Innovation Science and Economic Development: Consultation on Transfers for Processing

Submission from Cybera Inc

August 6, 2019

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 agency responsible for accelerating high-tech adoption in Alberta. One of Cybera's 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 aid innovation, enterprise and ingenuity.

Cybera is guided by a strategic leadership team and is home to some of the world's top cloud and networking experts who work together to build cloud infrastructure, data storage, and advanced networking solutions. In addition, Cybera 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 the Office of the Privacy Commissioner (OPC) to provide comments on its proposed amendments to, and interpretation of the Personal Information Protection and Electronic Documents Act (PIPEDA) as it relates to data transfers for processing, including transborder data flows. 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 the OPC 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. For these reasons, Cybera agrees with the OPC's recommendation to move Canada away from a self-regulation regime towards a regime of demonstrable accountability, with the OPC assuming greater investigative and punitive authorities.

Longer Term – Future Law

How should a future law effectively protect privacy in the context of transborder data flows and transfers for processing?

1. In Cybera's view, the efficacy of any future privacy legislation cannot rest solely on its effectiveness in protecting privacy, but must also consider its ability to allow for commercial and scholarly innovation, to which transfers of data for processing are integral. As this is the central tension at the heart of privacy law, and as the importance of data transfers will become a central pillar of the modern economy, the importance of striking the correct balance between protecting personal information and allowing for a relative free-flow of data for novel and innovative uses cannot be overstated.

2. According to McKinsey, cross-border bandwidth use grew from 4,700 thousand gigabits to 210,000 between 2005 and 2015, and now has a bigger impact on GDP growth than the global goods trade.[1]

3. This growth is only projected to continue and will pose complex problems with how individuals' personal information will need to be protected.[2] Because of this and because of emerging trends such as the internet of things and big data, governments and regulatory bodies may need to come to terms with the possibility that individual control over personal information simply may not be possible in all circumstances. With this view in mind, it may be necessary to adopt a risk mitigation model with respect to data transfers, while also bolstering punitive and regulatory measures to create an effective deterrent to malicious activity.

4. As a corollary to this, obtaining express consent from citizens may also not be feasible in all contexts. While Cybera does not advocate for a change in the consent principle upon which PIPEDA is based and which is integral to maintaining consumer trust, express consent should not, in our view, be taken as a panacea that will reconcile all relevant concerns arising from data transfers. In many cases, an overreliance on express consent has proven cumbersome to both consumers and organizations and has had the counterproductive effect of degrading consumer vigilance in the long term. For example, the EU's experience with cookie consent demonstrated that consumers are generally unwilling to withhold consent if it means forgoing access to the content and services they desire, which may result in consumers becoming increasingly conditioned to automatically consent to all requests over time to maximize convenience. The EU's experiment with cookie consent laws also raises the corollary question of whether meaningful consent can be given if that consent is the condition on which a consumer maintains or gains access to desired content or services in their optimal format. This problem is compounded by the fact that the current monopolization of the digital interactive media space means that substitutes may be limited for many services.

5. Furthermore, it may not be possible in all circumstances to easily separate the additional benefits derived from a transfer of personal information from the integral functioning of the original service to which it applies. For example, it is not clear how a consumer can continue to benefit from a service if they do not consent to a transfer of their personal information to a 24/7 customer service entity. In Cybera's view, this is an example of a transfer that should be understood within the context of a consumer's implied relationship with the service provider. In this case, additional consent should not be needed, given that the accountability principle still applies to the controller.

---

[1] https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/digital-globalization-the-new-era-of-global-flows

[2] https://www.ntia.doc.gov/files/ntia/publications/measuring_cross_border_data_flows.pdf

6. This should not be taken to mean, however, that express consent should not be relied upon wherever it is feasible to do so. The issue of autonomy with respect to personal information is of paramount concern in the modern context. Countless examples, including the Equifax case and the Cambridge Analytica case, demonstrate that protection of personal information cannot be left solely to commercial entities.

7. Under these circumstances, privacy legislation must be formulated around an understanding of the risks and rewards of data collection and use. In this context, the effectiveness of any future legislation with respect to protecting privacy should be measured by the degree of accountability it places on controllers for the data in their possession and the level of consent required to collect, use and/or disclose that data.

