Information and Privacy
Commissioner of Ontario
Commissaire à l'information et à la
protection de la vie privée de l'Ontario

VIA ELECTRONIC MAIL & ONLINE SUBMISSION

April 12, 2024

Gareth Sansom
Deputy Director, Technology & Analysis
Criminal Law Policy Section
Justice Canada
284 Wellington Street
Ottawa, Ontario K1A 0H8

Dear Gareth Sansom:

RE: Consultation on the *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*

Dear Mr. Sansom,

Thank you for inviting the Information and Privacy Commissioner of Ontario (IPC) to provide feedback on the consultation paper on the *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence* (Protocol).

The Department of Justice indicates that the Government of Canada has signed but has yet to ratify the Protocol. If the government ratifies the Protocol without any reservations, foreign investigative entities will be able to obtain subscriber information and traffic data associated with anyone in or from Canada from any communication service provider for the purpose of investigating any crime without necessarily having to seek any form of prior judicial authorization.[1] This would include, but not be limited to, cybercrime. The Department of Justice has also stated in its consultation documents that it is undertaking a comprehensive domestic review of the Protocol and existing Canadian laws, while also consulting with experts and engaging provinces and territories to inform the next steps.

As a modern and effective regulator, the IPC actively works to build trust in next-generation law enforcement capabilities within the province of Ontario. We recognize that the Protocol could significantly extend the capabilities of "competent authorities" (hereafter "investigative entities") in Ontario and potentially modify how foreign investigative entities can access electronic evidence that is retained in Ontario or held by Ontario organizations.

[1] The Protocol will also empower investigators to obtain internet domain name registration information, though this is not raised in the IPC's response to this consultation.

In this response, we discuss some of the potential impacts of the Protocol on Ontarians' privacy rights. We strongly support the positions the Office of the Privacy Commissioner of Canada (OPC) has put forward in its response to the Department of Justice's consultation. We also provide some specific jurisdictional information associated with the Protocol, including those related to our oversight powers as Ontario's information and privacy regulator. Finally, we recommend the Government of Canada engage with other relevant provincial or federal institutions to fully assess how other laws and operational practices may intersect with the questions posed in this consultation and the Protocol more generally.

Mandate of the Information and Privacy Commissioner of Ontario

The Commissioner is an independent officer of the Legislature who is appointed by and reports to the Legislative Assembly of Ontario. The IPC oversees compliance with Ontario's access and privacy legislation, which includes the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), the *Personal Health Information Protection Act* (PHIPA), Part X of the *Child, Youth and Family Services Act* (CYFSA), and the privacy framework under the *Anti-Racism Act* (ARA).

The IPC's mandate covers provincial and municipal government institutions subject to FIPPA and MFIPPA, respectively. This includes police services boards, police services, other Ontario government-based investigative entities that have law enforcement powers and duties as part of various municipal and provincial institutions, and the broader public sector.[2] Our mandate does not generally extend to government entities established by governments outside of Ontario or to any private sector organizations engaged in commercial activity.[3]

Potential Impact of the Protocol on Ontarians' Privacy Rights

Ontario is the most populous province in Canada. The Protocol's implementation could significantly impact the privacy rights of Ontarians when requests are made by foreign investigative entities to Ontario organizations. In the case of private sector service providers operating in Ontario that retain Ontarians' personal information, these businesses would be subject to the federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) and overseen by the OPC. In other cases, such as where Ontario public sector organizations may operate communications service providers or offer other services relevant to the Protocol, then FIPPA or MFIPPA would apply and be overseen by the IPC. In either situation, if the Protocol is ratified then Ontarians can

[2] See: s. 1 of the *Broader Public Sector Accountability Act*, 2010, for a listing of what institutions are included as part of the broader public sector in Ontario. In some situations, broader public sector institutions may operate as Communications Service Providers.

