Expediting Human Rights Abuses: A Constitutional and Human Rights Analysis of the Second Additional Protocol to the *Budapest Convention on Cybercrime*

Kate Robertson and Verónica Arroyo
Citizen Lab, Munk School of Global Affairs & Public Policy
University of Toronto
Submission to the Department of Justice Consultation on the Second Additional Protocol
March 2024

munkschool.utoronto.ca

At Trinity College
1 Devonshire Place
Toronto, ON
Canada M5S 3K7
T: 416.946.8900 F: 416.946.8915

At the Observatory
315 Bloor Street West
Toronto, ON
Canada M5S 0A7
T: 416.946.8929 F: 416.946.8877

At the Canadiana Gallery
14 Queen's Park Crescent West
Toronto, ON
Canada M5S 3K9
T: 416.978.5120 F: 416.978.5079

Part 1. Introduction

1. The Citizen Lab at the Munk School of Global Affairs & Public Policy, University of Toronto ("Citizen Lab"), is an interdisciplinary laboratory which focuses on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security. Our work relies on a "mixed methods" approach to research combining practices from political science, law, computer science, and area studies. Citizen Lab research has included, among other work: investigating digital espionage against civil society; documenting Internet filtering and other technologies and practices that impact freedom of expression online; analyzing privacy, security, and information controls of popular applications; and examining transparency and accountability mechanisms related to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

2. We welcome the opportunity to comment on Canada's consideration of the *Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence* ("the Protocol" to the "Budapest Convention"), and the question of whether Canada should ratify the Protocol. This submission outlines core deficiencies in the Protocol, which underpin our **recommendation that Canada decline to ratify the Protocol**.

3. By way of background, the Budapest Convention is an existing international treaty that requires that its signatories develop common criminal laws and investigative procedures related to the investigation and prosecution of cybercrime. For example, the Budapest Convention requires signatories to develop the capability to investigate, preserve, and gather specified forms of electronic evidence.

4. The Protocol would impose an array of new obligations on State signatories to reform their laws authorizing the cross-border sharing of specified electronic evidence in law enforcement investigations. The Protocol would reform cross-border data sharing for **subscriber information** (e.g. name, address, phone number, and billing address), **domain name registration data**, **stored computer data** (including private communications), and **transmission (traffic) data**.

5. For many years, Citizen Lab research has examined transparency, accountability, and human rights considerations applicable to the collection, use, and sharing of personal

information by State authorities, including law enforcement authorities (LEAs), and private companies. This research has included examination of the relationship between governments and private companies, and novel technologies used in law enforcement investigations or national security monitoring or surveillance programs.

6. Citizen Lab research also examines how activists and dissidents living in Canada are impacted by digital transnational repression.[1] Digital transnational repression refers to the various ways that individuals continue to be harassed and targeted online by authoritarian governments, even after they leave their country of origin. Although transnational repression "is not a new phenomenon, such tactics are expanding through the market growth for digital technologies and the spread of Internet-connectivity, among other factors."[2]

7. A number of cross-border data sharing instruments applicable to law enforcement investigations either exist, or are under negotiation at this time.[3] The potential expansion of the Budapest Convention through the Protocol is only one of several new cross-border data sharing regimes under active consideration by States around the world. These often discordant layers of legal process add to the risk and complexity of the challenge that the international community faces when assessing how to oversee cross-border law enforcement activities.

8. This submission will outline how the Protocol normalizes and condones inadequate human rights standards amongst its signatories. In doing so, the Protocol threatens human rights around the world, including invasions of privacy; unfair, unaccountable, or discriminatory treatment by State authorities; and an expanding landscape for digital transnational repression. **Core human rights deficiencies in the Protocol underpin our recommendation that Canada decline to ratify the Protocol**. Instead, we recommend that Canada play a leadership role in prioritizing and committing to international efforts to address gaps in human rights compliance, and to invest in fully

[1] Noura Al-Jizawi, Siena Anstis, Sophie Barnett, Sharly Chan, Niamh Leonard, Adam Senft, and Ron Deibert, "Psychological and Emotional War: Digital Transnational Repression in Canada," Citizen Lab Research Report No. 151, University of Toronto, March 2022.
[2] *Ibid* at page 1.
[3] These legal instruments include, for example, various bilateral or multilateral mutual legal assistance treaties, the EU's E-Evidence Regulation and Directive, and agreements or negotiations under the USA's *Clarifying Lawful Overseas Use of Data Act* (H.R. 4943).

resourcing cross-border data-sharing protocols that require and harmonize robust human rights protections from all signatories.

9. The submissions in this brief are set out in five parts. **Part 2** summarizes the human rights dangers associated with the Protocol. **Part 3** details the core human rights deficiencies in the Protocol, focusing on Articles 6-9, 12, 13, and 14. **Part 4** examines potential policy rationales surrounding the Protocol, and submits that eliminating or reducing human rights safeguards to expedite large volumes of cross-border data sharing is disproportionate and unnecessary to those potential objectives. **Part 5** situates the Protocol within Canada's existing human rights framework, and addresses why Canada must prioritize filling existing gaps in human rights protections in Canada, which are applicable to cross-border police investigations. Finally, **Part 6** concludes with several recommendations to accompany the overarching recommendation that Canada should decline to ratify the Protocol.

Part 2. The Potential Impact of the Protocol: Expediting Human Rights Abuses

10. This section addresses how the Protocol poses serious human rights dangers and undermines the development of international human rights norms applicable to digital rights in cross-border investigations. The Protocol does so by normalizing, and even paving the way for, data-sharing protocols that are not safeguarded by robust human rights protections.

11. At present, the predominant method for LEAs to gather evidence from another country is through reliance on mutual legal assistance treaties ("MLATs") that are negotiated either bilaterally or multilaterally between States. Under MLATs, the typical method of gathering and sharing electronic evidence is through court-issued, judicially authorized orders to seize and disclose electronic records that are necessary to a foreign criminal investigation.

12. The Protocol proposes to establish alternative mechanisms for LEAs to access and share private information across borders. As summarized in Canada's consultation paper, the "Protocol would create a more direct process for requesting electronic evidence, providing alternatives to the mutual legal assistance channels which are generally not well-equipped to handle high volumes of requests requiring expeditious

production."[4] However, as will be discussed in Part 3 of this submission, the Protocol's proposed method of expediting higher volumes of cross-border sharing of evidence is generally by eliminating or diminishing human rights safeguards, including the obligation to obtain prior, independent judicial authorization when seizing private information and sharing it with foreign LEAs. Rather than "establishing high standards, the protocol prioritizes law enforcement access at almost every turn."[5]

13. The reduction or elimination in independent oversight and other safeguards poses serious human rights dangers. Canadian authorities have witnessed first-hand the tragic and horrific consequences that inappropriate data sharing with foreign authorities can inflict on even innocent persons. The detention, rendition, and torture of Maher Arar after Canadian authorities shared inappropriate and inaccurate information with US authorities provides a "chilling example of the dangers of unconditional information sharing."[6] The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar properly recognized that information sharing with foreign authorities "is a highly sensitive and potentially risky exercise."[7]

14. Under the Protocol, the framework for cross-border data sharing to foreign authorities for criminal investigative purposes carries similar dangers and complexities:

    a. The Protocol contemplates sharing information about individuals in Canada with foreign LEAs who are investigating any number of criminal offences. This could include offences under foreign laws in relation to activities that would not be considered criminal in Canada, or other discriminatory, disproportionate and overbroad criminal laws that would not survive constitutional scrutiny in Canadian courts. This could include, for example,

---

[4] Department of Justice Canada, Consultation on the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (December 2023).
[5] Tamir Israel & Katitza Rodriguez, "On New Cross-Border Cybercrime Policing Protocol, a Call for Caution" *Just Security* (13 May 2022), online: <https://www.justsecurity.org/81502/on-new-cross-border-cybercrime-policing-protocol-a-call-for-caution/>.
[6] *Wakeling v United States of America*, 2014 SCC 72 at para 104 [per Karakatsanis J. writing in dissent on other grounds].
[7] *Report of the Events Relating to Maher Arar: Analysis and Recommendations* (Ottawa: Commission of Inquiry Into the Actions of Canadian Officials in Relation to Maher Arar, 2006) at page 74, online (pdf): <https://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/eng/AR_English.pdf>.

laws criminalizing political dissent and expression, public interest security research, sexual orientation, or abortion care.

b. Without robust human rights guardrails, States may abuse the expedited data-sharing regime under the Protocol to track, de-anonymize, and surveil human rights dissidents living in Canada or elsewhere. For example, the Protocol may pave the way for investigations by foreign governments into seemingly legitimate allegations of criminal wrongdoing, but which are actually capricious or fabricated allegations leveled against dissidents, journalists or the political opposition to chill or punish free expression. One of the central mechanisms of transnational repression is the co-optation of "other countries to act against a target through detention, unlawful deportation, and other types of forced renditions, ***which are authorised through pro forma but meaningless legal procedures***."[8] The Protocol provides another opportunity for States to leverage legal procedures in rights-respecting countries in order to engage in acts of transnational repression.[9]

c. The Protocol also exposes individuals to potential invasions of privacy, with corresponding free expression harms, by creating risks that their personal information will be gathered or seized from telecommunication providers, social media companies, or a host of other online app and service providers without sufficient justification. Independent, prior judicial authorization (to verify that there is a reasonable, factual justification for disclosure), is a core

[8] Council of Europe, Parliamentary Assembly, *Transnational repression as a growing threat to the rule of law and human rights*, Documents, Doc 15787 (2023), online (pdf): <https://www.ecoi.net/en/file/local/2093307/doc.+15787.pdf>.

[9] This risk was identified by Canada during negotiations surrounding the United Nations draft Cybercrime Convention. Canada's submission states that "...the current Article 35 on international cooperation obligates State Parties to cooperate on Convention offences, as well as "serious crime." This term is likely to be defined as an offence punishable by a certain number of years of imprisonment in a state's domestic criminal law (three or four years are the current proposals). This could effectively obligate and/or enable international cooperation and mutual legal assistance, under the auspices of the Convention, for any conduct punishable by three or four years imprisonment under domestic law when a computer system/ICT device is involved, a scope of conduct subject to the whims of what a government may legislate as a 'serious crime' at any time": *Proposal by Canada on behalf of a group of 66 States and the European Union to the Ad Hoc Committee on Cybercrime (AHC) to further define the scope of the draft Convention* (5 February 2024), online (pdf): <https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Concluding_session/Submissions/Canada_3.3_05.02.2024.pdf>.

backbone of privacy and free expression rights in a free and democratic society. However, it is treated as entirely optional by the Protocol. Independent oversight and review is a longstanding and sustainable mechanism for enabling law enforcement objectives to be balanced and achieved, while protecting public confidence that private information will not be disclosed in circumstances where intrusions are not reasonably justified.

d. Inadequate data-sharing protocols also expose individuals to risks that their personal information will be subjected to inappropriate uses by foreign LEAs, such as processing in discriminatory algorithmic policing technologies (including what is often referred to as predictive policing programs). The growing use of algorithmic policing technologies by LEAs, and the absence of corresponding clear, necessary, and proportionate limits in countries around the world, are an emergent threat to human rights for individuals and communities around the world. The Protocol further endangers these rights by enabling LEAs to fuel algorithmic technologies with new data sources that are not accompanied by necessary scrutiny and controls to prevent rights violations caused by disproportionate and unjustified surveillance, and/or discriminatory, unreliable, or inaccurate inferences generated by algorithmic tools.[10]

15. The history of abuse of INTERPOL's Red Notice program illustrates the danger of cross-border policing mechanisms which fail to make adherence to robust human rights standards a precondition to participation, and which are governed by inadequate and under-resourced oversight systems. INTERPOL is an international data-sharing organization that intermediates between policing agencies from member countries around the world. A Red Notice is one type of request issued by INTERPOL to

[10] Kate Robertson, Cynthia Khoo, and Yolanda Song, "To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada" (September 2020), Citizen Lab and International Human Rights Program, University of Toronto. See also, Opinion 1/15, *Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada* [2017], ECLI:EU:C:2017:592 at paras 168-174 and 232 (3)(b) and 3.(b), where the European Court of Justice (CJEU) ruled that an agreement between the EU and Canada was incompatible with EU law, in part due to the absence of specific safeguards concerning the automated processing of data shared under the agreement. Here, the Protocol also does not address the concerns raised by the CJEU. See also, *Joint Civil Society Response to Discussion Guide on a 2nd Additional Protocol to the Budapest Convention on Cybercrime* (28 June 2018) at pages 27-29, online (pdf): <https://www.eff.org/files/2018/07/31/globalcoalition-civilsociety-t-cy_201816-final1.pdf>.