8. Effective privacy legislation should obligate relevant organizations to secure meaningful and informed consent for data collection, use and disclosure. This should be done in a manner that is straightforward and transparent, while also allowing for more flexible forms of consent — ie, implied consent — in instances where commercial, consumer or research interests can be advanced through a transfer of data (assuming that the purposes of doing so align with the original collection, and that the originator of that data is notified of the transfer).

9. 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 constitute 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.[3]

10. With respect to transfers for processing, including transborder transfers, Cybera recommends that the OPC refrain from the previously discussed regulatory reinterpretation of PIPEDA absent any statutory changes that could significantly clarify some of the legal uncertainties around this issue. Doing so would allow for the consent

[3] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_33/?wbdisable=true

principle, which is integral for consumer confidence to be maintained, while also clarifying obligations with respect to transfers of data, and the penalties for doing so irresponsibly. As demonstrated in the Equifax case, this lack of clarity can, in Cybera's view, be traced to deficiencies in PIPEDA's wording, especially with respect to clear definitions of 'disclosure' and 'use'.

11. It is not clear whether PIPEDA — as currently formulated — provides enough information to alone determine whether a transfer of data should be categorized as use or disclosure. Furthermore, this consultation demonstrates the need for providing greater clarity with respect to the definitions of transfers of data, and the types of uses of that data. While the current consultation arose from transborder issues resulting from the Equifax breach, PIPEDA does not distinguish transfers that cross borders from transfers between entities within Canada, meaning there are no statutory means to apply a set of regulations to one category without affecting the other.

12. Similarly, the definition of "use" may also be too broad. Cybera is of the view that there is a meaningful distinction to be made between transfers of data made for commercial uses, and those made for scholarly or research purposes, one being driven by profit, with the other largely motivated by the public good. Furthermore, there exists within academia additional layers of ethical standards with respect to scholarly research based on personal information that do not exist in the commercial sector. These additional standards should factor into how sets of data are used for each of these purposes. As such, Canada's privacy legislation should be cognizant of personal data used for research purposes and, where possible, separate such data usage from commercial uses. British Columbia's Personal Information Protection Act (PIPA), is an example of legislation that does this quite clearly and unambiguously.

13. In Cybera's view, PIPEDA already provides a useful measure of flexibility with respect to the types of consent needed in particular circumstances. To the degree that this framework can be maintained in future legislation, tying the level of consent to the type and sensitivity of data, as is currently the case under PIPEDA, is a good approach in a general sense. However, there is room to clarify this framework further by better defining the categories of data uses.

14. Clearer guidelines with respect to data transfers are being implemented in other jurisdictions, such as GDPR. We therefore feel the Canadian guidelines are in need of further legislative clarification.

Is it sufficient to rely on contractual or other means, developed by organizations and reviewed only upon complaint to the OPC, to provide a comparable level of protection? Or should a future law require demonstrable accountability and give a public authority, such as the OPC, additional powers to approve standard contractual clauses before they are implemented and, once they are adopted, proactively review their implementation to ensure a comparable level of protection?

1. In Cybera's view, the OPC's current complaints-based regime is not sufficient to safeguard privacy. In light of the complexities of the modern data economy discussed above, it is necessary for Canada's privacy regulator to assume additional authorities to protect the privacy of citizens' personal information, including additional powers to proactively review and audit.

2. Under the current system, the vast majority of privacy-related cases in which the OPC intervenes are the result of a consumer complaint.[4] 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. A central problem with the complaints-based model is that it relies on consumers' observations or experience with an encountered problem, but does not proactively capture detrimental commercial activity (which the consumer is often unaware of).

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

How should a future law effectively protect privacy where contractual measures are unable to provide that protection?

1. 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.

[4] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-consent-under-pipeda/submissions-received-for-the-consultation-on-consent/sub_consent_33/?wbdisable=true

2. 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.

Shorter Term – Current Law

In your view, does the principle of consent apply to the transfer of personal information to a third party for processing, including transborder transfers? If not, why is the reasoning outlined above incorrect?

1. As stated previously in this document, it is not obvious that the question of whether a transfer for processing can be taken as a 'use' or 'disclosure' can ultimately be resolved based on the information given in the current formulation of PIPEDA alone. This ultimately is the question that, once answered, will inform to what degree the principle of consent should apply to the matter of transfers for processing, including transborder transfers. As the interpretation now proposed by OPC is a reversal of its own nearly decade-long interpretation of the matter, Cybera is of the view that the safest and fairest approach to resolving this question should be through a parliamentary process rather than a regulatory reinterpretation. For this reason, Cybera commends the OPC for deferring its previous consultation on this matter in favour of Innovation, Science and Economic Development's current initiative with respect to the modernization of PIPEDA.[5]

2. However, in the interim, Cybera suggests that the reasoning provided by the OPC in the June 11, 2019 discussion paper[6], to which this document is a response, is requires further review on several grounds.

