Ms Lara Ives
Executive Director
Policy, Research and Parliamentary Affairs
Office of the Privacy Commissioner of Canada
Lara.Ives@priv.gc.ca

06 August 2019

Re: Access Now's submission to the Office of the Privacy Commissioner's consultation on transfers for processing

Dear Ms Ives,

Thank you for your invitation to provide information and observations on the consultation on transfers for processing under the Personal Information Protection and Electronic Documents Act (PIPEDA).

Access Now is an international organisation that defends and extends the digital rights of users at risk around the world. By combining innovative policy, user engagement, and direct technical support, we fight for open and secure communications for all.[1]

The global movement of data is at the heart of a free and open internet. This requires legal certainty for stakeholders to operate and clear protections for users to ensure that their rights travels with their data and that transfers happen in a rights-respecting manner. In this context, robust data transfer frameworks which ensure a high level of data protection are key to deliver these benefits for all actors. As a starting point, governments and public authorities must ensure that the transfer of personal data complies with international human rights law, including with obligations and responsibilities on data protection, privacy and access to remedies.

To assist the Office of the Privacy Commissioner in discussing short-term and long-terms rules for transborder transfers, we provide answers to selected questions posed in the consultation. Below, we respond first to the question for stakeholders on the interpretation of the current law so users' rights can be strengthened in the short term before providing comments on how to articulate rules on transfer for processing on the potential future law with a view to improve users' rights in the long term.

A. Considerations for transfers for processing under the current law (Shorter term)

[1] Access Now

In your view, does the principle of consent apply to the transfer of personal information to a third party for processing, including transborder transfers?

First, it is important to note that the principle of consent applied to the transfers of personal data to a third party is usually an **exemption** from the general principles or grounds for transfer. As a general rule, data may only be transferred to third countries if an adequate level of protection is provided for or if appropriate safeguards have been developed and the data subjects enjoy enforceable and effective rights in order to continue to benefit from their fundamental rights and safeguards.

Following this model, in the European Union, the General Data Protection Regulation ("GDPR") states that, in the absence of a valid mechanism for transfer and as a derogation, a transfer of personal data to a third country or an international organisation may take place if "the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards".[2] This means that the use of consent for personal data transfer is not considered as a long-term mechanism for transfer but as solution for punctual, exceptional cases.

Consent should be defined as **informed and explicit,** requiring an **affirmative action** from the user. It must be **freely given** and the user must have the **capacity to withdraw consent at any time**. This means, for instance, that pre-ticked boxes would not qualify as valid consent.
In addition, entities processing personal data cannot deny a user access to a service on the basis of the user refusing the transfer of their data as in this case consent would not be considered freely given.

Additionally, in order to constitute a valid ground for a data transfer, consent needs to be **specifically given** for a particular data transfer or set of transfers. For instance, if a data subject's consent is obtained for a purpose that does not foresee a future transfer, the consent provided at the time of the collection and use of the data by a company at that time is not valid for the transfer of such data. Therefore, entities seeking to transfer the data based on consent must make sure to obtain specific consent to do so before the transfer happens.
According to the principle of purpose limitation, personal data should be collected and processed only for a defined purpose. This purpose should be specific, explicit and limited in time and data should not be further processed in any manner incompatible with that purpose. When the processing has multiple purposes at the time of collection, consent should be sought and given specifically for all of them.

Consent must be **informed**. This means that the data subject must be properly informed in advance of the specific circumstances of the transfer. Data subjects should be informed of (i)

[2] European Union General Data Protection Regulation, (EU) 2016/679

the purpose of the transfer, (ii) identity of the entity processing the data, (iii) the type of data that will be transferred and for how long, (iv) the existence of the right to withdraw consent and (v) the identity or the categories of recipients that will have access to this data.
Particularly in the case of transfer, data subjects should also be informed of the specific risks resulting from the transfer, including (vi) the fact that law enforcement and national security authorities may access their personal data, (vii) all countries to which the personal data are being transferred to, and (viii) that the third country to which the data will be transferred does not provide for an adequate level of data protection.

B. Considerations for transfers for processing under a future law (PIPEDA amendments, longer term)

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

Data protection frameworks should be designed to ensure secure free flow of data by establishing adequate mechanisms for data transfer and effective safeguards for users' rights. These mechanisms must be put under strict and transparent oversight and include effective remedies to **ensure that the rights of users travel with the data**.

Different types of mechanisms for transfer for processing can be designed. In the EU, under GDPR, data transfer outside the European Economic Area may only take place if the transfer is made to a country that has been granted an adequacy status or when another lawful data transfer mechanism is in place. The determination of an adequacy decision means that the laws, statutes, and practices of a third country are analysed to establish whether this country ensures an equivalent level of data protection. This requires an analysis of a country's domestic laws and international commitments into which it has entered in the area of data protection, access to data by public authorities, and access to remedy.
To contribute to this exercise and as part of our work to defend and extend privacy and data protection rights globally, Access Now has provided comments on the development and implementation of a large number of data protection and privacy proposals. This includes regional norms such as the EU GDPR, the Brazilian Marco Civil, the African Union Convention on Cyber Security and Personal Data Protection, as well as in national legislative and reform processes in Argentina, Ecuador, the United States, Tunisia, India and many more. On this basis, we have created a guide providing recommendations to lawmakers when developing or reforming privacy and data protection laws.[3] This guide includes specific recommendations on data transfers. In addition, Access Now been commenting extensively on the adequacy decision to transfer personal data from the EU and the United States. We have provided detailed recommendations for parties engaged in a negotiation process for such arrangements.[4]

[3] Access Now - Creating a data protection framework, a guide for lawmakers
[4] Access Now - Submission to First Privacy Shield Review and Access Now - Submission to Second Privacy Shield Review

Finally, in the absence of an adequacy decision, other mechanisms for transfer can be developed with the Office of the Privacy Commissioner on the basis of contracts or agreements that may be similar to binding corporate rules (BCRs) and standard data protection clauses (SCCs) used in the EU for instance.

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?

A future law in Canada should give the Office of the Privacy Commissioner powers to review, approve, and scrutinise the use of mechanism similar to SCCs. This mechanism creates a positive relationship between the Office of the Privacy Commissioner and data controllers as it requires direct dialogue and control. Beyond basic data protection principles and rights, it will be important that the model clause created by the OPC would include obligations on privacy by design, data security, as well as data breach and reporting obligations. Additionally, we recommend including a mechanism to foster accountability by encouraging entities to keep records of their decisions and actions related to the transfer for processing and any further processing. Finally, the Office of the Privacy Commissioner should have the authority to request the suspension or end of processing, including for transfer, under SCCs, in particular if it established that data is being transferred to a third country who is violating fundamental rights.

Conclusion

Thank you very much for the opportunity to participate in this consultation. The relevance and scale of data transfer in the digital economy is such that it requires broad consultation with stakeholders to refine and develop rules that provided for legal certainty and effectively protect users' rights, including privacy and data protection.

We welcome the openness of the Office of the Privacy Commissioner in reaching out to civil society and NGOs to contribute to this public consultation. We look forward to continuing the engagement with Office of the Privacy Commissioner in this process.

We remain at your disposal for any questions you may have.

Sincerely,

Estelle Massé
Global Data Protection Lead