law enforcement worldwide, which is a request to locate and arrest a person pending extradition, surrender, or similar legal action. Member countries apply their own national laws in deciding whether to issue an arrest warrant, or whether to arrest a person who is subject to a Red Notice. The Red Notice program has come under intense international criticism due to repeated instances of State abuses of the program. For example, INTERPOL has issued Red Notices against anti-corruption advocates, political activists, refugees, opposition politicians who were publicly critical of State conduct, a professional athlete and refugee who had voiced government criticism, human rights dissidents living in exile, and more.[11]

16. While INTERPOL has implemented some changes, there are continuing calls for reform in light of ongoing gaps and abuses of INTERPOL's existing oversight structure.[12] For example, in 2022, a Bahraini dissident was extradited by Serbia (a country that has already ratified the Protocol) to Bahrain following an INTERPOL Red Notice, even though the extradition directly contravened an injunction that had been issued by the European Court of Human Rights.[13] Other recent calls for reform urge attention towards abuses of "a different Interpol mechanism to round up critics from abroad by

[11] Sam Meachem, "Weaponizing the Police: Interpol as a Tool of Authoritarianism", Harvard International Review, April 11, 2022 <https://hir.harvard.edu/weaponizing-the-police-authoritarian-abuse-of-interpol/>; Helen Davidson, "He's free, but who's to blame for Hakeem al-Araibi's ordeal?", *The Guardian* (12 February 2019), online: <https://www.theguardian.com/sport/2019/feb/12/hes-free-but-whos-to-blame-for-hakeem-al-araibis-ordeal>; Serdar San, "Transnational policing between national political regimes and human rights norms: The case of the Interpol Red Notice system", (2022) 26:4 Theoretical Criminology 601 at pages 601-619; Stockholm Centre for Free Expression, "Turkey's Abuse of INTERPOL: How Erdoğan Weaponized the International Criminal Police Organization for Transnational Repression" (August 2021), online (pdf): <https://stockholmcf.org/wp-content/uploads/2021/08/SCF-Interpol-Abuse-Report_2021.pdf>; Council of Europe, *Transnational repression as a growing threat to the rule of law and human rights*.

[12] European Parliament, Policy Department for External Relations, "Study: Misuse of Interpol's Red Notices and impact on human rights – recent developments" (January 2019), online (pdf): <https://www.statewatch.org/media/documents/news/2019/feb/ep-study-interpol-red-notices.podf.pdf>.

[13] Dominic Dudley, "European Human Rights Court Calls On Serbia To Explain Extradition Of Bahraini Dissident"", *Forbes* (26 January 2022), online: <https://www.forbes.com/sites/dominicdudley/2022/01/26/european-human-rights-court-calls-on-serbia-to-explain-extradition-of-bahraini-dissident/?sh=6cbd7da6615e>; Ruth Michaelson, "'Illegal' extradition of Bahraini dissident from Serbia calls Interpol's role into question", *The Guardian* (16 February 2022), online: <https://www.theguardian.com/global-development/2022/feb/16/extradition-of-bahraini-dissident-from-serbia-calls-interpol-role-into-question>.

misusing Interpol's Stolen and Lost Travel Document (SLTD) system, which is subject to less internal scrutiny and checks."[14]

17. INTERPOL is not subject to the oversight of any international judicial authority, and instead relies on a committee created by its own processes for oversight: the Commission for the Control of INTERPOL's Files (the CCF).[15] INTERPOL's Secretary General Juergen Stock recently described that INTERPOL is limited in its capacity to better protect individuals from State abuses of the Red Notice program.[16] His comments underscore the risks surrounding international cooperation mechanisms for policing across borders which are governed by weak or under-resourced oversight mechanisms and human rights controls. The circumstances have raised concern that the "abuse of Interpol's cooperative policing mechanism is a worrying case study in a broader effort by autocrats to capture international institutions and weaponize them against global democracy."[17]

18. The Protocol raises similarly grave concerns by proposing an international cross-border data sharing regime that also fails to require robust digital human rights commitments and standards, as will be further outlined below in Part 3, and by deferring to the national laws of signatories to define those standards.

---

[14] Ali Yildiz & Ben Keith, "After Spotlight on Red Notices, Turkey is Abusing Another Interpol Mechanism", *Just Security* (13 July 2023), online: <https://www.justsecurity.org/87260/after-spotlight-on-red-notices-turkey-is-abusing-another-interpol-mechanism/>. See also, regarding the potential for abuse in regards to INTERPOL's blue notice system (blue notices seek to collect additional information about a person's identity, location or activities in relation to a criminal investigation"): INTERPOL Commission for the Control of INTERPOL's Files, *Activity Report of the Commission for the Control of INTERPOL's Files for 2021* (2021), CCF/122/12 at para 16: indicating that as of its (most recent) annual report in 2021, the CCF was reviewing whether there is potential for abuse or abuse of INTERPOL's blue notice system.

[15] European Parliament, "Misuse of Interpol's Red Notices and impact on human rights": recommending the need for independent oversight of the CCF (at pages 32-33). The report states that "...both written sources and interviews with governmental and non-governmental organisations suggest that Interpol's vetting process remains inconsistent", and that "[a]buses continue to be observed in high-profile cases and ordinary cases alike.")

[16] Francois Murphy, "Interpol can't do much more to stop abuse of 'red notices', chief says", *Reuters* (28 November 2023), online: <https://www.reuters.com/world/interpol-cant-do-much-more-stop-abuse-red-notices-chief-says-2023-11-28/>.

[17] Meachem, "Weaponizing the Police".

19. The stakes are high for all people in Canada, but also for the human rights and safety of all people around the world. If the protections that mutual legal assistance norms and treaties are eliminated or diminished, "**much of the world's population may be left vulnerable to arbitrary and abusive data collection practices by domestic law enforcement agencies**."[18] Moreover, "far from being a hypothetical concern, both history and contemporary events show that the absence of legal restrictions on government access to data when that data is technically easily obtainable, quickly results in abuses of power, human rights violations, and political control."[19]

Part 3. Core Deficiencies in the Protocol: Mandatory Expediency and Optional Human Rights

20. Part 3 addresses core human rights deficiencies in the Protocol, including deficiencies identified by human rights experts and civil society organizations prior to the adoption of the Protocol in November 2021:

A. "Direct cooperation" provisions under Article 6 and 7 fail to require adequate *Charter* or human rights protections to safeguard anonymity, privacy, and free expression

21. Article 6 and 7 both would oblige signatories to pass laws facilitating "direct co-operation" between requesting State authorities and service providers/entities in the territory of the requested State:

    a. Article 6 would be applicable if criminal investigators in a requesting State seek to **de-anonymize the registrant behind a domain name** by obtaining information from an entity providing domain name registration services.

    b. Article 7 would oblige signatories to introduce the legislative measures necessary to empower its "competent authorities" to issue an order compelling the production of **subscriber information** directly to a service provider in the territory of a requested State. States must also pass laws to permit service providers in its own territory to directly receive and respond to a foreign order

[18] Christine Galvagna, "The Necessity of Human Rights Legal Protections in Mutual Legal Assistance Treaty Reform" (2019) 9:2 Notre Dame Journal of International & Comparative Law 57 at page 66.
[19] *Ibid*.

> compelling the production of subscriber data. The scope of Article 7 is broad, and could require a wide range of online or internet service providers (such as email, social media, or messaging app providers) to de-anonymize users, and provider other information referable to an individual's online activities, such as IP addresses. The definition of subscriber information is very broad, and could foreseeably be interpreted to include other sensitive information beyond subscriber identity, including "logon information, dynamic lP addresses, records of carrier-grade NAT (CGN) IP address, port number mappings, and location data."[20]

22. Only Article 7 permits State reservations at the time of ratification.

23. Articles 6 and 7 both fail to require independent oversight over direct co-operation procedures to safeguard privacy interests and free expression. The Protocol permits LEAs or prosecution authorities to act as the designated "competent authorities" that can issue direct requests or orders to a foreign service provider. Articles 6 and 7 also fail to incorporate mechanisms to enable the requested State to refuse the request if it is inconsistent with human rights, since service providers can simply elect to disclose the information before receiving approval the authorities of the requested State.[21]

24. Independent oversight of law enforcement's access to sensitive data, including the data at issue in Article 6 and 7, is a critical safeguard to protect privacy and free expression rights:

> Access to subscriber data will frequently reveal sensitive details regarding the daily lives of individuals—almost invariably so when the individuals in question are protected by immunities and privileges. **Unfettered access to subscriber**

[20] Electronic Frontier Foundation, EDRi, IT-Political Association of Denmark & Electronic Privacy Information Center, *Joint Civil Society Response to the provisional draft text of the Second Additional Protocol to the Budapest Convention on Cybercrime* (November 2019) at page 4, online (pdf): <https://rm.coe.int/civilsocietysubmission-t-cydraftsecondadditionalprotocol/168098bc6d>.

[21] As outlined by the European Digital Rights (EDRi) network, there is no mechanism in Article 7 that would enable a State to prevent a service provider from responding before authorities in the requested Member State have considered relevant grounds for refusal and made a decision about whether to refuse or uphold the order: EDRi, *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention* (2022), online (pdf): <https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf>.

data poses a dire threat to online anonymity and places whistleblowers, journalists, politicians, political dissidents, and others at risk.[22]

25. In a joint civil society response to the draft text of the Protocol, human rights organizations criticized the Explanatory Report to the Protocol's failure to accurately describe the privacy interests associated with subscriber data:

> Any online subscriber who does not want his or her speech connected to their permanent identity has an interest in anonymity. Online speakers may be concerned about political or economic retribution, harassment, or even threats to their lives; or they may use anonymity as part of their personal expression or self-development. The value of anonymity to free expression is broadly recognised. Librarians believe library patrons should have the right to read anonymously—an essential prerequisite for intellectual freedom and privacy. Publishers have fought to preserve the anonymity of their customers on the grounds that being known as a reader of controversial works can create a chilling effect. Anonymity allows journalists' sources to come forward and speak without fear of retaliation.
>
> David Kaye, the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, highlighted the importance that online anonymity plays in furthering free expression in digital contexts (A/HRC/29/32, paras 47 et seq). The European Court of Human Rights held that the right to private life encompasses an individual's interest in having her identity protected with respect to her online activity and that individuals maintain a reasonable expectation that their otherwise anonymous online activity will remain anonymous, even where the individual takes no steps to shield her IP address from third parties.[23]

---

[22] Derechos Digitales, Electronic Frontier Foundation, EDRi, the Samuelson-Glushko Canadian Internet Policy & Public Interest Clinic (CIPPIC), Fundación Karisma and Association of Technology, Education, Development, Research and Communication (TEDIC), *Privacy & Human Rights in Cross-Border Law Enforcement: Joint Civil Society Comment to the Parliamentary Assembly of the Council of Europe (PACE) on the Second Additional Protocol to the Cybercrime Convention (CETS 185)* (August 2021) at pages vi-vii, online (pdf): <https://www.eff.org/files/2021/08/17/20210816-2ndaddprotocol-pace-ver2-final.pdf>.

[23] Electronic Frontier Foundation et al, *Joint Civil Society Response* at page 4.

26. The Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, Freedom of Expression and the Internet notes the following connection between anonymity, privacy, and free expression:

> As far as freedom of expression is concerned, the violation of the privacy of communications can give rise to a direct restriction when—for example—the right cannot be exercised anonymously as a consequence of the surveillance activity. In addition, the mere existence of these types of programs leads to an indirect limitation that has a chilling effect on the exercise of freedom of expression.[24]

27. The Protocol is inconsistent with existing constitutional law in Canada requiring LEAs to obtain prior judicial authorization before obtaining subscriber information from a service provider.[25] Canada's consultation paper on the Protocol states that in *R v Spencer*, "[t]he SCC did not indicate that a court order was necessarily required [to obtain subscriber information], but it suggested that the requirement that there be a 'reasonable law' could be met by a court order."[26] This summary of *Spencer* fails to give full effect to the scope of the Court's ruling. The Supreme Court did not open the door in *Spencer* to the police gaining warrantless access to subscriber data from private companies. Quite the opposite, the Court closed this door. A police request to link a given IP address to subscriber information is, in effect, "a request to link a specific person (or a limited number of persons in the case of shared Internet services) to specific online activities."[27] The Supreme Court stated that this type of request "engages the anonymity aspect of the informational privacy interest by attempting to link the suspect with anonymously undertaken online activities, activities which have been recognized by the Court in other circumstances **as engaging significant privacy interests**."[28]

28. The Court held that in the circumstances of the case, "the police request to Shaw for subscriber information corresponding to specifically observed, anonymous Internet

[24] Organization of American States, Office of the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Freedom of Expression and the Internet*, OEA/Ser.L/V/II, CIDH/RELE/INF. 11/13, (2013) at para 150.
[25] *R v Spencer*, 2014 SCC 43.
[26] Canada, *Consultation on the Second Additional Protocol* (December 2023).
[27] *R v Spencer*, 2014 SCC 43 at para 50.
[28] *Ibid*.

activity engages a **high level of informational privacy**."[29] The Court also concluded that the breach of privacy in this case was "**serious**", given "anonymity is an important safeguard for privacy interests online."[30] This judicial guidance was not laying the groundwork for a warrantless seizure power. Warrantless searches and seizures are presumptively unreasonable, but are especially so when judicial supervision is feasible and available (there are no exigent circumstances),[31] and the privacy interests at stake are significant.[32] The Protocol's failure to require independent oversight is discordant with these principles.

