August 6, 2019

Office of the Privacy Commissioner of Canada
30 Victoria St, 8th Floor
Gatineau, K1A 1H3
Québec, Canada

Re: Consultation on Transfers for Processing

Dear Privacy Commissioner Therrien,

Inpher appreciates the opportunity to comment on the Office of the Privacy Commissioner's ("OPC") *Consultation on Transfers for Processing*[1] to discuss the application and interpretation of the Personal Information Protection and Electronic Documents Act of 2000 ("PIPEDA") for effective privacy protection in the context of transborder data flows.

The OPC serves as an independent agency that is empowered to enforce data privacy laws across Canada. The Privacy Commissioner has a parliamentary mandate to enforce the Privacy Act[2] and PIPEDA, particularly to ensure that strong privacy safeguards undergird domestic and international data transfers which facilitate significant business and consumer activities.

Inpher Background

We are a US-based cryptography and machine-learning company with the conviction that encryption and privacy are foundational to the future of computing and commerce. Inpher applies years of academic research on Fully Homomorphic Encryption ("FHE") and secure Multi-Party Computation ("MPC") into commercially-ready applications that financial institutions are using in production today.[3]

Inpher's customers include some of the world's largest multinational financial institutions that use our software platform for privacy-preserving analytics and computation with mathematical guarantees of data security and sovereignty. This 'secret computing' technology enables compliant data processing across siloed departments, cross-jurisdictional and cross-industry information sharing, and zero-knowledge cloud computing, as the host never 'sees' the data nor has access to the keys. Our legal and public policy department facilitates public education on privacy-preserving technologies and advocates for data protection by design, global privacy, and algorithmic accountability.

---

[1] Office of the Privacy Commissioner of Canada, *Consultation on transfers for processing – Reframed discussion document* (Proposed on Apr. 9, 2019 for Aug. 6, 2019 deadline), https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/consultation-on-transfers-for-processing/#fn3

[2] Privacy Act, RSC 1985, c. P-21, https://www.canlii.org/en/ca/laws/stat/rsc-1985-c-p-21/latest/rsc-1985-c-p-21.html

[3] Inpher, *Case Studies*, https://www.inpher.io/case-studies-1#case-studies

We support the OPC's decision to re-examine the efficacy of its current guidelines on data transfers. Since the OPC last released its guidelines on this matter in 2009,[4] international privacy standards have been raised to address complexities in emerging technologies and novel risks in data processing. To combat skyrocketing data breaches[5] and abuses of personal information, extraterritorial laws are embracing privacy-enhancing technologies ("PETs") as a way to protect individual rights against preventable risks.

The EU General Data Protection Regulation ("GDPR") requires data controllers and processors to implement 'data protection by design and default,'[6] affirming the importance of PETs in cross-jurisdictional data transfers. Moreover, notable intergovernmental bodies including the United Nations ("UN")[7], Organization for Economic Co-operation and Development ("OECD"),[8] and European Union Agency for Cybersecurity ("ENISA")[9] have all promoted the implementation of PETs to minimize risks to privacy and data protection.

We believe it is timely and critical for the OPC to address shortcomings in PIPEDA's reliance on consent and contractual clauses as its primary mechanisms for consumer privacy. These privacy "self-management"[10] tools—privacy policies and service agreements—can be easily overridden by bad or negligent actors. Consequently, unauthorized access to data often goes undetected until it is too late to contain the information leak.

Rapidly evolving cryptographic PETs such as FHE and MPC offer incorruptible *ex ante* privacy safeguards against unauthorized access by intermediaries and third parties.[11] The regulatory

---

[4] OPC, Guidelines for processing personal data across borders (Jan. 2009), https://www.priv.gc.ca/en/privacy-topics/airports-and-borders/gl_dab_090127/

[5] IBM, *IBM Study Shows Data Breach Costs on the Rise; Financial Impact Felt for Years* (Jul. 23, 2019), https://newsroom.ibm.com/2019-07-23-IBM-Study-Shows-Data-Breach-Costs-on-the-Rise-Financial-Impact-Felt-for-Years

[6] EU General Data Protection Regulation (GDPR) Article 25, *Data protection by design and by default*, http://www.privacy-regulation.eu/en/article-25-data-protection-by-design-and-by-default-GDPR.htm.

[7] United Nations, *UN Handbook on Privacy-Preserving Computation Techniques*, http://publications.officialstatistics.org/handbooks/privacy-preserving-techniques-handbook/UN%20Handbook%20for%20Privacy-Preserving%20Techniques.pdf

[8] OECD, *Revised Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*: "The Joint Proposal also incorporates various recent data protection measures, including information management strategies, employee training, and appointment of individuals who are responsible for an organization's data protection practices, codes of practice, audits, privacy enhancing technologies, and privacy impact assessments." https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

[9] European Union Agency for Cybersecurity (ENISA), *Privacy Enhancing Technologies 'Time to Adopt PETs'*, https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies

[10] Daniel J. Solove, *Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1879, 1880 (2013)

[11] Yehuda Lindell & Benny Pinkas, *Secure Multiparty Computation for Privacy-Preserving Data Mining*, The Journal of Privacy and Confidentiality (2009), http://jpc.cylab.cmu.edu; *ING Belgium Sees Opportunities for 'Secret' Sharing of Encrypted Data*¸ The Wall Street Journal (Jun. 1, 2017), https://blogs.wsj.com/cio/2017/06/01/ing-belgium-sees-opportunities-for-secret-sharing-of-encrypted-data/

focus on data transfers should shift to implementing PETs that can keep data securely encrypted in storage, transit, and *in-use* (while being processed), so that sensitive plaintext information is not exposed to those who may violate their data-sharing agreement or fiduciary obligations to engage in misconduct.