[3] The responsibility for overseeing compliance with privacy requirements by private sector organizations operating in Ontario falls to the OPC.

expect to see a significant increase in the volume of requests for communication-related information by foreign and Canadian investigative entities, with a corresponding impact on the right to privacy.

The IPC strongly supports the positions taken by the OPC in its March 22, 2024, submission to the Department of Justice as part of the consultation on the Protocol. In particular, the IPC agrees that, barring truly exceptional circumstances, subscriber information should only be accessible with judicial authorization, in keeping with Canadian Charter rights and values as interpreted by the Supreme Court of Canada.[4] Article 7 of the Protocol would appear to allow foreign investigative entities to gain direct access to subscriber information about Ontarians without judicial authorization, thereby circumventing the firmly entrenched rights and values of our own land. Accordingly, we support the OPC's recommendation that Canada should consider opting out of Article 7. We also recommend that traffic data should only be accessible with judicial authorization. Ultimately, it is critical that protective guardrails are in place, including in the form of *ante* and *ex post* reviews by an independent authority.

Moreover, the IPC stands by the adoption of strong safeguards pronounced by the Global Privacy Assembly's October 2021, *Resolution on principles for governmental access to personal data held by the private sector for national security and public safety purposes*, which our office proudly co-sponsored.[5] The principles outlined in this resolution, including independent oversight and transparency, should help inform Justice Canada's evaluation of the adequacy of the safeguards proposed in Articles 13 and 14 of the Protocol. This is important as it regards *both* subscriber and traffic data as having significant privacy implications, particularly when pieced together, in terms of what they can potentially reveal about the private actions, thoughts, and beliefs of individuals.

We appreciate that the Protocol's intent is to enhance domestic and foreign investigative entities' ability to obtain electronic information for investigations. However, we note with some concern that there is a possibility of jurisdictions with less robust rule of law to compel information from Ontario public or private sector organizations in situations where a Canadian investigative entity may be unable to obtain a similar order. As such, the IPC would encourage the federal government to ensure Canadian Charter-based standards that must be met by both foreign jurisdictions and Ontario investigative entities when seeking access to personal information held by Ontario-based organizations. Absent appropriate rule of law or proportionality standards, there is a risk that the Protocol may have the effect of infringing upon the human rights of persons whose data is obtained

---

[4] See the Supreme Court's decision in *R v. Spencer*, 2014 SCC 43, and the more recent decision in *R. v. Bykovets*, 2024 SCC 6.

[5] See: Global Privacy Assembly "Adopted resolution on Government Access to Data, Privacy and the Rule of Law: Principles for Governmental Access to Personal Data held by the Private Sector for National Security and Public Safety Purposes" (October 2021) at https://globalprivacyassembly.org/wp-content/uploads/2021/10/20211025-GPA-Resolution-Government-Access-Final-Adopted.pdf.

from Ontario-based public or private sector organizations at the hands of foreign jurisdictions that do not share our free and democratic values.

Transparency and accountability in the sharing of evidence with foreign authorities

The IPC believes that Ontarians would benefit from transparency when or if Ontario-based organizations receive requests for personal information from investigative entities. The OPC has advocated for publicly reporting how frequently Canadian private sector organizations receive, and are responsive to, requests from investigative entities with the intent of making public the regularity of these requests and disclosures.[6] In light of the likely increased volume of Ontarians' personal information which may be disclosed to foreign investigative entities, the IPC would support a requirement that organizations develop and issue public transparency reports, including when receiving requests from Ontario and foreign investigative entities.

The IPC does not have statutory oversight of private sector organizations but notes that any data breaches that pose real risk of significant harm to individuals must be reported to the OPC under federal privacy law. Provincial and municipal organizations are required, under FIPPA and MFIPPA, respectively, to adhere to security standards.[7] However, they are not statutorily required to report data breaches to the IPC. Public sector institutions are strongly encouraged to inform the IPC when they have experienced a data breach. However, not all significant breaches affecting Ontario's public sector organizations are reported to the IPC. This lack of reporting represents a significant gap in effective oversight.