29. These conclusions were reaffirmed by the Supreme Court in *R v Bykovets*, where the majority ruled that a police request from an online services provider for an IP address constitutes a search under section 8 of the *Charter*.[33] The Court recognized that an IP address is "the key that can lead the state through the maze of a user's Internet activity."[34] Information inferred from a device's Internet activity "can be deeply personal, including linking that activity to a particular user's identity."[35] Therefore, section 8 of the *Charter* ensures "that the veil of privacy all Canadians expect when they access the Internet is only lifted when an independent judicial officer is satisfied that providing this information to the state will serve a legitimate law enforcement purpose."[36]

30. As will be discussed in more detail below in Part 3(C), the Supreme Court's rulings are supported by related jurisprudence from the Court of Justice of the European Union, as well as the European Court of Human Rights.[37]

---

[29] *Ibid* at para 51.
[30] *R v Spencer*, 2014 SCC 43 at para 78.
[31] *Hunter v Southam*, [1984] 2 SCR 145.
[32] *R v MacKenzie*, 2013 SCC 50 at para 86.
[33] *R v Bykovets*, 2024 SCC 6.
[34] *Ibid* at para 13.
[35] *Ibid* at para 41. Justice Karakatsanis, writing for the majority, explains that "[e]ven if the IP address does not itself reveal the user's identity, the prospect and ease of a *Spencer* warrant means that the user's identity can later be revealed, not only in relation to the potentially criminal Internet activity in question, but in relation to all the information that can be inferred from the user's Internet activity". *Ibid* at para 80.
[36] *Ibid* at para 90.
[37] *Benedik v Slovenia*, No. 62357/14 (24 April 2018); *Breyer v Germany*, No. 50001/12 (30 January 2020) at paras 102-3, 107; *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson et al*., Joined Cases C-203/15 and C-698/15, [2016], ECLI:EU:C:2016:979 at para 120; *Digital Rights Ireland v Minister for Communications et al.*, C-293/12 and C-594/12 [2014], ECLI:EU:C:2014:238 at para 62.

31. The privacy interferences associated with the de-anonymization of online subscribers are similarly applicable to measures taken by law enforcement measures to de-anonymize domain name registrants.[38] Article 6 of the Protocol would permit police agencies around the world to notice online content that interests or bothers them, and to request that a domain name registrar provide the police with the host's identity.

32. The responsibility of determining whether to disclose sensitive private information to a foreign law enforcement agency should not be delegated to private companies, such as through the "voluntary cooperation" arrangements contemplated under Article 6.[39] The Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar states that the authorities that make decisions with respect to whether to share information must have "a sophisticated understanding of the risks involved in doing so."[40] Moreover, Canadian courts have repeatedly rejected the notion that private companies have the authority to give "consent" to searches and seizures of private data on behalf of other individuals.[41]

B. Article 8: Other expedited procedures for obtaining traffic and subscriber data; more optional human rights

33. Article 8 introduces new obligations governing the disclosure of stored computer data (including traffic data and subscriber data) to foreign authorities, which could be used

[38] See Monika Zalnieriute and Thomas Schneider, "ICANN's procedures and policies in the light of human rights, fundamental freedoms and democratic values", Council of Europe, DGI(2014)12, October 8, 2014, at paras 91-116, 127-128; Yael Grauer, "Website Owners Deserve the Right to Stay Anonymous", *Slate*, June 26, 2015, <https://slate.com/technology/2015/06/icann-proposal-would-eliminate-whois-anonymity-for-commercial-website-owners.html>; European Data Protection Board, Letter to Internet Corporation for Assigned Names and Numbers, July 5, 2018, <https://www.edpb.europa.eu/sites/default/files/files/file1/icann_letter_en.pdf>. Domain name registrars typically collect the following information from domain name holders: the domain name, server name, registrar identity, date of creation, expiration date, name, and postal address of the registrant, name, postal address, email address, telephone number of the technical and administrative contact for the domain name. Disclosure of this information is subject to risks of privacy intrusions caused by tracking and analyzing patterns in online behavior, de-anonymization, undermining the freedom of expression associated with online speech and activities, and other risks of exposure of individuals to risks of spam and harassment. As in *R v Bykovets*, 2024 SCC 6, where the Canadian Supreme Court said ruled that there is an expectation of privacy in IP addresses, DNS information also acts as a "key" to unlocking a user's Internet activity (at para 13).

[39] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, Human Rights Committee, 2013, UN Doc A/HRC/23/40, at paras 72-77.

[40] *Report of the Events Relating to Maher Arar* at page 74.

[41] *R v Cole*, 2012 SCC 53; *R v Reeves*, 2018 SCC 56; *R v Spencer*, 2014 SCC 43. See also, *Tele2 Sverige AB v Post- och telestyrelsen and Secretary of State for the Home Department v Tom Watson et al*., Joined Cases C-203/15 and C-698/15, [2016], ECLI:EU:C:2016:979.

as an alternative to both Article 7 and MLATs. It imposes obligations on States to pass laws that enable:

a. a requesting Party to have the ability to issue an order to be submitted as part of a request to another Party; and,

b. for the requested Party to have the ability to give effect to that order by compelling a service provider in its territory to produce subscriber information or traffic data in the service provider's possession or control.

34. Article 8 would also attempt to expedite cross-border data sharing procedures by reducing the amount of information that is provided to the requested State regarding the underlying circumstances justifying the demand.

35. In contrast to Articles 6 and 7, Article 8 does afford State signatories greater opportunity to add requirements for independent judicial review of requests prior to disclosure to a requesting State. However, it is treated as entirely optional under Article 8. Under Article 8, police agencies in one country could foreseeably issue an order to seize stored computer data in another country, with an order that is reviewed and endorsed only by the police agencies of the requested State.

36. Furthermore, if the requesting State demands it, Article 8 prohibits the authorities in requested States from providing information about the supporting grounds purporting to justify the seizure to the service provider who is subject to the order. In doing so, Article 8 effectively nullifies the ability of service providers to meaningfully challenge unjustified orders.

37. Article 8 sets limits regarding the amount of supporting information that is required. It contains no requirements mandating that all material facts be fully, frankly, and fairly described–information that is essential for meaningful scrutiny and oversight. The explanatory reports even describes that any summary of facts should be "brief."[42] All additional information is treated as optional.

38. While human rights safeguards being treated as optional, Article 8(4) stipulates that States "shall" act expeditiously in the processing of orders.

[42] Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence - Explanatory Report* (2021) at para 133, online: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b>.

C. Article 9 is inconsistent with constitutional safeguards to protect personal information, including stored computer data, from excessive privacy intrusions

39. Article 9 of the Protocol mandates extraordinary powers to expedite the seizure and disclosure of stored computer data in emergency circumstances to a foreign country where there is imminent risk to life or safety. It contemplates the disclosure of stored computer data without any prior judicial authorization, even if expedited judicial oversight is available.

40. In *R v Tse*, the Supreme Court of Canada struck down a power that authorized law enforcement to intercept certain private communications without prior judicial authorization, if the officer believed on reasonable grounds that the interception was immediately necessary to prevent an unlawful act that would cause serious harm, *provided judicial authorization could not be obtained with reasonable diligence*.[43] The Supreme Court held that although stringently defined emergency powers can be reasonably justifiable, they still must be accompanied by additional safeguards to help ensure that the power is not being abused.[44] After-the-fact notice provides a measure to ensure that the individual's whose private information has been seized can challenge the seizure, and provides a balancing measures to better ensure that the extraordinary power is not being abused. The Supreme Court stated that notice is not the only type of safeguard that can serve this function.[45] The absence of such a notice requirements, or alternative safeguard, was constitutionally fatal to the law.

41. In the Protocol, Article 9 fails to ensure that emergency powers to obtain stored computer data is subject to adequate safeguards to ensure any intrusions are reasonably justified. Safeguards are necessary, given Article 9 potentially applies to extremely private information, such as the content of private communications or medical or health information. Notice to the individual is not required, and no alternative safeguards are obligatory (such as *ex post facto* judicial review of the disclosure, or judicial supervision of requests for confidentiality), in circumstances where notice is not given.[46]

---

[43] *R v Tse*, 2012 SCC 16.
[44] *Ibid* at para 84.
[45] *Ibid* at para 86.
[46] As will be further detailed below, Article 14.11 permits *either* "publication of general notices" or notice to the individual whose information, and further stipulates that the requested State "shall not" give personal notice if

D. The Protocol is Inconsistent with international human rights standards requiring independent judicial oversight and review of the sufficiency of grounds

42. As noted above, the Protocol fails to require independent judicial oversight over the seizure and disclosure of private data, including domain registration identities, subscriber information, traffic data, or other stored computer data. The "competent authorities" that could issue requests or orders compelling the production of private information, or who could review and authorize incoming requests or orders, include law enforcement or prosecution authorities. Neither LEAs, nor prosecution agencies, are independent within the meaning of the *Charter* or international human rights standards.[47]

43. By way of example, Serbia has ratified both the Budapest Convention and the Protocol. Notably, Serbia elected not to reserve in respect of Article 7, and for the purposes of Articles 6, 7, and 8, Serbia has declared that its "competent authority" will be the Department for the High-Tech Crime in Serbia's public prosecution office. This is of particular note given Serbia's recent extradition of a political dissident to Bahrain where he continues to face indefinite detention and risks of inhumane treatment.[48] As noted above, this took place despite an injunction that had been issued against the extradition by the European Court of Human Rights.

44. A central problem with the Protocol's deferential stance is that the Protocol directly condones or permits violations of international human rights standards.[49] The Explanatory Report to the Protocol asserts that due to "the many different legal systems and cultures", it is "not possible" to identify in detail the "applicable

---

the requesting State has requested confidentiality. The circumstances that justify a request for confidentiality appear to be unlimited, and potentially indefinite: Article 14.11-12.

[47] *Hunter v Southam*, [1984] 2 SCR 145; *Szabó and Vissy v Hungary*, No. 37138/14 (12 January 2016) at para 77; *Digital Rights Ireland v Minister for Communications et al.*, C-293/12 and C-594/12 [2014], ECLI:EU:C:2014:238 at paras 43-48.

[48] Human Rights Watch, *'We Will Find You': A Global Look at How Governments Repress Nationals Abroad* (22 February 2024), online: <https://www.hrw.org/report/2024/02/22/we-will-find-you/global-look-how-governments-repress-nationals-abroad>.

[49] See generally, Eliza Watt, *State Sponsored Cyber Surveillance* (Boston, MA: Edward Elgar Publishing, 2001) at pages 232-270.

conditions and safeguards for each power or procedure."[50] However, the Protocol's failure to set minimum standards that must be satisfied to justify privacy invasions is not merely a matter of procedural detail. The procedures governing search, seizure, and disclosure of private information by the police are a core element of international human rights standards that must inherently be interwoven into the search and seizure regime at issue in the Protocol.

45. Numerous sources of international human rights law detail human rights obligations governing search and seizure laws that authorize electronic surveillance. To begin, key resolutions by the United Nations General Assembly in 2013 and 2014 referred to the importance of independent and effective oversight surrounding the collection of personal data:

> …the Resolutions call upon all states 'to respect and promote the right to privacy, including in the context of digital communications'; and to take measures to prevent its violation by ensuring that the relevant national legislation complies with their obligations under international human rights law. To this end, they urge states to establish or maintain independent and effective oversight to ensure transparency of, and accountability for, surveillance and/or interception of communications and collection of personal data.[51]

46. The UN Office of the High Commissioner for Human Rights (OHCHR) has also called for the involvement of all branches of government in the oversight of surveillance programs to supplement judicial oversight as well as for the establishment of independent civilian oversight agencies.[52] In 2018, the OHCHR reiterated the "need for

[50] Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence - Explanatory Report* (2021) at para 185, online: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b>.