3. The OPC presents the following arguments in favour of its current proposal;

a) "a transfer of personal information between one organization and another clearly fits within the grammatical and ordinary sense of "disclosure": « make known, reveal » (Canadian Oxford English Dictionary)"

4. In Cybera's view, it is not clear that the interpretation of the grammatical and ordinary sense of 'disclosure', as relevant to the context of PIPEDA, can be reduced to the given

[5] https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/
[6] https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00107.html

definition. In addition, many definitions of 'disclosure' from sources other than that provided by the OPC include the qualifier that a disclosure means the revelation of 'new' information.[7] On this definition, information transferred to a processor from a controller may not be interpreted as newly disclosed from the perspective of the originator of that data if the purpose of the original collection was the same as the transfer. While there is significant room for debate on this matter, Cybera is of the opinion that the OPC is overreaching in claiming that this interpretation and definition "clearly fits" with the facts of the matter in this context. For example, privacy legislation in other jurisdictions, including GDPR, explicitly distinguish transfers from disclosures, thereby challenging the OPC's stated interpretation.[8]

b) "In addition, a number of provincial statutes in Canada, deemed substantially similar to PIPEDA, either consider transfers for processing as disclosures, or adopt specific rules for these activities and, notably, explicitly exempt these activities from a consent requirement"

5. With respect to the provincial legislation referenced — specifically Alberta and British Columbia's Personal Information Protection Acts (PIPA) — it is important to acknowledge that, should the underlying framework with respect to transfers/disclosures in these legislations be accepted, they still pose a challenge to the OPC's overarching reasoning with respect to consent and transfers. That these legislations exempt the consent principle in instances of data transfers may instead indicate that the framers of the provincial legislation observed an impracticality in applying consent to those data transfers where consent could reasonably be implied, and that PIPEDA mediates this impracticality through other means.

6. Notably, governance issues arising from transborder data flows have been relevant to policy makers since the start of modern computing, and may likely have factored into the reasoning of both provincial and federal legislative framers.[9] It is therefore possible that, should the framers of PIPEDA have had a concern about such transfers, and should they have felt that such instances were not already covered by their framing of PIPEDA, they would have explicitly created provisions to mediate the matter. That they did not indicates they may have felt that the framework established by PIPEDA with respect to transfers already covered this ground, and thus did not need to implement exemptions.

[7] https://www.lexico.com/en/definition/disclose
[8] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL
[9] https://core.ac.uk/download/pdf/73971451.pdf

c) "If Parliament intended consent not to apply, would it not, as several provincial legislatures have done, exempt processing situations from the consent requirement"

7. Cybera questions this reasoning as, similar to the matter currently under question, it is not clear from PIPEDA whether Parliament intended for processing situations to be interpreted as a "use" or "disclosure". If the original intention of PIPEDA was for a processing situation to be interpreted as a use, then there would be no need for Parliament to explicitly state that an exemption was needed for the consent requirement. Contrary to this, the continued reference to the 'purpose' of underlying collections, disclosures, and uses instead suggests that consent could be implied in matters where it is reasonable to do so, thus making the need to allow for an exemption unnecessary, as also stated above.

8. Cybera acknowledges that there is significant room for debate on these matters. For this reason, we are of the view that this topic should be properly addressed through ISED's current initiative to modernize PIPEDA, rather than at the regulatory level proposed by the OPC.

What should be the scope of the consent requirements in the Act in light of the objective of Part 1 of PIPEDA as set out in section 3, the new section 6.1 (and its reference to the nature, purpose and consequences of a disclosure), and the OPC's Guidelines for obtaining meaningful consent, in force since January 1 2019? Specifically:

a) In what circumstances should consent be implicit or explicit?

1. The framework established by GDPR, in particular its 'legitimate business interest' exemption, serves as a good example of a legislative measure that provides a reasonable degree of flexibility on this matter while also providing effective safeguards.[10] In addition, the Alberta PIPA and BC PIPA also allow exemptions for instances of transfers for processing. When pertaining to this matter, future legislation should be framed such that an implied relationship or an existing business interest can be interpreted to allow for implied consent. In all other circumstances, explicit consent should be relied upon.

