Digital Advertising Alliance of Canada

Submission in response to the Office of the Privacy Commissioner of Canada's consultation on transfers for processing – reframed discussion document

August 6, 2019

Submitted on behalf of the DAAC by:

Julie Ford
Executive Director
Digital Advertising Alliance of Canada

Thank you to the Office of the Privacy Commissioner of Canada for allowing submissions to the important conversation on whether consent should be required for transfers of data for processing. The Digital Advertising Alliance of Canada (DAAC) is pleased to provide this submission in response the discussion document released by your Office.

Executive Summary

The Digital Advertising Alliance of Canada (DAAC) is a not-for-profit consortium of the leading national advertising, media agency and marketing associations whose members share a commitment to delivering a robust and credible self-regulatory program for responsible online interest-based advertising (IBA), called AdChoices. Additionally, in June 2019, we released a solution for political advertising transparency called the Political Ads Program.

Our position in the digital ecosystem provides us with a unique vantage point to assess the impact of the Office's discussion document. Our responses to the questions come from an interest-based advertising perspective.

The DAAC urges the OPC to consider extending the consultation period and continue the conversation by conducting a series of in-person meetings and roundtables with various industries.

Commentary

Introduction and Consultation Recommendations

We must have sound privacy laws that allow for an innovative digital industry, and, are realistic to the needs of individuals in Canada.

The DAAC's position in the digital ecosystem provides us with a unique vantage point to assess the impact of the policy position change the Office is considering.

Balancing the free flow of data in accordance with NAFTA/USMCA must be considered before a policy position change occurs. Our recommendation would be to include input from trade representatives where possible.

We recommend further stakeholder engagement, such as in-person meetings, to help contextualize the impact such a policy change would make.

If the primary concern surrounds the risk of data being shared with countries that do not have the same protections as Canadian laws, then the OPC should instead provide guidance for how companies may mitigate those risks through a series of workshops, consultations, or more prescriptive guidance documents addressing that specific topic.

Consent

Our many-years experience in answering to the public, of matters having to do with advertising data online, provides us with insight into what really matters to individuals.

Individuals do not want to be interrupted in their online experience. They do not want to be burdened with having to read lengthy privacy policies or make decisions that they don't fully understand what they are/are not consenting to. They just want to engage with their corners of the web, and use the apps they have downloaded, with ease.

As it is written, the policy position is so broad that it would require consent for all service providers a company uses, which could include marketing vendors, agencies, IT personnel, insurance providers, and more.

We assert that interjecting consent further into the online experience will hinder, not help, online users with their enjoyment of the web. There will certainly be privacy "power-users" who will read the policies and act upon their consent choices. But that is not the majority of internet users. Consent is not a practical one-stop-shop solution when it comes to privacy online.

The majority of online users, particularly those of younger generations, understand how data needs to flow across borders to provide them with what they want, when they want it, and they understand that data is used & shared to accomplish this.

IBA is under an implied consent regime provided that individuals are made aware of the practice, get timely and detailed information about it, are able to opt-out and that opt-outs take effect immediately and are persistent, and that information is limited to non-sensitive information and destroyed as soon as

possible or effectively de-identified[1]. Our self-regulatory program is modelled after this framework. With this new position in mind, the trickle-down effect would be that consent vendors (many of which are based in the US) used by some of our participants to adhere to IBA requirements, would be required to get opt-in consent for those vendors in order to get implied consent for IBA. The operational consequences get murkier the further you think it through.

The DAAC is in agreement that sensitive data for IBA requires opt-in consent to use; however, consent for this needs to be accomplished within reason. Would a reasonable person expect that they will be prompted for express consent each time their insurance provider changes a marketing vendor? Or if their bank changes ad agencies, and that agency might receive reports about segments of data from within the bank's customer relationship management platform (CRM)? Consent cannot be meaningful when you truly cannot control it without breaking a service you're aiming to use.

To add further complication, trade secrets may often include what vendors organizations are working with, which could be highly advantageous for competitors to know.

Regardless of the level of consent, implied or express, it will always require action upon the consumer to exercise their choices. This action must be meaningful, easy to use, and effective. And in the absence of action, there needs to be accountability.

Accountability

Accountability within PIPEDA already provides the necessary flexibility organizations need when deciding how to best protect the personal information it's transferring for processing.

Reputable organizations, both within Canada and abroad, spend hours of time (and countless funds) to be accountable guardians of data. The Office must recognize that the real, most actionable, tool in their arsenal is within accountability. Unlike meaningful consent, which is fluid and based on each individual that a company interacts with, businesses can control the levels of accountability and safeguards they implement.

If organizations do get express consent for sensitive data use (for IBA, as example), do individuals even want that as the deciding factor on its own? The DAAC posits that Canadians do not want consent as the main factor for protecting their personal information. There needs to be robust and credible accountability work to back it up, and possibly be the sole focus of regulator intervention.