[51] Watt, *State Sponsored Cyber Surveillance* at pages 129-130. In 2016, the United Nations General Assembly again reiterated that States must "establish or maintain existing independent, effective, adequately resourced and impartial judicial, administrative and/or parliamentary domestic oversight mechanisms capable of ensuring transparency, as appropriate, and accountability for State surveillance of communications, their interception and the collection of personal data: *The Right to Privacy in the Digital Age*, United Nations General Assembly, 71st Session, UN Doc A/RES/71/199 (2016) GA Res 71/199 at para 5(d).

[52] *The Right to Privacy in the Digital Age: Report of the Office of the United Nations High Commissioner for Human Rights*, Human Rights Committee, 2021, UN Doc A/HRC/27/37 at para 37.

the authorization, review and supervision of surveillance measures by independent bodies at all stages, including when they are first ordered, expressing a preference for the judicial authority carrying out these functions."[53] The OHCHR emphasizes that authorization and oversight functions should be institutionally separate.[54]

47. The UN Human Rights Council Resolution 28/16 noted that "when aggregated, [metadata] can reveal personal information and can give an insight into an individual's behaviour, social relationships, private preferences and identity."[55] The Resolution expressed deep concerns regarding the impact of changing technology on the surveillance capabilities of state actors, and the adverse impact that surveillance, including extraterritorial surveillance, and the collection of personal data, will have on human rights, particularly when carried out on a mass scale.[56]

48. In his report, the Special Rapporteur Frank La Rue, likewise noted that the collection and analysis of communications data and metadata (which may include identity information, information about an individual's location and online activities, and logs and related information about the e-mails and messages they send or receive), "can be both highly revelatory and invasive, particularly when data is combined and aggregated."[57] The report called upon States to review and modernize national laws to take into account shifting technological landscape, with the corresponding expansion of surveillance capabilities that must be independently supervised.

49. The United Nations Human Rights Committee–the treaty body responsible for overseeing the implementation of the *International Covenant on Civil and Political Rights*–has also consistently reiterated the need for independent monitoring of state surveillance, "and has repeatedly insisted that states should guarantee that the processing and gathering of information be subject to review and supervision by an

[53] *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, Human Rights Committee, 2018, UN Doc A/HRC/39/29 at para 39.
[54] *Ibid* at para 40.
[55] *The Right to Privacy in the Digital Age*, Human Rights Committee, 28th Session, UN Doc A/HRC/RES/28/16 (2015) HRC Res 28/16.
[56] *Ibid*.
[57] *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, *Frank La Rue*, Human Rights Committee, 2013, UN Doc A/HRC/23/40.

independent body, with a strong preference for judicial authorization of such measures."[58]

50. The Inter-American Court of Human Rights has also ruled that the right to privacy under Article 8 of the *American Convention on Human Rights*, includes a requirement that impartial and independent judicial authorities review and approve all surveillance requests.[59] According to the *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression*, the surveillance of communications and personal data "shall be monitored by an independent oversight body and governed by sufficient due process guarantees and judicial oversight, within the limitations permissible in a democratic society."[60]

51. Throughout jurisprudence spanning decades, the European Court of Human Rights (ECtHR) has likewise issued numerous decisions reiterating the importance of independent oversight and review of the lawful basis for surveillance, as a key factor in

[58] See, for example, *Concluding Observations on the Fourth Periodic Report of the United States of America*, Human Rights Committee, 2014, UN Doc CCPR/C/USA/CO/4; *Concluding Observations on the Seventh Periodic Report of the United Kingdom of Great Britain and Northern Ireland*, Human Rights Committee, 2015, UN Doc CCPR/C/GBR/CO/7; *Concluding Observations on the Fifth Periodic Report of France*, Human Rights Committee, 2015, UN Doc CCPR/C/FRA/CO/5; *Concluding Observations on the Sixth Periodic Report of Italy*, Human Rights Committee, 2015, UN Doc CCPR/C/IT/CO/6; *Concluding Observations on the Fourth Periodic Report of the Republic of Korea*, Human Rights Committee, 2015, UN Doc CCPR/C/KOR/CO/4 at para 42; *Concluding Observations on the Seventh Periodic Report of Sweden*, Human Rights Committee, 2016, UN Doc CCPR/C/SWE/CO/7 at paras 36–37; *Concluding Observations on the Sixth Periodic Report of Canada*, Human Rights Committee, 2015, UN Doc CCPR/C/CAN/CO/6 at para 10; *Concluding Observations on the Fourth Periodic Report of Rwanda*, Human Rights Committee, 2016, UN Doc CCPR/C/RWA/CO/4; *Concluding Observations on the Initial Report of South Africa*, Human Rights Committee, 2016, UN Doc CCPR/C/ZAF/CO/1; *Concluding Observations on the Second Periodic Report on Turkmenistan*, Human Rights Committee, 2017, UN Doc CCPR/C/TKM/CO/2; *Concluding Observations on the Second Periodic Report of Honduras*, Human Rights Committee, 2017, UN Doc CCPR/C/HND/CO/2 at para 39. The Human Rights Committee also requires that contracting states provide the HRC with information pertaining to the authorities entitled to exercise control over the interference with privacy rights with strict regard for the law: General Comment No 16.

[59] "The Word 'Law' in Article 30 of the *American Convention on Human Rights*," Organization of American States, Inter-American Court of Human Rights, *Advisory Opinion OC-6/86* (1986) at para 38.

[60] UN Special Rapporteur on the Protection and Promotion of the Right to Freedom of Opinion and Expression and the Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights, *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression* (2013) at para 9, online: <<http://www.oas.org/en/iachr/expression/showarticle.asp?artID=927&lID=1>>.

determining whether there are adequate and effective guarantees against abuse.[61] In *Szabó and Vissy v. Hungary*, the ECtHR stated the following about independent prior authorization:

> [T]he rule of law implies, *inter alia*, that an interference by the executive authorities with an individual's rights should be subject to an effective control which should normally be assured by the judiciary . . . judicial control offering the best guarantees of independence, impartiality and a proper procedure. In a field where abuse is potentially so easy in individual cases and could have such harmful consequences for democratic society as a whole, it is in principle desirable to entrust supervisory control to a judge. . . . Accordingly, in this field, control by an independent body, normally a judge with special expertise, should be the rule and substitute solutions the exception, warranting close scrutiny. . . . For the Court, supervision by a politically responsible member of the executive, such as the Minister of Justice, does not provide the necessary guarantees.[62]

52. In *Benedik v Slovenia*, the ECtHR applied these principles in a case involving law enforcement access to subscriber data associated with an IP address. During the investigation at issue, Swiss law enforcement had obtained the subscriber information associated with a dynamic IP address from an internet service provider in Slovenia.[63] No prior judicial authorization had been obtained by the Swiss authorities before obtaining access to the subscriber information. The Court concluded that the circumstances had resulted in a violation of the right to privacy under Article 8 of the *European Convention on Human Rights*. In concluding that there were no safeguards to guard against abuse by State officials, the Court noted that there had been "***no independent supervision of the use of these police powers…, despite the fact that those powers, as interpreted by the domestic courts, compelled the ISP to retrieve the stored connection data and enabled the police to associate a great deal of information concerning online activity with a particular individual without his or her consent***."[64] It is notable that, in its analysis, the ECtHR noted that the *Budapest*

[61] *Case of Klass and Others v Germany*, No. 5029/71 (6 September 1978); *Roman Zakharov v Russia*, No. 47143/06 (4 December 2015) at paras 257 -258; *Szabó and Vissy v Hungary*, No. 37138/14, (12 January 2016) at para 77; *Big Brother Watch and Others v the United Kingdom*, Nos. 58170/13, 62322/14 and 24969/15 [GC] (25 May 2021) at paras 336, 350-352, 356, 377, 425; *Ekimdzhiev and Others v Bulgaria*, No. 70078/12 (11 January 2022) at paras 306-323, 334-347, 356.
[62] *Szabó and Vissy v Hungary*, No. 37138/14 (12 January 2016) at para 77.
[63] *Benedik v Slovenia*, No. 62357/14 (24 April 2018).
[64] *Ibid* at para 130.

Convention itself stipulates that investigative measures under the Convention must "as appropriate in view of the nature of the procedure or power concerned, *inter alia*, ***include judicial or other independent supervision, grounds justifying application, and limitation of the scope and the duration of such power or procedure***."[65]

53. The above body of international human rights law was well-summarized under the *International Principles on the Application of Human Rights to Communications Surveillance*,[66] which state that independent oversight and review is mandatory and not optional. The Principles state:

> Determinations related to Communications Surveillance must be made by a competent judicial authority that is impartial and independent. The authority must be:
>
> 1. separate and independent from the authorities conducting Communications Surveillance;
> 2. conversant in issues related to and competent to make judicial decisions about the legality of Communications Surveillance, the technologies used and human rights; and

[65] *Ibid* at para 126.

[66] Electronic Frontier Foundation, "Necessary & Proportionate: International Principles On the Application of Human Rights to Communications Surveillance" (May 2014), Principle 6, online (pdf): <https://necessaryandproportionate.org/files/en_principles_2014.pdf> [*Necessary & Proportionate Principles*]. The *Necessary & Proportionate Principles* have been widely cited, and in 2015, the Report of the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression mentioned that the *Necessary & Proportionate Principles* are "compelling demonstrations of the law that should apply in the context of the digital age": Human Rights Council, *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*, Human Rights Committee, 2015, UN Doc A/HRC/29/32 at para 15. See also, Electronic Frontier Foundation, "Background and Supporting International Legal Analysis for the International Principles On the Application of Human Rights to Communications Surveillance" (May 2014), online (pdf): <https://necessaryandproportionate.org/global-legal-analysis/#fnref:74>; European Union Agency for Fundamental Rights, "Surveillance by intelligence services: fundamental rights safeguards and remedies in the EU" (February 2023), online (pdf): <https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/PEGA/DV/2023/02-28/FRASubmissiontothePEGACommittee_EN.pdf>; Privacy International, "DOJ Cross-Border Legislation: Meeting Human Rights Requirements from Both Sides of the Pond" (May 2017) <https://privacyinternational.org/long-read/2001/doj-cross-border-legislation-meeting-human-rights-requirements-both-sides-pond#:~:text=It%20is%20essential%20that%20access,or%20body%20should%20be%20made>.

3. have adequate resources in exercising the functions assigned to them.[67]

54. The Protocol also seeks to reduce the amount of information that a requesting agency must provide to a requesting State and/or service provider on the grounds that it would streamline the processing of requests for or orders compelling the production of private data.[68] However, under international human rights standards, prior review by the independent judicial authority is required to establish that there are sufficient factual and legal grounds to justify the invasion of privacy—a key safeguard against arbitrary and unreasonable interferences.[69] It cannot be an exercise of proforma rubber stamping.[70] The Protocol's direct requirement or encouragement of providing less information to requested States and service providers (including in some cases even prohibiting information from being shared with service providers), directly undermines this review function.

55. Although Article 13 cites the need for adequate protection for human rights and civil liberties, this generic provision is undermined by the fact that the Protocol itself threatens to redefine international practices surrounding cross-border investigations to the detriment of human rights standards. The Protocol constructs a data-sharing regime that permits or requires access and sharing laws that fall well short of the standards reviewed in this section. In doing so, the Protocol threatens to adversely impact the coherent development of customary international law, and widespread ratification of the Protocol itself may threaten pre-existing human rights treaties if States subsequently argue that those earlier treaties apply "only to the extent that [their] provisions are compatible with" the Protocol.[71] Furthermore, as noted in the

[67] *Necessary & Proportionate Principles,* Principle 6.
[68] See Protocol, Article 6(3), Article 7(4), or Article 8(3) and (4).
[69] See, for example, *Case of Klass and Others v Germany*, No. 5029/71 (6 September 1978) at paras 55-56; *Roman Zakharov v Russia*, No. 47143/06 (4 December 2015) at paras 262-263; UN Special Rapporteur & the Special Rapporteur of the Inter-American Commission on Human Rights, *Joint Declaration on Surveillance Programs and Their Impact on Freedom of Expression* at paras 8 and 9; *The Right to Privacy in the Digital Age: Report of the United Nations High Commissioner for Human Rights*, Human Rights Committee, 2018, UN Doc A/HRC/39/29 at para 39; Watt, *State Sponsored Cyber Surveillance* at pages 242-247. See also, *Necessary & Proportionate Principles*, Principle 5.
[70] *Roman Zakharov v Russia*, No. 47143/06 (4 December 2015) at paras 262-263.
[71] *Vienna Convention on the Law of Treaties*, 23 May 1969, 1155 United Nations Treaty Series 331 (entered into force on 27 January 1980) at Article 30. Article 30(3) and (4) sets out circumstances where, in the case of successive treaties covering the same subject matter, the "earlier treaty applies only to the extent that its

next section, the Protocol also does not require State signatories to commit to the data protection requirements in Convention 108+. Given the ongoing pace of technological change and development,[72] it is particularly critical that human rights standards be directly interwoven into law enforcement powers and procedures, to generate an effective and resilient data-sharing protocol that is capable of providing a long-term path forward.