[10] https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/

Do you think the proposed interpretation of PIPEDA is consistent with Canada's obligations under its international trade agreements? If not, why would the result be different from the current situation, where the elements identified in question 6(b) must be disclosed as part of the openness principle?

1. As it pertains to international trade agreements to which Canada is a party, the issue of transborder data flows is complicated. There may not exist sufficient case law on the subject to determine what affect the OPC's proposed change would have as a legal matter. However, the question may be better understood from a more holistic perspective.

2. Canada is currently entering a situation where we are being pulled in opposite directions by our trade obligations to the US and our ongoing adequacy status with the EU.[11] While the North American Free Trade Agreement (NAFTA), Canada-United States-Mexico Agreement (CUSMA) and the Comprehensive and Progresive Agreement for the Trans-Pacific Partnership (CPTPP) have provisions which seek to discourage data localization and encourage a relative free-flow of data transfers, the EU is moving in a more restrictive direction with respect to these matters. As such, attempting to formulate privacy laws that meet one obligation while compromising the other may be a short-sighted approach.

3. However, the proposed change in policy is relevant to, and may affect, the following provisions of CPTPP and CUSMA;

4. Article 14.11.12 of CPTPP reads;
    I. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person."
    II. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
        a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade, and
        b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

[11] http://www.michaelgeist.ca/2018/10/setting-the-standard-how-the-usmca-quietly-reshapes-global-digital-trade-agreements/

5. Article 19.11 of CUSMA reads;
    I. No Party shall prohibit or restrict the cross-border transfer of information, including personal information, by electronic means if this activity is for the conduct of the business of a covered person.
    II. This Article does not prevent a Party from adopting or maintaining a measure inconsistent with paragraph 1 that is necessary to achieve a legitimate public policy objective, provided that the measure:
        a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
        b) does not impose restrictions on transfers of information greater than are necessary to achieve the objective.

6. While the wording of these provisions are similar, the wording in CUSMA is subtly more restrictive, particularly in the line: “No Party shall prohibit or restrict.” The word ‘restrict’ in this provision is particularly broad and could easily be applied to a number of policy approaches, including the OPCs proposed change with respect to transfers for processing. However, both provisions allow for the caveat that national regulations can be adopted with respect to transborder data flows, given they achieve a “legitimate public policy objective”, though this term is also not clearly defined.

7. In addition, footnote five of article 19.11 of CUSMA reads: “A measure does not meet the conditions of this paragraph if it accords different treatment to data transfers solely on the basis that they are cross-border in a manner that modifies the conditions of competition to the detriment of service suppliers of another Party”.[12] This provision may prove problematic to the OPC’s intention to implement the discussed policy change, as it arguably corresponds to the motivations behind implementing the proposed change, which is evidenced by the OPC’s reasoning outlined in the relevant discussion document. However, because the policy change does not solely apply to transborder data transfers, it is possible that the proposed change may not trigger this provision.

8. With respect to the second part of the question, notification and consent have clearly different impacts on the question of transborder policy. A notification regime does not give consumers the ability to opt-out of a given data transfer, thereby making the question of compliance with data transfer provisions irrelevant. Consent, especially express consent, does give an individual the ability to localize their own data within Canada, if they so wish, but as this right does not apply solely to transborder transfers but transfers in general, the effect of this policy on the relevant CUSMA provision is unclear.

[12] https://www.international.gc.ca/trade-commerce/assets/pdfs/agreements-accords/cusma-aceum/r-cusma-19.pdf

9. Cybera is of the view that the effect that the discussed changes may have on relevant trade agreements needs to be investigated in a more comprehensive manner than the process posed in this consultation. In addition, the degree that aligning transborder policy with regional trade agreements might adversely affect Canada's adequacy status with the EU also needs further discussion.

Conclusion

Cybera once again thanks the OPC for the opportunity to provide comment on this matter and we look forward to your office's continued engagement with the issue of PIPEDA and transfers for processing, including transborder transfers. In this regard, Cybera hopes to see stakeholders' engagement with the current consultation reflected in the OPC's response to ISED's ongoing efforts to modernize 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 a regulatory reinterpretation of PIPEDA while relying instead on legislative amendment to PIPEDA to clarify the matter of consent and data transfers.

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

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

7. Engage in further study on the relevance of an adequacy model for Canada.

8. Engage in further study on the matter of transborder data flows as it pertains to Canada's trade relationships with the US and EU.