matter of data portability has been viewed as unique, in that it sits at the intersection of numerous legal fields, including data protection, intellectual property, consumer protection, competition law, etc. [10]

[10] https://reader.elsevier.com/reader/sd/pii/S0267364917303333?token=ADCC1321661E946E78EA2A8CB26834F29F0720FB2EA27DD9CFBE0A8657A9E656F294D12F0C29F441EBB36557A16D7EAE

21. As a corollary to this, Cybera questions the effectiveness of regulating all matters pertaining to data protection issues in one statutory law that must remain applicable to a broad variety of areas, and remain relevant over a long period of time. This concern is particularly glaring in the field of data policy, as technological change is rapid and unpredictable and needs agile and responsive frameworks to address changing needs

22. With respect to data mobility and data portability, these are issues that are perhaps better addressed through a regulatory body that is framed from the perspective of electronic commerce, unfair business practices, or competition law more broadly, rather than data protection. In addition, concerns related to lock-in and high-switching costs are already addressed within existing antitrust frameworks.

23. From a competition policy perspective, to demonstrate that a violation of consumer welfare has occurred would require one to establish market dominance coupled with exclusionary practices. In contrast, a blanket, *per se* data mobility rule that applies to all entities within a jurisdiction — i.e. Article 18 of the GDPR — would necessarily treat all entities equally, regardless of size. This would disfavor smaller entities relative to larger ones.[11]

24. In this respect, Article 18 of the GDPR goes much further in establishing data mobility as a right than any other similar regulation, and its full effects on the data economy are still not fully understood. In addition, competition law in both the EU and the US take a more holistic view on the issue of lock-in and high switching costs. It sees some broad industry-wide benefits in some circumstances, but also requires that claims be addressed from the perspective of demonstrating harm.[12]

25. In addition, there is the question of what data should be covered by data mobility regulations. This is a difficult question to answer in the modern context. The line that demarcates which data originates from the data subject — and which data is generated from the controller — will become increasingly difficult to determine as data usage evolves. A large proportion of existing online data derives from a combination of consumer data and controllers' analytic data. A common example is a Facebook users' friends list: while users choose their friends list, Facebook holds a wider range of related data such as declined, defriended, and suggested friend requests.

26. Applying Article 18 of the GDPR to this example does not lead to a definitive conclusion as to how this latter data should be treated. Applying any data mobility regulation to derived data would also have the additional result of complicating matters related to

[11] https://pdfs.semanticscholar.org/b826/c58ff279d3e6b3ae96583dcd5f023585b68b.pdf
[12] https://eu-competitionlaw.com/competitionantitrust-challenges-in-technology-aftermarkets/

intellectual property and technical feasibility. While ISED does refer to this concern in its discussion document, that ISED is considering creating an exception in cases that trigger intellectual property or technical feasibility concerns demonstrates the shortcomings in adopting a data self-determination approach to portability. Technological innovation and the increasing complexity of data analytics, machine learning, and artificial intelligence will increasingly diffuse proprietary information in the data economy, making the allowance of an IP and technical feasibility exception increasingly ubiquitous, and thereby self-defeating. This, again, would almost certainly favor dominant market entities and make it difficult for small startups to enter the market.

27. For this reason, Cybera argues that ISED should avoid the expansive approach to the matter of data portability that the GDPR uses.

2. Enabling Responsible Innovation

A. Possible Solution - Enabling Data Trusts

28. Cybera supports ISED's proposal to investigate the establishment of a data trust regime. As ISED noted, several jurisdictions — notably the UK, in its 2017 review of the artificial intelligence industry — have supported the idea of data trusts as a potential solution to modern data governance issues.

29. The flexibility inherent to data trusts may provide a framework with which the governance of data can co-evolve with emerging data uses. In addition, data trusts would allow for the consent of a group of beneficiaries to be aggregated into one legal trustee, thereby reducing the existing consent and knowledge burden on individual data subjects.

Could PIPEDA be harnessed to encourage the development of data trusts, in particular the existing exception to knowledge and consent for the disclosure of personal information for research and statistical purposes?

30. Yes, the existing exception to knowledge and consent for the disclosure of personal information for research and statistical purposes under PIPEDA could be harnessed for the development of data trusts.

3. Enhancing Enforcement and Oversight

31. Cybera is of the view that the matter of enforcement is one of the most important areas in need of change in Canada's regulatory environment. Currently, Canada is far behind other jurisdictions in terms of regulatory enforcement with respect to data governance.

32. In this sense, the current principle-based structure of PIPEDA is helpful in providing the flexibility needed to mediate the above-mentioned complexities. It is Cybera's view that maintaining the general structure and interpretation of PIPEDA would not significantly expose individuals to breaches of their privacy, as long as regulatory tools exist to hold controllers demonstrably accountable for the data they have collected. We also believe the OPC should be given greater order-making and punitive powers, such as the ability to offer a meaningful deterrent to unlawful or improper activity. Canada is unique among developed countries in having a complaints-based ombudsman model for our privacy regulator, which places us at a significant disadvantage with respect to data governance relative to other jurisdictions. Data protection and privacy agencies in the UK, US and EU, for example, have much broader enforcement and punitive powers relative to the OPC.

33. Under the current system, the vast majority of privacy-related cases in which the OPC intervenes are the result of a consumer complaint. This is problematic for a number of reasons. The volume of user data generated, collected and transferred — and the complexity of the systems used to manage that data — make it difficult for consumers to identify breaches of their privacy or even where their information is located, as the current consultation demonstrates. Much of this information may only be discoverable through a proactive approach and/or through resources outside the reach of individual consumers. In addition, emerging issues and technological advancements will continue to make it unlikely that a complaints-based system could give the OPC enough relevant and timely information about those privacy concerns to proactively investigate and monitor. In addition, it should be expected that a complaints-based model would not scale as consumer complaints will only grow as more systems "move to the cloud", creating unmanageable pressure on the OPC to respond and investigate in a timely manner. A central problem with the complaints-based model is that it relies on consumers' observations or experiences with an encountered problem, but does not proactively capture detrimental commercial activity (which the consumer is often unaware of).

34. In addition to recommending that the OPC be given additional powers of contractual approval and review, Cybera proposes giving the OPC the additional power to levy monetary fines, as is standard practice among other developed jurisdictions. The GDPR framework of levying a sanction of up to a maximum of four percent of annual global revenue may serve as an example model (though this percentage may still be too low).
35. Though this would be a comprehensive and structural change to Canada's privacy framework, adopting something akin to the EU's adequacy framework may also be an option worth investigating. The European example would allow the OPC to enforce standards with an understanding of the broad privacy standards of the country to which

Canadian data is sent. As stated, this would be a fundamental shift in Canada's current framework and would require significant further study.

36. In Cybera's view, the OPC should be given the additional power to approve standard contractual clauses and proactively review their implementation.

4. Conclusion

Cybera once again thanks ISED for the opportunity to provide comment on the matter of modernizing PIPEDA.

In this consultation, Cybera proposed the following recommendations:

1. Allow for a degree of flexibility in future privacy legislation to maintain a relative free-flow of data, including for transfers for processing, and transborder transfers for processing.

2. Maintain the principles of consent and accountability in future legislation, while allowing for implied consent to apply to transfers, where possible.

3. Continue to allow reasonable exceptions for data used for academic, scholarly and research purposes, and regulate these uses as a separate legal category from commercial uses.

4. Refrain from an overly broad requirements for data mobility and instead address the issue from a competition or antitrust perspective

5. Give the OPC greater powers of proactive review, investigation and audit.

6. Give the OPC the power to levy monetary penalties.