E. Article 14 fails to fully protect personal information

56. Article 14 of the Protocol sets out additional protections for personal information exchanged in cross-border investigations. However, Article 14 does not go far enough to provide adequate protection for personal information in accordance with international human rights standards. Article 14 creates optional rules and/or bypass mechanisms that benefit parties that lack strong data protection mechanisms, to the detriment of international progress regarding the protection of personal information. The "net impact of this one-sided approach is an untenable erosion of human rights."[73]

57. For example, Article 14 allows State signatories to supplant Article 14's own requirements by a secret "agreement", to set substandard protections for biometric data, to opt-out of notification requirements for security incidents with no explanation, and to opt-out of record-keeping requirements concerning the storage of personal data. States are also limited in their ability to require additional protections from foreign States as a precondition to the transfer of data. For example, signatories cannot require specific conditions for the processing of sensitive information that must be produced under the Protocol. Writing during the negotiations of the Protocol, human rights experts also note Article 14 does not ensure a level of data protection

provisions are compatible with those of the later treaty." The danger that the Protocol will directly undermine human rights treaties such as the ICCPR is amplified by the fact that Article 13 only indirectly references the human rights obligations and instruments identified in Article 15 of the *Budapest Convention*, leaving the Protocol more vulnerable to competing, rights-undermining interpretations. Furthermore, the Protocol fails to expressly conform with Article 30 of the Vienna Convention on the Law of Treaties by stipulating that the Protocol "is subject to, or that it is not to be considered as incompatible with" earlier or later human rights treaties, to ensure that those human rights obligations will indisputably prevail.

[72] For example, the UN Human Rights Committees' General Comment Number 16, concerning the right to privacy, was written in 1988 and has become outdated, due to the "vast technological leaps that have taken place since its adoption": UN General Assembly Resolution, *The Right to Privacy in Digital Age*, United Nations General Assembly, 68th Session, UN Doc A/RES/69/166 (2015) GA Res 69/166.

[73] Derechos Digitales et al, "Privacy & Human Rights in CrossBorder Law Enforcement" at page vi.

which is consistent with modern data protection instruments such as Convention 108/108+:

> This is highly problematic as the draft Protocol includes provisions for international transfers of personal data on a systematic scale, including between private service providers and law enforcement authorities in Parties that have not ratified Convention 108/108+.[74]

58. Creation of a parallel data protection system in Canada: Article 14 would result in the creation of a parallel data protection system inside Canada for international law enforcement. It is not obvious why Canada should tolerate the imposition of an exceptional approach to the protection of personal privacy, particularly given the wide scope of the Protocol in today's increasingly digital world. The Protocol and the Budapest Convention apply to specific criminal offenses committed in computer systems, but also *any criminal offense for which there may be evidence in electronic form*. The Protocol mandates the collection of data from service providers in relation to a broad array of public and private entities, including instant messaging, social media, health care providers, online shopping platforms, DNA ancestry testing, and personal information connected to generative AI tools. Authoritarian states or even overzealous law enforcement agencies need only request the data under the auspice that the data is relevant to a criminal investigation of nearly any kind, and are able to access this parallel system.

59. The Protocol allows for the creation of ad hoc agreements that bypass even the data protection standards set out in Article 14: Article 14, paragraph 1 (b) and (c) allow signatories to come to "other agreements or arrangements" to replace Article 14's safeguards. As noted by human rights experts, "[a] secret informal arrangement with no meaningful safeguards at all could seemingly qualify."[75] Moreover, even if the requesting and requested State do not have an existing agreement in place, they can establish one at any time.

60. Article 14 prohibits States from requesting additional general data protection conditions, or from blocking data transfers due to the risk of human rights abuses: Article 14.2.a and 14.15 read together prohibit a transfering party from requesting

[74] *Ibid* at page 24.
[75] *Ibid* at page 24.

additional "generic" data protection conditions before data sharing. Prohibiting more meaningful data protection conditions is problematic for privacy rights generally, but also for requested States that have more robust data privacy laws than those of the requesting State. Those States may otherwise be prohibited from transferring data out of their territory unless sufficient safeguards are guaranteed in the requesting State. Furthermore, even in the face of concerns about the risk of potential human rights abuses in a requesting State, the Protocol prohibits the suspension of a transfer based on human rights risks, and instead demands an intolerably high threshold of "***substantial evidence*** of a breach or that a breach is imminent" before a requested State can prevent the transfer. The Explanatory Report expressly states that "grounds for refusal established by a requested Party should be narrow and exercised with restraint."[76]

61. For example, the European Digital Rights (EDRi) network has raised that the Protocol does not take into consideration the ongoing review that already takes place by European data protection authorities regarding data transfer.[77] According to the Article 58.2.j of the GDPR, the member states' data protection authorities have the power to suspend transfers. However, Article 14.15 of the Protocol only allows a requested State to suspend a transfer if there is a "systematic or material" breach and requires a consultation between parties. Further risks will arise if those consultations take place at a government level that does not involve data protection authorities.

62. A further implication of these barriers (as illustrated in the European Data Protection Board's interpretive Opinion 1/2022[78]) is that Canada would be prohibited from requiring that a requesting State have an independent data protection authority as a

[76] Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence - Explanatory Report* (2021) at para 142, online: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b>.

[77] European Digital Rights, *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention* (2022) at page 7, online (pdf): <https://edri.org/wp-content/uploads/2022/04/EDRi-Position-Ratification-EU-Member-States-Cybercrime-Second-Additional-Protocol.pdf>.

[78] European Data Protection Supervisor, *Opinion 1/2022 on the two proposals for Council Decisions authorising Member States to sign and ratify , in the interest of the European Union, the Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence* (20 January 2022), online (pdf): <https://www.edps.europa.eu/system/files/2022-04/22_01_20_opinion_en.pdf>.

safeguard for privacy rights. Data protection authorities[79] are independent and are able to apply specialized expertise on data protection matters.

63. Alternatively, Canada also could not require, as a precondition to sharing information under the Protocol, that the requesting State have established data protection rights. Such rights could include the right to erasure, for example, following the conclusion of criminal investigation, the right to restrict further processing until the personal information is rectified, or a right to an explanation in the event that an automated decision was made using their personal information (as contemplated under paragraph 6.2.3 of Canada's Directive on Automated Decision Making[80]).

64. No guarantee that biometric data will be protected outside Canada: Article 14.4 of the Protocol defines Sensitive Data as including "biometric data considered sensitive in view of the risks involved." Under this definition, not all biometric data must be safeguarded with the additional protections applicable to sensitive data.[81] For example, the Explanatory Report to the Protocol asserts that for some jurisdictions, "certain photographs or video-footage, even if they reveal physical or anatomical features such as scars, skin marks and tattoos, would not generally be considered to fall into the category of sensitive biometric data."[82] As a result, Article 14.4 leaves it open to States to determine the level of protection that should be afforded to biometric data.

[79] Data protection authorities do not appear to fit the definition of oversight authorities set out in Article 14.14.
[80] Government of Canada, "Directive on Automated Decision-Making" (2019), online: <https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592>.
[81] Katitza Rodriguez, "EFF to Council of Europe: Cross Border Police Surveillance Treaty Must Have Ironclad Safeguards to Protect Individual Rights and Users' Data", *Electronic Frontier Foundation* (8 September 2021), online: <https://www.eff.org/deeplinks/2021/09/eff-council-europe-cross-border-police-surveillance-treaty-must-have-ironclad>; Article 19, *ARTICLE 19's briefing The Council of Europe Convention on Cybercrime and the First and Second Additional Protocol* (2019), online (pdf): https://www.article19.org/wp-content/uploads/2022/06/Budapest-Convention-analysis-May-2022.pdf.
[82] Cybercrime Convention Committee (T-CY), *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence - Explanatory Report* (2021) at para 237, online: <https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b>.

65. In doing so, the Protocol is inconsistent with modern data protection principles,[83] which stipulate that biometric data is inherently sensitive data given the inextricable link between biometric data and the person's identity and existence. In Canada, the Office of the Privacy Commissioner of Canada has stated that facial biometric information is, in fact, sensitive data – a conclusion that was confirmed in the joint investigation of Clearview AI conducted by the privacy commissioners of Canada, Quebec, British Columbia, and Alberta.[84] Moreover, Article 6 of Convention 108+ provides that biometric data uniquely identifying a person constitutes a special category of data, and the processing of biometric data shall only be allowed where specified safeguards are enshrined in law. Additionally, the Directive of Law Enforcement of the European Union, the General Data Protection Regulation and California Privacy Rights Act also consider biometric data as a special/sensitive category of personal data.[85]

66. Despite all this, by virtue of Article 14.2 of the Protocol, Canada would still be prohibited from requiring commitment to requisite data protection standards for biometric data, as a precondition to transfers under the Protocol. This means that

[83] For example, on July 4, 2023, the European Court of Human Rights ruled in *Glukhin v. Russia* that the use of facial recognition technology from photographs against a peaceful solo protestor is intrusive and violates the right to privacy enshrined in the European Convention on Human Rights. The Court noted the absence of strong safeguards against the abuse and arbitrariness in the use of facial recognition technology, meaning that the use of facial biometric data requires special safeguards: *Glukhon v. Russia*, No. 11519/20 (4 October 2023) at para 83.

[84] Office of the Privacy Commissioner of Canada, "Interpretation Bulletin: Sensitive Information" (May 2022), online: <https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/pipeda-interpretation-bulletins/interpretations_10_sensible/>; *Joint Investigation of Clearview AI by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the information and Privacy Commissioner for British Columbia and the Information Privacy Commissioner of Alberta* (2 February 2021), PIPEDA Findings #2021-001, online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[85] EU, *Directive 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA*, [2016] OJ, L 119/89; EU, *Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, [2016] OJ, L 119/1*; California Consumer Privacy Act of 2018*, California Civil Code §1798.192 (2022).

once the biometric data leaves Canada's borders, there would be no guarantee as to how it would be treated as it will depend solely on the receiving party.

67. The Protocol includes a discretionary, unaccountable option to opt-out of notification requirements in the event of a security incident, with no repercussions: Canada's legal system has long imposed mandatory notification requirements for security breaches and incidents. Both in the public and private sectors, there is a mandatory obligation to notify. For the former, federal institutions must notify the Office of the Privacy Commissioner of Canada and the Treasury Board of Canada Secretariat when sensitive information is involved.[86] For private sector organizations, the notice obligations arise when it is believed that the security breach creates a real risk of significant harm.[87] The type of sensitive information at issue in a law enforcement investigation is highly likely to risk significant harm in the event of a data breach.

68. Contrary to requirements in Canada, Article 14.7.b states that a notice may be "omitted when such notification may endanger national security." This clause creates at least three problems. First, national security is a malleable, discretionary concept that is influenced by the legal and political circumstances of each country. A requesting State that has received data might deem even minor problems or political repercussions to be a source of "national security" risk. Second, opting-out of the notification requirement jeopardizes the right to due process of the person whose personal information has been compromised. Third, secrecy surrounding security breaches results in lack of accountability, and prevents requested States from taking the originating security vulnerabilities into account when considering whether to

[86] Office of the Privacy Commissioner of Canada, "Report a privacy breach at your federal institution" (last modified 2 May 2023), online: <https://www.priv.gc.ca/en/report-a-concern/report-a-privacy-breach-at-your-organization/report-a-privacy-breach-at-your-federal-institution/>. For example, in 2017, the Government of Ontario had to notify at least 5,600 Ontarians who were victims of a data breach caused by a printing error. While in that case the information exposed was related to health card numbers, birth dates, and home addresses, the issues that the protocol applies to involve information that goes beyond that data: Vito Pilieci, "Ontario government scrambling after printing mistake causes data breach affecting thousands," *Ottawa Sun* (5 May 2017), online: <https://ottawasun.com/2017/05/05/ontario-government-scrambling-after-printing-mistake-causes-data-breach-affecting-thousands>.

[87] Office of the Privacy Commissioner of Canada, "What you need to know about mandatory reporting of breaches of security safeguards" (last modified 13 August 2021), online: <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.

respond to a further request in the future. A notification, on the other hand, forces the requesting State to be accountable and remedy all applicable security vulnerabilities.