Therefore, we urge the Privacy Commissioner to adopt modified guidelines that encourage the development and standardization of PETs. It is now imperative for organizations to institute PETs as structural safeguards to achieve robust privacy protections in domestic and international data transfers for processing. The soft-touch approach to privacy based on 'notice and consent' has consistently failed to protect consumers and to uphold global data protection values.

Regulatory standards for encryption-based privacy safeguards will obviate the risk of personal data being transferred and exposed to a jurisdiction with inadequate rights and remedies for privacy. Innovation and wider application of PETs in data transfers will benefit institutions, consumers, and regulators[12] by enabling secure analytics and information oversight without sacrificing data privacy for data utility, or vice versa.

Deficiencies in PIPEDA's Consent Mechanism

Cryptographic technologies can protect data at rest, in transit, and *in-use* with mathematical certainty, whereas mere operational policies to monitor consent and authorizations cannot ensure absolute privacy firewalls.

Updated OPC guidelines on data transfers should require companies to adopt PETs that encrypt personal information during all stages of the processing lifecycle, rather than relying on consumer consent at the time of collection. PIPEDA's current consent mechanism is insufficient to protect consumer privacy in the traditional online ecosystem where data can take on new and unforeseen utilities and insights.

Advances in MPC and FHE allow functions to be performed on encrypted data without revealing the underlying information. PETs can thus ensure that privacy will continue to be protected during the transfer, storage, and processing of data—whilst preserving the data's valuable utility. Application of such privacy-preserving technologies obviates traditional tradeoffs in privacy and analytical precision (for example, with differential privacy methods), and allow secure collaboration across data hosts.

Design-based privacy programs also eliminate the information asymmetry between consumers and businesses, which has perpetuated bad practices through unfair and deceptive privacy policies. PETs lift the consumers' burden to read thousands of pages of privacy policies and fineprints in order to protect their own interests. They instill organizational accountability by

[12] Szeto, Martin and Akbar Miri, *Analysis of the Use of Privacy-Enhancing Technologies to Achieve PIPEDA Compliance in a B2C e-Business Model*, Eighth World Congress on the Management of eBusiness (WCMeB 2007) (2007): 6-6.

requiring businesses to implement better technological safeguards and protective measures for privacy.

No Oversight of Contractual Safeguards

Contractual safeguards established by Principle 4.1.3 of PIPEDA do not offer effective privacy protections in cross-border data transfers.[13] The provision requires organizations to use "contractual or other means to provide a comparable level of protection while the information is being processed by a third party." However, the OPC has neither assigned content to this rule with guidance on adequacy requirements, nor approved standard contractual clauses ("SCCs") for equivalent privacy protections in recipient jurisdictions of international data transfers.

The validity of SCCs for cross-border data transfers is currently being challenged by the European Court of Justice.[14] Contractual arrangements offer virtually no protection against foreign legal systems that provide limited judicial redress for data that has been transferred into that jurisdiction. This was highlighted by the *Schrems I* decision of the Court of Justice of the European Union ("CJEU") in 2015 that invalidated EU to U.S. data transfers under the Safe Harbor scheme.[15]

We also agree with the OPC's observation that its limited enforcement powers rarely provide the occasion for the Privacy Commissioner to examine contractual measures developed by organizations to give effect to Principle 4.1.3 of PIPEDA. As there is limited legislative authority for the Privacy Commissioner to audit and investigate data transfer contracts for adequate privacy protections in recipient countries, we urge the OPC to articulate guidelines for privacy-preserving business practices which will impose baseline technical requirements to structurally embed strong data protection principles across jurisdictions.

Authority to Oversee Privacy-Preserving Business Practices

To stimulate and effectuate privacy-preserving business practices, we believe the OPC should seek wider oversight authority from Parliament to prevent and correct data practices before they can result in a breach or misuse.

The authority to engage in proactive enforcement to mitigate violations *ex ante* is an indispensable safeguard for individual rights. Without the certainties provided by order-making powers—to investigate, mandate action, suspend risky practices, prohibit misrepresentations,

---

[13] Principles Set Out in the National Standard of Canada Entitled Model Code for the Protection of Personal Information, CAN/CSA-Q830-96, PIPEDA 4.1.3. "An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party."

[14] ECJ Case C-311/18
Data Protection Commissioner v Facebook Ireland and Maximillian Schrems ("Schrems II")

[15] Case C-362/14, Maximillian Schrems v. Data Protection Comm'r, 2015 ECLI 650, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=en&mode =lst&dir=&occ=first&part=1&cid=702383.

and sanction violators—the OPC can only act reactively, where the privacy harm has already been inflicted. Robust order-making powers are a bulwark against enforcement blind spots, because it would provide the OPC with a toolkit to identify, prevent, and redress harms.

In a leading democracy where threats to personal privacy require expeditious and competent action, it makes little sense that the OPC must submit to the discretion of the court for a judicial enforcement of its recommendations. There is an urgent need for legislative reform to give the OPC order-making powers, which is integral to the Privacy Commissioner's ability to protect privacy rights, mandate business compliance with PIPEDA, and implement privacy-enhancing practices.

Thank you for the opportunity to comment on this important consultation. If you have any questions regarding our comments, or if Inpher could be of any assistance, please do not hesitate to contact me at sunny@inpher.io.

Sincerely,

Sunny Seon Kang
Senior Privacy Counsel, Head of Policy
Inpher, Inc.