Responses to Jurisdictional Questions

Where the Protocol applies to foreign investigative entities making requests of private sector Ontario organizations, we advise the Department of Justice to engage the OPC for information about how PIPEDA would apply in those situations, including the kinds of redress available to residents of Ontario if their personal information is requested by or disclosed to foreign agencies and if their privacy is breached in the process.

For the purposes of the Protocol, the IPC only has oversight powers and responsibilities concerning investigative entities that are institutions or part of institutions regulated under Ontario's access and privacy legislation. Pursuant to this, we note the following:

- FIPPA and MFIPPA set rules for the collection, use, disclosure, retention, and protection of personal information in the custody or control of provincial and municipal institutions, respectively. This includes rules for providing notice, ensuring accuracy, enabling

[6] See: "Transparency Reporting by Private Sector Companies" at https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2015/transp_201506/.
[7] See: MFIPPA s. 47 (g) and FIPPA s. 60 (d). See also, O/Reg 460 4(1).

individuals' right to access and correct their personal information, and disclosure of personal information for the purposes of law enforcement (including when it comes to disclosures to foreign law enforcement agencies);[8]

- The IPC has limited power to investigate or issue privacy-related orders under these acts.[9] When data has already been disclosed out of the province, the commissioner's powers may be further limited if the receiving organization is not regulated under Ontario law. In these situations, the IPC faces even greater challenges in its abilities to enforce the laws without explicit authority to share information with, or coordinate with, other regulators undertaking investigations in other jurisdictions.[10]

- The IPC does have power to compel the production of records and issue binding orders in cases involving individual access and correction appeals, but institutions – particularly those performing law enforcement functions – can avail themselves of various statutory exemptions that significantly restrict the rights of individuals in such cases;[11]

- FIPPA and MFIPPA recognize that institutions may, in some circumstances, disclose personal information to foreign law enforcement bodies when a treaty or other international agreement exists.[12] While institutions are advised to consider informing individuals when a disclosure is made to an investigative entity, they may sometimes be limited in their ability to do so based on specific constraints in FIPPA / MFIPPA, the *Criminal Code*, or other relevant legislation.

Finally, the consultation document envisions the possible uses of automated processing of personal information to make decisions. The IPC and all other Canadian privacy commissioners have asserted that accountability for automated decision-making systems rests with the relevant organization developing and using such systems and have recommended strong guardrails to ensure their activities are trustworthy and privacy protective.[13] The IPC also notes that automated decision making, in the context of

[8] See Part II of MFIPPA and Part III of FIPPA.
[9] See, for example, section 46(b) of MFIPPA and section 59(b) of FIPPA.
[10] See: "RE: Schedule 2 of Bill 149, the Working for Workers Four Act, 2023" at https://www.ipc.on.ca/wp-content/uploads/2024/02/2024-02-07-bill-149-committee-submission.pdf page 6.
[11] See Part I of MFIPPA and Part II of FIPPA.
[12] See: s. 42(1) of FIPPA and s. 32(1) of MFIPPA.
[13] See "Principles for responsible, trustworthy and privacy-protective generative AI technologies" at https://www.priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/gd_principles_ai/.

investigative entities' activities, can represent 'high risk' activities, which should result in a meaningful human review of outputs by a qualified expert and be subject to enhanced accountability and transparency requirements accordingly.

Conclusion

Our comments in this submission are limited to matters over which the IPC has jurisdiction. We recommend that the federal government also consult with other relevant provincial institutions, municipal agencies, and members of the broader public and private sectors to gain a fuller appreciation of their views and operational practices.

Thank you again for consulting with the Information and Privacy Commissioner of Ontario as the Government of Canada continues to undertake this important consultation concerning the Protocol.

Sincerely,

Michael Maddock
Assistant Commissioner, Strategic Initiatives and External Relations
Information and Privacy Commissioner of Ontario