69. No mandate to keep records about personal information storage: While each party shall retain the personal information only as long as it is necessary and appropriate, there is no obligation to keep records about this retention. Article 14.8 only mandates parties to have records that demonstrate how the personal information has been accessed, used, and disclosed, leaving out information about how long and where the information has been stored. The European Data Protection Board in their Opinion 1/2022 also highlights this omission.[88] It is crucial to maintain records regarding data retention to enable effective review and accountability.

F. Other Unresolved Problems in the Final Text of the Protocol

70. Prior to the adoption of the Protocol, numerous civil society organizations, including EDRi, the Samuelson-Glushko Canadian, Internet Policy & Public Interest Clinic (CIPPIC), and the Electronic Frontier Foundation, identified the need for broader consultation surrounding the drafting of the Protocol, and for amendments to address the overarching problem that the Protocol mandates expediency while making human rights safeguards optional or even in some circumstances prohibited. These recommendations were not resolved before the adoption of the Protocol in 2021. This means that, in addition to the issues addressed through Part 3, the drafters of the Protocol have failed to address other problems, including the following:

    a. **Article 12 - Secretive joint investigation agreements:** The Protocol allows parties to establish "joint investigation" agreements when enhanced coordination is deemed to be of particular utility. However, it does not place any explicit conditions limiting the scope of these agreements, nor does it require that the existence or circumstances surrounding those agreements be made public. As noted by civil society organizations, "Article 12 places no meaningful restrictions on data transfers between agencies and jurisdictions, the investigative team can jointly accumulate private data by the most intrusive means available,"[89] and all this can be done in absolute darkness, with no public scrutiny. The provision further endangers human rights by opening the

[88] European Data Protection Supervisor, *Opinion 1/2022*.
[89] Derechos Digitales et al, *Privacy & Human Rights in CrossBorder Law Enforcement* at page 12.

door to the construction of joint investigation teams based in a jurisdiction with the most permissive search and seizure laws, such that all surveillance activities throughout the investigation would be governed by the national laws that are the least protective of privacy rights. In Canada, this element of the Protocol has the potential in particular to significantly exacerbate risks and problems associated with legal uncertainty in Canada's human rights framework applicable to cross-border investigations (an issue that will be discussed further in Part 5).

b. The Protocol thus raises the threat of an expanded shadow network for data obtained from spyware or cyber espionage to proliferate through unchecked, such as through secret agreements reached under Article 14(1) or through Article 12's joint investigation agreements. The Protocol imposes no limits on the type of information that can be shared through data sharing agreements or arrangements under Articles 12 and 14(1), despite growing recognition of the need for international action to address privacy threats proliferating from new surveillance technologies and private sector actors.[90] While the parties are obligated to provide "adequate" protection of human rights and liberties, at present, State practice concerning the respect for international human rights standards is inconsistent.[91] In 2019, the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression stated:

> It is insufficient to say that a comprehensive system for control and use of targeted surveillance technologies is broken. It hardly exists. While human rights law provides definite restrictions on the use of surveillance tools, States conduct unlawful surveillance without fear of legal consequence. The human rights law framework is in place, but a framework to enforce limitations is not.[92]

[90] Surveillance and Human Rights: Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Human Rights Council, 2019, UN Doc A/HRC/41/35, discussing the development of targeted surveillance technologies and practices (such as computer interference, mobile device hacking, socially-engineered intrusions, network surveillance, facial and affect recognition, IMSI catchers (Stingray surveillance), and deep packet inspection), and the need for . As noted by the Special Rapporteur, in the surveillance space, "[p]rivate industry has stepped in, unsupervised and with something close to impunity" (at para 6).

[91] Watt, *State Sponsored Cyber Surveillance* at 93-141.

[92] *Ibid* at para 46.

Furthermore, "there remain significant gaps in the regulation of cross-border *cyber* espionage—as a method of espionage—under international law."[93] Notwithstanding these known risks and uneven State practices, the Protocol does nothing to prevent data obtained through targeted surveillance technologies, including data obtained unlawfully, from being shared through secret agreements and arrangements established under Articles 12 and 14(1).

c. **Overbroad and unaccountable discretion to impose gag orders without judicial oversight:** The Protocol includes investigative confidentiality provisions. For instance, in the joint investigations agreements, both parties are free to set the terms of confidentiality. However, as in the case of these joint agreements, the Protocol provides discretionary powers in dealing with confidential issues, which amplifies the dangers surrounding unsupervised "direct" access to subscriber and domain information. Excessive confidentiality shields State abuses, such as investigations targeting at-risk citizens such as journalists, whistleblowers, political dissidents, and more. Instead, investigative secrecy and confidentiality subject to judicial oversight, and should be delimited to circumstances where revealing information could compromise an ongoing investigation or risk the human rights of other people. [94]

d. **Dual criminality is not a requirement for the issuance of a request or order:** The potential for data sharing procedures in the Protocol "to chill or otherwise negatively affect free expression is exacerbated by the absence of a dual criminality requirement."[95] As noted in Part 2, cross-border data sharing in respect of any form of criminal offense, such as offenses criminalizing political speech, exposes individuals to risks of human rights abuse or digital transnational repression, including risks for journalists, human rights defenders, political dissidents, politicians, and lawyers.

[93] Siena Anstis, "Regulating Transnational Dissident Cyber Espionage" (2023) 73:1 International & Comparative Law Quarterly 259.

[94] Derechos Digitales et al, *Privacy & Human Rights in Cross-Border Law Enforcement* at pages 18-19.

[95] Electronic Frontier Foundation et al, *Joint Civil Society Response*; EDRi, *Ratification by EU Member States of the Second Additional Protocol of the Council of Europe Cybercrime Convention* at page 6.

e. **Fair trials, due process, and exculpatory records**: As noted by civil society organizations,[96] the Protocol provides no mechanisms for protecting fair trial rights by enabling the collection of exculpatory evidence by defendants and their counsel. On balance, this leads to procedural inequality that privileges furnishing only prosecution and law enforcement authorities with access to data.

Part 4. Eliminating or reducing human rights safeguard to expedite large volumes of cross-border data sharing is disproportionate, unnecessary, and non-compliant with international human rights

71. As noted in Part 3 of this submission, the primary method that the Protocol proposes to use to expedite cross-border data sharing is to eliminate or reduce human rights safeguards, including independent oversight over foreign requests or orders for private data. As noted above, Canada's consultation paper describes that there is backlog and delay associated with MLAT protocols, and that mutual legal assistance channels are "generally not well-equipped to handle high volumes of requests requiring expeditious production."[97]

72. However, the consultation paper does not specify the extent or source of the delay associated with MLATs, or what efforts Canada has made to remedy its role in the delay. Moreover, eliminating judicial oversight is a particularly severe response to ostensible delay, particularly if provisioning the MLAT system with adequate resources would reasonably alleviate delay. In Canada, recent jurisprudence pertaining to the *Charter* right to speedy trial describes the importance of ensuring the justice system is sufficiently resourced, noting that, "[o]ne obvious way to reduce the backlog of cases is to make sure that judicial vacancies are filled so that trials do not get adjourned."[98] The same can be said for furnishing MLAT procedures with the resources and processing deadlines that are necessary and sufficient to obtain the desired response time. In the US context:

> …civil society from around the world including EFF and EDRI have consistently recommended: offering technical training for law enforcement authorities; simplifying and standardizing data request forms; creating single points of

[96] Electronic Frontier Foundation et al, *Joint Civil Society Response.*
[97] Canada, *Consultation on the Second Additional Protocol* (December 2023).
[98] *R v Bowen-Wright*, 2024 ONSC 293 at para 52.

> contact for data requests; and most importantly, increasing resources, especially in the United States, where the bulk of the requests end up. We've seen this work first-hand: thanks to a recent U.S. MLAT reform program, which increased its resources to handle MLATs, the U.S. Department of Justice has already reduced the amount of pending cases by a third.[99]

73. It is notable that in the USA–the country which tends to receive the most MLAT requests worldwide–the US Department of Justice (DOJ) reduced its backlog by a third by hiring a total of only 37 lawyers and 35 paralegals between 2015 and 2019.[100] However, a recent audit by the Office of the Inspector General (OIG) cited the need to address continuing staffing shortages to reduce backlog.[101] The OIG stated staffing levels have been stagnant, and that the DOJ's Office of International Affairs "does not currently have a hiring and retention plan to address its staffing challenges."[102]

74. The privacy and human rights interests of individuals around the world should not be eroded as a result of the unwillingness of governments to adequately resource established mechanisms for safeguarding privacy rights. Even within Canada's borders, the constitutional **requirement** to reduce delay in the justice system does not trump the need to protect fundamental human rights, including the privacy rights that Canada's search and seizure laws are designed to safeguard.

75. Furthermore, weak human rights standards in some countries is itself a source of delay in MLAT procedures–a problem that would continue to plague the Protocol's regime given its failure to require standardized commitment to harmonized human rights standards. In its audit of the US DOJ, the OIG noted that attorneys had to allocate excessive amounts of time to process requests that had come from countries with

---

[99] Katitza Rodriguez, Danny O'Brien, and Maryant Fernandez, "Behind the Octopus: The Hidden Race to Dismantle Global Law Enforcement Privacy Protections", Electronic Frontier Foundation, , <Electronic Frontier Foundation,>, citing U.S. Department of Justice, "FY 2019 Budget Request", <https://www.eff.org/deeplinks/2018/08/behind-octopus-hidden-race-dismantle-global-law-enforcement-privacy-protections>.

[100] *Ibid*.

[101] Department of Justice, Office of the Inspector General, *Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests Audit Division*, 2021, at p ii, <https://oig.justice.gov/sites/default/files/reports/21-097.pdf>.

[102] *Ibid*.

weaker legal frameworks.[103] In that sense, the Protocol should be strengthening and standardizing human rights standards and training–not weakening them.

76. Finally, as noted by human rights experts, the Protocol risks aggravating delay by adding unnecessary complexity to existing cross-border data sharing protocols by creating overlapping, unharmonized, and potentially incompatible regimes.[104] The U.N. Security Council's Counter-Terrorism Committee Executive Directorate has stated that a fragmented cross-border investigative landscape "frustrates one of the key goals of the reform initiatives, which is to simplify an overly complex and fragmented set of jurisdictional concerns for accessing digital evidence."[105]

Part 5. Canada Must Prioritize and Address Existing Gaps in Human Rights Protections in Canada Applicable to Cross-border Police Investigations

77. The question of whether Canada should ratify the Protocol must also be considered within the broader context of Canada's existing laws, including the insufficiency of existing human rights safeguards governing cross-border investigations.

78. At present, even without ratification or implementation of the Protocol, individuals in Canada are already exposed to human rights risks due to existing gaps and uncertainty in constitutional and human rights safeguards surrounding cross-border law enforcement investigations. These gaps relate, in part, to ongoing uncertainty surrounding the extent to which the *Charter* is applicable to the extraterritorial actions of the government in cross-border investigations or actions.[106] Since 2007, the Supreme Court of Canada's decision in *R v Hape*,[107] has provided the analytical framework for determining the extent to which the *Charter* applies to extraterritorial

[103] Department of Justice, Office of the Inspector General, *Audit of the Criminal Division's Process for Incoming Mutual Legal Assistance Requests Audit Division*, 2021, at p 13, <https://oig.justice.gov/sites/default/files/reports/21-097.pdf>.
[104] Israel & Rodriguez, "On New Cross-Border Cybercrime Policing Protocol, a Call for Caution".
[105] *Ibid*, citing United Nations Security Council Counter-Terrorism Committee Executive Directorate, "The State of International Co-operation for Lawful Access to Digital Evidence: Research Perspectives" (January 2022) at page 24.
[106] Department of Justice Canada, "The Canadian Charter of Rights and Freedoms, Section 32(1)—Application of the Charter" (last modified 29 June 2023) <https://justice.gc.ca/eng/csj-sjc/rfc-dlc/ccrf-ccdl/check/art321.html>, stating that "[t]he extent of the application of the *Charter* to government acts that occur outside Canada is not entirely clear as the Supreme Court has not dealt with a number of important contexts in which the Canadian government acts outside the territory of Canada.
[107] *R v Hape*, 2007 SCC 26.

searches and seizures conducted by Canadian police officers in another country. The Court determined that, subject to certain exceptions, *Charter* standards cannot be applied to the actions of Canadian officials when conducting an investigation extraterritorially.