Questions for Stakeholders (Longer term – Future law), Answered

1. How should a future law effectively protect privacy in the context of transborder data flows and transfers for processing? Canada should approach any future law with a deep respect for decisions and opinions of past experts and reports. Canadian privacy experts and regulators should be proud of the balance that PIPEDA has provided, and in fact inspired in other jurisdictions. Amendments are not recommended. And any amendments proposed should be approached extremely carefully in order to maintain innovation and growth in Canada.

[1] Guidelines on privacy and online behavioural advertising – https://www.priv.gc.ca/en/privacy-topics/technology/online-privacy-tracking-cookies/tracking-and-ads/gl_ba_1112/

2. 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? While on paper the latter scenario described in this question seems straightforward, it is unclear as to the depth the OPC is willing to go to ensure there is demonstrable accountability. The level of staff expertise, time, and volume of information to assess seems unsurmountable. If it will begin reviewing contracts and assessing their implementation, what happens if still something goes wrong?

   The OPC currently has powers under PIPEDA which it can already take advantage of, perhaps explore the extent of those powers first.

   Complaints-based investigations, pro-active research, investigations with the intent of improvement and not to solely penalize organizations who are trying to do good work, and providing general advice, but not business specific assessments, are beneficial.

3. How should a future law effectively protect privacy where contractual measures are unable to provide that protection? Rely on accountability measures to pick up where contractual measures cannot reach. Contractual measures are a standard, reliable, way of doing business in the digital ecosystem. However, data may be still mishandled or misused unwillingly which is where pro-active accountability measures provide extra protections. There are software, hardware and human accountability measures that can be implemented to provide that extra level of support. Organizations like the DAAC's self-regulatory program are a valuable resource in the IBA sector, but there could be other sectoral organizations that handle other areas of complicated data flows. Don't hesitate to ask for their help.

Questions for Stakeholders (Shorter term – Current law), Answered

4. 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? No. Programmatic advertising, and even standard online advertising, requires the use of multiple stakeholders to source, bid, place and report on campaigns. The number of stakeholders used often changes. To be consistent with guidance and reports of findings published to date, and to retain a viable workforce in marketing and advertising in Canada, the Office must keep online advertising practices under an implied consent regime, particularly for interest-based advertising, provided that the individual has the ability to opt-out cleanly and effectively. What we should instead focus on is enhancing safeguards and accountability.

5. Does Principle 4.1.3 affect the interpretation or scope of the principle of consent? If so, what is the legal basis or grounds for this interpretation? No. We suggest that the phrase "in its possession or custody" used in Principle 4.1.3 implies that the organization already took measures (including consent, implied or express as needed) to obtain the personal information. It describes the accountability measures that should be in place.

6. 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? Assuming consent is required, is it express or implied? Make three assumptions #1 that it's sensitive data (e.g. payment data) #2 it's purely for processing for the first party (nothing new introduced for third party commercial gain) #3 there's a robust contractual agreement in place (audit provisions, etc. in a written form). What's the reasonable expectation of the user at this point? Is there a meaningful residual of significant harm? Is it sensitive? What's the individual's reasonable expectation?
    b. What should be the level of detail in the information given to the person affected? Do you agree that consent should be comprised of at least the following elements: (i) the purposes for which the responsible organization seeks to use the personal information, (ii) the fact that it uses third parties for processing but that it provides for a comparable degree of protection, (iii) when the third parties are outside of Canada, the countries where the personal information will be sent, (iv) the risk that the courts, law enforcement and national security authorities in those countries may access the personal information? Transparency practices that provide users with the necessary information they need to make an informed decision is undeniably valuable. But keeping this information up-to-date, easy-to-read and actionable is operationally challenging. Statements should be placed in policies that organizations create to cover these issues, but even then, it's an incredible amount of work to assemble and maintain this information, that most users would likely not use in a meaningful way. Our self-regulatory program often consults with organizations, encouraging them to list out all the third parties they are working with. This exercise can take months with some large organizations, and involves legal counsel and assistance from several departments (IT, web dev, marketing, etc.). We have made much headway in encouraging our program participants to assemble these teams, and there have been hours upon hours of work involved to make accurate notices.
    c. Should the notice to the affected person name the third parties? Our self-regulatory program asks our participants to name the third parties they are working with for interest-based advertising. In many circumstances, this information is turned into a table of vendors with descriptions next to them. Ad tech providers are well equipped to manage these types of charts, but first-party advertisers and publishers are often not, and can find it challenging to keep them up-to-date. Part of our program's role is to help them with this.
    d. Should the notice contain other pieces of information? That would be up to the organization to decide, based on their business practices. Ad Standards, our

accountability provider, offers suggestions for drafting effective disclosures on page 9 of their 2018 compliance report[2], emphasizing that describing the types of data being collected, used and shared should be clearly explained.