79. The majority of the Supreme Court of Canada in *R v McGregor* recently took note of the "extensive body of academic criticism in which the *Hape* framework is challenged on various constitutional and international law grounds."[108] The minority in *McGregor* similarly noted that "[n]umerous theoretical and practical problems have unfortunately followed *Hape*, as highlighted by the wealth of judicial and academic criticisms that have emerged in the last 15 years."[109] These criticisms focus on *Hape*'s unstable doctrinal foundations, which rest on a mistaken and overbroad understanding of what the principle of State sovereignty requires.[110] In a comparative analysis of how other countries apply domestic human rights instruments to the extraterritorial actions of state officials, Leah West notes that "Canada stands alone in its position that international law prohibits the extraterritorial application of the state's municipal human rights obligations."[111]

80. In effect, the law in Canada has resulted in "Canadian officials asking for other states' permission to apply Canada's constitutional limits to Canada's own conduct."[112] By overextending the scope of the principle of state sovereignty, the *Hape* framework has left gaps where *Charter* protections exceed the rights guaranteed in international

[108] *R v McGregor*, 2023 SCC 4 [*per* Côté J]. The majority of the Court ultimately determined that it was not an appropriate case to determine the issue.
[109] *Ibid* at para 78 [*per* Karakatsanis and Martin JJ].
[110] See, for example, Leah West, "Canada Stands Alone: A Comparative Analysis of the Extraterritorial Reach of State Human Rights Obligations" (2022) 55:3 *UBC Law Review* 845 at page 849; Amir Attaran, "Have *Charter* Will Travel? Extraterritoriality in Constitutional Law and Canadian Exceptionalism", Case Comment on *R v Hape*, (2009) 87:2 *Canadian Bar Review* 515; John H Currie, "Weaving a Tangled Web: Hape and the Obfuscation of Canadian Reception Law" (2007) 45 *Canadian Yearbook of International Law* 55; John H Currie, "*Khadr*'s Twist on Hape: Tortured Determinations of the Extraterritorial Reach of the Canadian *Charter*", Case Comment on *Canada (Justice) v Khadr*, (2008) 46 *Canadian Yearbook of International Law* 307; Robert J Currie & Joseph Rikhof, *International & Transnational Criminal Law*, 3rd ed (Toronto: Irwin Law, 2020) at pages 631–39; Scott Fairley, "International Law Comes of Age: *Hape v. The Queen*" (2008) 87:1 *Canadian Bar Review* 229; Kent Roach, "*R. v. Hape* Creates Charter-Free Zones for Canadian Officials Abroad" (2007) 53:1 *Criminal Law Quarterly* 1; Gibran Van Ert, "Canadian Cases in Public International Law in 2007–8" (2009) 46 *Canadian Yearbook of International Law* 633.
[111] West, "Canada Stands Alone" at page 853.
[112] *R v McGregor*, 2023 SCC 4 at para 74 [*per* Karakatsanis and Martin JJ].

human rights instruments.[113] The framework also creates "uncertainty for Canadian state actors acting abroad who are unlikely to be familiar with Canada's international human rights obligations."[114]

81. Even if one were to accept that the *Hape* framework rested on correct foundations, Canada would still appear to be facing a human rights gap of another kind. The majority in *Hape* wrote that even in circumstances where the *Charter* does not apply to the actions of government officials participating in an extraterritorial investigation, Canadian officials could still nevertheless be governed by international human rights obligations.[115] However, treaties, which are "the key source of Canada's international human rights obligations, do not take effect in Canadian law directly unless they have been implemented through legislation."[116] The *Charter* is the means by which Canada has implemented many of its international human rights obligations.[117] If the *Charter* does not apply to the actions of Canadians officials requesting or participating in cross-border investigations, the Canadian government is still obliged to fulfill its international human rights obligations with domestic legislation that implements human rights protections in those contexts as well.[118]

82. Of particular relevance to the Protocol, legislative reform is needed to enable judicial oversight of cross-border requests by Canadian law enforcement for the seizure of data by foreign authorities. Judicial oversight serves as a safeguard to ensure that privacy interferences are reasonably justified, and that law enforcement authorities do not circumvent Canada's search and seizures laws by outsourcing monitoring and

[113] *Ibid* at para 75 [*per* Karakatsanis and Martin JJ].
[114] *Ibid*.
[115] *R v Hape,* 2007 SCC 26 at para 101. This exception was applied by the Supreme Court in *Canada (Justice) v Khadr*, 2008 SCC 28 at para 18. However, the provision of a *Charter* remedy for a violation of international human rights law has also led to further unresolved tensions, given *Charter* remedies are typically extended as a result of *Charter* violations. See Amir Attaran, "Have *Charter* Will Travel? Extraterritoriality in Constitutional Law and Canadian Exceptionalism", Case Comment on *R v Hape*, (2009) 87:2 *Canadian Bar Review* 515 at page 520; and Robert J Currie, *International & Transnational Criminal Law*, 3rd ed (Toronto: Irwin Law, 2020) at page 623, writing that "[i]n the end, all we are left with is that the Charter does not apply extraterritorially, except when it does."
[116] *R v McGregor*, 2023 SCC 4 at para 75 [*per* Karakatsanis and Martin JJ].
[117] *Ibid*.
[118] See for example, Robert J Currie, "Charter Without Borders? The Supreme Court of Canada, Transnational Crime, and Constitutional Rights and Freedoms" (2004) 27:1 Dalhouse Law Journal 235 at page 280, discussing the need for clarification to ensure that Canada's domestic human rights standards applicable to mutual legal assistance proceedings also conform with Canada's international human rights obligations. See also John H Currie, "Weaving a Tangled Web: Hape and the Obfuscation of Canadian Reception Law" (2007) 45 *Canadian Yearbook of International Law* 55 at p 83-84.

surveillance activities to foreign authorities that are governed by privacy laws that fall short of *Charter* standards.

83. At present, Canada's search and seizures laws are generally structured around the increasingly untenable premise that the Canadian government is not responsible under the *Charter* for searches and seizures exercised by foreign authorities in response to a request by Canadian authorities.[119] In 1998, a four-judge majority of the Supreme Court ruled in *Schreiber v. Canada (Attorney General)*, that the *Charter* does not apply to the issuance of a letter of request to foreign authorities seeking their assistance with respect to a Canadian criminal investigation.[120] An alternative framing has appeared in the jurisprudence, which stipulates that "a reasonable expectation of privacy will generally correspond to the degree of protection" provided for under foreign law where private records are located.[121] This premise was reiterated in 2007 in *Hape* when the Court stated that "it is the individual's decision to go to or operate in another country that triggers the application of the foreign law."[122]

84. However, the notion that individuals are free to simply choose the level of privacy protection they desire for their online information has been eclipsed by more recent jurisprudence. In 2017, the Supreme Court recognized that in the modern digital landscape, the availability of meaningful choice surrounding protection of our personal information online is often illusory. The use of online apps, social media platforms, and forms of digital services is ubiquitous in Canada. In *Douez v. Facebook Inc.*,[123] the Supreme Court recognized that individuals will often lack meaningful choice about matters affecting their personal information shared online:

> …in today's digital marketplace, transactions between businesses and consumers are generally covered by non-negotiable standard form contracts presented to consumers on a "take-it-or-leave-it" basis.
>
> > In particular, unlike a standard retail transaction, there are few comparable alternatives to Facebook, a social networking platform with extensive reach. British Columbians who wish to participate in the many

[119] *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841 at para 31, per L'Heureux-Dube J for the majority.
[120] *Ibid*.
[121] *Ibid* at para 23, per Lamer CJ writing in dissent, but paragraph 23 was endorsed by the majority in *R v Hape* at para 99.
[122] *R v Hape*, 2007 SCC 26 at para 99.
[123] *Douez v Facebook Inc.*, 2017 SCC 33.

> online communities that interact through Facebook must accept that company's terms or choose not to participate in its ubiquitous social network. **As the intervener the Canadian Civil Liberties Association emphasizes, "access to Facebook and social media platforms, including the online communities they make possible, has become increasingly important for the exercise of free speech, freedom of association and for full participation in democracy" (I.F., at para. 16). Having the choice to remain "offline" may not be a real choice in the Internet era.**[124]

85. There are critical dangers with an analytical approach that tethers constitutionally-protected privacy interests to foreign laws without regard for international human rights standards, or *Charter* principles protecting privacy:

    a. First, using foreign law to define reasonable expectations of privacy fails to consider whether the foreign law at issue is consistent with international human rights standards, or whether those laws and/or human rights standards are meaningfully enforced in the jurisdiction. Taking the Supreme Court's framing in *Canada (Justice) v Khadr*, if Canada requests that a search or seizure take place in a jurisdiction where the legal framework falls short of international human rights obligations, it is unclear why this would not constitute "participation in processes that violate Canada's binding international human rights obligations."[125]

    b. Second, in some circumstances, a company's practices concerning the use of personal information might be purportedly compliant with the laws of a foreign jurisdiction, while simultaneously violating *Canada's* privacy laws in relation to the personal information of individuals located in Canada.[126]

    c. Third, the majority in *Schreiber* focused on how, even though the investigation had been initiated by Canadian authorities through a letter of request, all of the actions that had relied "on state compulsion in order to interfere with the respondent's privacy interests" had been taken by foreign authorities.[127] However, in subsequent jurisprudence, the Supreme Court has now repeatedly

[124] *Ibid* at paras 55-56.
[125] *Canada (Justice) v Khadr*, 2008 SCC 28 at para 2.
[126] See for example, *Joint Investigation of Clearview AI.*
[127] *Schreiber v Canada (Attorney General)*, [1998] 1 SCR 841 at para 31 [majority reasons].

recognized that other law enforcement *requests* (that rely on no compulsion powers) also have the potential to interfere with privacy interests that are protected under the *Charter*.[128]

d. Fourth, given reasonable expectations of privacy are defined contextually, it is incoherent for the framework under section 8 to exclude analysis of the expectations of privacy that an individual in Canada has in relation to *Canadian officials*–particularly in circumstances where *Canadian* law enforcement officials are investigating *a person in Canada*, and are triggering the seizure of records relating to *online activity of an individual located in Canada.* In other settings where the Supreme Court has rejected the authority of third parties to disclose information to Canadian law enforcement authorities, the inquiry is not whether the individual had an expectation of privacy *against the third party*; what matters is the individual's expectation of privacy vis-a-vis Canadian law enforcement authorities.[129]

e. Fifth, as noted in paragraph 83 above, the majority in *Schreiber* focused on how the actions which ultimately interfered with the privacy interests in that case were carried out by foreign authorities who are not subject to the *Charter*. However, in 2014, the majority of the Supreme Court ruled that Canadian authorities are constitutionally obliged to consider the foreseeable effects of Canadian state conduct on human rights violations committed in a foreign jurisdiction. In *Wakeling v United States of America*, the Supreme Court of Canada recognized that Canadian police services have a constitutional duty consider the foreseeable human rights risks of sharing personal information with foreign law enforcement authorities:

> Where a disclosing party ***knows or should have known*** that the information could be used in unfair trials, to facilitate discrimination or political intimidation, or to commit torture or other human rights violations — concerns rightly expressed by Justice Karakatsanis — s. 8 requires that the disclosure, if permissible at all, be carried out in a reasonable manner. In the most serious examples, where there are no

[128] See, for example, *R v Bykovets*, 2024 SCC 6; *R v Reeves*, 2018 SCC 56; *R v Cole*, 2012 SCC 53; and *R v Spencer*, 2014 SCC 43.
[129] See, *R v Wong*, [1990] 3 SCR 36; *R v Colarusso*, [1994] 1 SCR 20; *R v Orlandis-Habsburgo*, 2017 ONCA 649; *R v Cole*, 2012 SCC 53; *R v Reeves*, 2018 SCC 56; *R v Spencer*, 2014 SCC 43.

steps that could be taken to mitigate the danger, s. 8 forbids disclosure entirely.[130]

There is no principled reason why the same protection against foreseeable human rights dangers should not also be afforded to people in Canada when law enforcement agencies request that foreign officials search or seize electronic data about individuals in Canada.[131] This is of particular importance given known risks and problems regarding compliance with human rights applicable to online privacy amongst states, as noted in paragraph 70.

86. In order to better address gaps in protection for human rights in cross-border investigations, the federal government should introduce legislation that would require judicial oversight of Canadian law enforcement requests for specified forms of assistance from foreign authorities. This oversight mechanism would ensure that requests are issued only when it is reasonably justified, and that any available and reasonable measures and conditions are put in place by Canadian LEAs to safeguards the privacy interests at stake. The scope of this oversight process should be the subject of review and consultation.[132]

87. The absence of judicial oversight over Canadian LEA requests for foreign searches and seizures can result in inappropriate consequences or even potential violations of human rights. As a hypothetical, at present, under the current structure of Canada's search and seizure laws, Canadian law enforcement officials could foreseeably contact a law enforcement official in the USA and request that the foreign official run a search of the facial recognition database offered by Clearview AI to assist in a Canadian police investigation. Despite findings in Canada that Clearview AI is violating Canadian privacy law,[133] Clearview AI is still continuing to operate, is used by US law

[130] *Wakeling v United States of America*, 2014 SCC 72 at para 80 [emphasis added]. See also, *Canada (Justice) v Khadr*, 2008 SCC 28 at para 27.
[131] For example, requiring judicial oversight over the question of whether Canadian authorities should issue a request for foreign assistance in specified circumstances does not trench into the same questions surrounding state sovereignty and consent, as were at issue in the *Hape*-related jurisprudence.
[132] For example, at a minimum, the legislation should be applicable in circumstances where no foreign court is anticipated to assess and determine whether there are requisite grounds to authorize the search or seizure of information that is the subject of a reasonable expectation of privacy of a person in Canada, if the data were located in Canada.
[133] *Joint Investigation of Clearview AI by the Office of the Privacy Commissioner of Canada,the Commission d'accès à l'information du Québec, the information and Privacy Commissioner for British Columbia and the Information Privacy Commissioner of Alberta* (2 February 2021), PIPEDA Findings #2021-001, online: Office of the Privacy

enforcement officials without judicial oversight, and has refused to remove Canadian profiles from their database.[134] Despite being unable to run searches of Clearview AI directly under Canadian privacy law,[135] Canada's current search and seizure laws still would not expressly require that Canadian law enforcement officials obtain judicial authorization in Canada before asking US officials to run a search of Clearview AI on their behalf. This is notwithstanding the fact that the search may be entirely focused on Canadians or persons in Canada, the comparison in Clearview AI's platform would be run using facial images photographed and uploaded in Canada (but which were unlawfully scraped by Clearview AI), and the search would not have taken place but for the request of a Canadian official.

88. Inadequate oversight over cross-border investigative requests by Canadian officials can also incentivize forum shopping or outsourcing of the use of unlawful investigative methods or inappropriate data collection by Canadian LEAs. In 2020, Citizen Lab research revealed that law enforcement officials in Ontario designed a technology to scan online chat rooms, and to scrape and store the content of the chat room conversations into a searchable database that is accessible to LEAs.[136] Of particular concern, the technology reportedly enables law enforcement authorities to gain access even to particularly private communications, such as communications involving two or few participants alone, or conversations that are password-protected.[137] Despite it being a technology that was designed in Canada by a Canadian LEA,[138] the tool was subsequently given to US-based law enforcement officials, and is now operated by US officials.[139] Then, Canadian LEAs proceeded to

Commissioner of Canada <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/>.

[134] *Clearview AI, Inc v Information and Privacy Commissioner of British Columbia* (2022), Supreme Court of British Columbia at para 2 [Petition to the Court], online (pdf): <https://www.oipc.bc.ca/orders/3630>.

[135] *Police Use of Facial Recognition Technology in Canada and the Way Forward* (10 June 2021), Special Report of the Office of the Privacy Commissioner of Canada, online: <https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/sr_rcmp/>.

[136] Robertson et al, "To Surveil and Predict" at pages 60-61.

[137] *Ibid*.

[138] *Ibid* and Kate Allen, "'Algorithmic policing' in Canada needs more legal safeguards, Citizen Lab report says" *Toronto Star* (1 September 2020), , online: <https://www.thestar.com/news/canada/algorithmic-policing-in-canada-needs-more-legal-safeguards-citizen-lab-report-says/article_587ce9f7-1db5-595c-a6e0-d3f6120882bf.html>.

[139] Allen, "'Algorithmic policing' in Canada needs more legal safeguards".

obtain access through their US counterparts, and did so without obtaining prior judicial approval.[140]

89. In short, in the digital age where individuals in Canada depend extensively on online services, Canada's current legal framework governing search and seizures is no longer fit-for-purpose.[141] Judicial oversight is the key mechanism for ensuring that the public can have confidence that individuals are *secure* against unreasonable searches and seizures, even when Canadian authorities request the assistance of a third party agent on their behalf.[142]

Part 6. Conclusion

90. This submission has reviewed key reasons why **Canada should not ratify the Protocol**. Instead, we recommend that Canada play a leadership role in prioritizing and committing to international efforts to address gaps in human rights protections applicable to cross-border data sharing in law enforcement investigations, and to invest in fully resourcing cross-border data-sharing protocols that require and harmonize robust human rights protections from all signatories. Canada and its international allies must also play a leading role in the development of an international treaty addressing transnational dissident cyber espionage.[143] The "absence of clear rules regarding cyber espionage is an opportunity for States: it provides a legal vacuum in which dissident cyber espionage can take place with few restraints."[144]

91. While the Protocol contains some opportunity for Canada to reserve against some of the most intrusive aspects of the Protocol, opportunities for reservations are too limited, and fail to offset the reality that the instrument itself, as a whole, represents a threat to human rights everywhere. As the European Court of Human Rights has previously noted:

[140] *Ibid*.
[141] Although the Courts have been alive to risks of inappropriate privacy intrusions triggered by Canadian law enforcement's tactical choice to rely on investigative methods in foreign jurisdictions, those concerns have generally been compartmentalized under "trial fairness" considerations that could result in the exclusion of evidence: *R v Terry*, [1996] 2 SCR 207 at para 26; *R v Giles*, 2015 BCSC 1744, at para 306. However, many investigative activities do not yield criminal trials, and the purpose of section 8 of the *Charter* is not to not to protect the fairness of trials, but is rather to prevent unreasonable privacy intrusions.
[142] *R v Duarte*, [1990] 1 SCR 30.
[143] Anstis, "Regulating Transnational Dissident Cyber Espionage."
[144] *Ibid* at 267.

> *…the mere existence* of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied. This threat necessarily strikes at freedom of communication between users of the telecommunications services and thereby amounts in itself to an interference with the exercise of the applicants' rights under Article 8, irrespective of any measures actually taken against them.[145]

92. These comments are apposite in the context of the Protocol. However tightly Canada may attempt to constrain the obligations that the Protocol would place on Canada to dilute its search and seizure laws, the Protocol would continue to be an affront to international human rights standards everywhere. To summarize:

    a. The Protocol permits State signatories to seize, share, retain, and use potentially even large volumes of private data from a host of service providers of information and communities technologies;

    b. The Protocol would specifically authorize, if not require, searches and seizures of private data (including information from telecommunication providers), in circumstances that fall short of international human rights obligations requiring independent authorization and review for just cause;

    c. It allows signatories to make secret agreements across borders between police agencies on their own, or between governments, that would potentially result in the wholecloth elimination of privacy and human rights safeguards;

    d. The Protocol's condonation of inadequate human rights safeguards is a direct threat to existing digital privacy rights under international human rights law. The Protocol threatens to adversely impact the coherent development of customary international law, and widespread ratification of the Protocol itself may threaten pre-existing and future international human rights treaties if States subsequently argue that those human rights treaties apply "only to the extent that [their] provisions are compatible with" the Protocol.[146]

---

[145] *Weber and Saravia v Germany*, No 54934/00 (29 June 2006) [emphasis added].
[146] See *supra* note 71, citing the *Vienna Convention on the Law of Treaties*, 23 May 1969, 1155 United Nations Treaty Series 331 (entered into force on 27 January 1980) at Article 30.

e. The optional data protection standards set out in Article 14 either fall short of, or are inconsistent with, modern data protection principles, including those in Convention 108+;

f. As discussed in paragraph 64, the Protocol further raises the threat of an expanded network for data obtained through spyware and cyber espionage to proliferate unchecked, such as through secret agreements reached under Article 14(1) or through Article 12's joint investigation teams;

g. By normalizing and tolerating an inadequate data sharing regime, the Protocol may be further weaponized against human rights by authoritarian governments around the world, who would point to the Protocol when justifying their own invasive surveillance and data sharing programs; and,

h. Gaining commitment to human rights standards in multilateral negotiations surrounding the United Nation's draft Cybercrime Convention (or other related instruments),[147] may be further undermined by States that point to the Protocol to justify the further entrenchment of lax standards, which could be applicable to more intrusive powers even than those contained in the Protocol.[148]

93. Domestically, Canada also cannot implement international treaty obligations that require lower human rights standards than those guaranteed by the *Charter*.[149] As noted in Part 3, Article 7 of the Protocol is inconsistent with constitutional rulings from the Supreme Court of Canada which prohibited warrantless seizure of subscriber data and IP data from private companies,[150] and its reasoning in those decisions is directly applicable, by analogy, to Article 6. While the Protocol attempts to differentiate between "requests" for voluntary disclosures from private companies (such as under Article 6), and compulsory orders, this is a distinction without a difference under the

[147] *Revised draft text of the convention*, Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, 2023, A/AC.291/22/Rev.1.
[148] Karen Gullo & Katitza Rodriguez, "EFF to Council of Europe: Flawed Cross Border Police Surveillance Treaty Needs Fixing—Here Are Our Recommendations to Strengthen Privacy and Data Protections Across the World" *Electronic Frontier Foundation* (30 August 2021), online: <https://www.eff.org/deeplinks/2021/08/eff-council-europe-flawed-cross-border-police-surveillance-treaty-needs-fixing>.
[149] *Kazemi Estate v. Islamic Republic of Iran*, 2014 SCC 62 at para 149.
[150] *R v Bykovets*, 2024 SCC 6; *R v Spencer*, 2014 SCC 43.

Charter.[151] The constitutionality of whether, or how, Canada could implement the remainder of the Protocol in Canada would be subject to intense constitutional scrutiny and court challenges, particularly given other problems identified with Articles 9, 12, 13, and 14. As an illustration of the chaotic effect of inadequate protections under international agreements, in 2015 and again in 2020, the European Court of Justice struck down the underpinnings of two successive versions of data sharing agreements between the EU and the USA, for failing to provide adequate safeguards for personal information sent to the USA.[152]

94. All individuals in Canada depend upon the increased security that meaningful judicial oversight and supervision provides as a safeguard for better ensuring that personal information about private online activity and communications is not unjustifiably obtained by LEAs without a reasonable basis for doing so. Human rights dangers are particularly acute when sharing private, sensitive information with foreign authorities, given the Protocol provides another opportunity for States to leverage legal procedures in rights-respecting countries in order to engage in acts of transnational repression.

95. This is why diminishing or eliminating core human rights safeguards, including independent judicial oversight, is a severe and disproportionate response to addressing administrative inefficiency in existing mutual legal assistance channels. Canada has existing mutual legal assistance mechanisms with countries in all parts of the globe, and has the ability to set standards with its allies to set fixed timelines, and to build capacity, training and resources to enable these mechanisms to be more effective, while better safeguarding human rights. Canada should lead by example in doing so.

---

[151] *Ibid* and *R v Reeves*, 2018 SCC 56; and *R v Cole*, 2012 SCC 53. As noted in Part 3, Canada's constitution rejects the authority of private companies to give purported consent on behalf of a user to the warrantless seizure of private data by LEAs

[152] Case C-362/14, *Schrems v. Data Protection Commissioner* [2015], ECLI:EU:C:2015:650 and Case C-311/18, *Data Protection Commissioner v. Facebook Ireland Ltd.*, [2020], ECLI:EU:C:2020:559. See also, Opinion 1/15, *Re Draft Agreement Between Canada and the European Union - Transfer of Passenger Name Record data from the European Union to Canada* [2017], ECLI:EU:C:2017:592 at paras 168-174 and 232 (3)(b) and 3.(b), where the European Court of Justice (CJEU) ruled that an agreement between the EU and Canada was incompatible with EU law, in part due to the absence of specific safeguards concerning the automated processing of data shared under the agreement.

96. Particularly given the significant *Charter* and human rights risks at stake, meaningful public debate about the Protocol should be properly informed with government transparency about existing cross-border data sharing systems by the Canadian authorities, including law enforcement and the Department of Justice. Currently, we have been unable to find statistics concerning the number of requests that are sent and received by Canada under mutual legal assistance treaties, which countries are involved in those requests, and what type of delay or backlog exists in Canada, if any. This information should be made readily available to the public as a companion to Canada's consultation paper. Furthermore, the government has not published readily available information about what reforms, including training and staffing, have been made in Canada to address any delay within mutual legal assistance proceedings in Canada.

97. Finally, as outlined in Part 5, Canada should not move forward with expanding law enforcement's unsupervised access data across borders without first ensuring that it has first fully addressed existing risks associated with uncertainty surrounding the applicability of the *Charter* and international human rights obligations to extraterritorial and cross-border investigations. Of particular importance, we recommend that the federal government should examine and reform, in consultation with the public and experts, its search and seizure laws to implement independent judicial oversight and supervision in respect of cross-border investigation requests. Particularly in the digital age where individuals in Canada depend extensively on online services, Canada's current framework is outdated, and no longer fit-for-purpose. The public should be entitled to have confidence that individuals are secure against unreasonable searches and seizures of their private, online data.