7. Since the 2009 Guidelines already require that consumers be informed of transborder transfers of personal information, and of the risk that local authorities will have access to information (preferably at the time it is collected), at a practical level, would elevating these elements to a legal requirement for meaningful consent significantly impact organizations? If so, how? Yes, as stated throughout this submission, it adds layers of complexity to an already complex ecosystem. Consent means choice. It requires there to be an alternative solution that the organization must provide to retain that customer, which is operationally problematic for most businesses. As noted earlier in this submission, if the goal is data localization due to other countries' inadequate privacy laws, then consent should not be the focus. It puts undue pressure on the consumer to understand the partner relationships of every business they're looking to become a customer of.

8. If the elements identified in question 6(b) were required conditions for meaningful consent under a new OPC statement of principle, what steps should the OPC take to address the needs of organizations to collect, use, and disclose personal information? We ask the OPC consider further consulting multiple industries before pursuing changes. One report of finding should not be a catalyst for swift change. The unintended consequences appear to far outweigh the benefit to consumers.

9. What elements should be included in obtaining consent for transfers for processing that are not transborder? The framing of this question suggests that data localization should receive special treatment, and potentially lessened requirements for compliance with PIPEDA.

10. 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 3(b) must disclosed as part of the openness principle? Canada is currently negotiating fundamental trade agreements with the US, Mexico and Europe. The operational impact of this discussion is being noticed by privacy representatives of those countries. The practical reality is that people are going to want to keep the data in Canada to adhere to transborder dataflow concerns that the discussion paper introduces. A data localization requirement changes how many industries operate, including digital advertising.

    International trade lawyers would need to look at the OPC's position in greater detail. USMCA includes a whole chapter on digital trade[3]. It addresses PI and transfers and location of computer facilities. It affirms all parties recognize the importance of frameworks that *promote* trade (to not constrain it). Article 19.11 states that no party shall prohibit or restrict transborder transfers, including personal information, if it is for the conduct of the business for the covered person. Article 19.12 states that no party should require a condition of providing business in that territory.

[2] https://adstandards.ca/wp-content/uploads/2019/07/2018-AdChoices-Compliance-Report.pdf
[3] https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/19_Digital_Trade.pdf

Is it appropriate for the OPC to be engaging in this discussion alone? This could affect international trade and should be carefully considered by government.

11. Any other comments or feedback you think may be helpful. See our final thoughts.

Final Thoughts

Consent, whether implied or express, should be fluid based on the situation data is being collected or used for.

We suggest that coalitions like ours should be encouraged to maintain sector-specific adherence to PIPEDA, with us reporting aggregated findings to the OPC on an annual basis. The OPC does not need to be entangled into sector-specific data use (unless there is a complaint); it is not feasible to do so in a meaningful way and would put a strain on OPC resources to fully understand how each sector and organization handles data.

Complexity is a word often used when describing the digital ecosystem. But in the Office's revised policy position, which goes beyond transborder dataflows in actuality, it suggests that all industries must reveal their complexity to the individuals they are serving. Does this proffering of more information and deeper specificity to users make consent more meaningful to them?

It also positions a world where bespoke consent models would become the norm, disrupting the regular business flows of major companies. Will this result in a more trusted marketplace? Or will this become a more unsatisfied one? We theorise it will be the latter.

Throughout this submission process the DAAC has carefully considered the OPC's viewpoints and concludes that altering PIPEDA is not necessary, particularly not in the way it is positioned in the discussion paper.

The digital advertising ecosystem has long committed to improvements, and continues to evolve, however we cannot rely solely on consent as the model to uphold. The DAAC exists to help organizations navigate PIPEDA for IBA and features a strong accountability component. Accountability is necessary, and in fact, crucial in this digital age.

We thank the OPC for reading and look forward to continuing our participation in the consultation process.

* * *

Submitted on behalf of the DAAC by:

Julie Ford
Executive Director
Digital Advertising Alliance of Canada

info@daac.ca

YourAdChoices.ca

PoliticalAds.ca

Categories: organization, industry, self-regulation, advertising, digital advertising, transborder

About the DAAC

The Digital Advertising Alliance of Canada (DAAC) is a not-for-profit consortium of the leading national advertising, media agency and marketing associations whose members share a commitment to delivering a robust and credible self-regulatory program for responsible online interest-based advertising, called AdChoices.

Our founding member organizations consist of the following trade associations:

- Association of Canadian Advertisers (ACA),
- Association of Creative Communications Agencies (A2C),
- Canadian Marketing Association (CMA),
- Canadian Media Directors' Council (CMDC),
- Conseil des directeurs médias du Québec (CDMQ),
- Institute of Communication Agencies (ICA), and
- Interactive Advertising Bureau of Canada (IAB Canada).

Ad Standards, Canada's independent national advertising industry self-regulatory body, is responsible for implementing the accountability and self-regulatory enforcement framework for the Canadian AdChoices program.

Readers may learn more about our organization's work at YourAdChoices.ca.

About the AdChoices Program

The DAAC's AdChoices program is an excellent example of the viability of PIPEDA's current consent requirement within a complex data ecosystem. The program has been specifically designed to build upon PIPEDA's principles for fair information practices, in particular PIPEDA's accountability, transparency, and consent principles.