VOLUME 7 · ISSUE 04

BALSILLIE PAPERS

Will Canada's Bill C-8 Impact the Future of EU-Canada Cross-border Data Flows?

Matt Malone

July 23, 2025

Canada's proposed cyber security for critical infrastructure bill, Bill C-8, which reintroduces Bill C-26 from the previous Parliament (with minor tweaks), could lead to a re-evaluation of the European Commission's adequacy decision concerning Canada's data protection laws. As such, the bill could push Canada to the brink of a disruption in the framework governing cross-border data flows between the two jurisdictions. Such a scenario would create tremendous uncertainty for actors in the digital economy who routinely process Europeans' personal data, such as airlines, financial institutions, information management service providers, cloud and data storage companies, and e-commerce platforms.

Introduction

Canada's proposed cyber security for critical infrastructure bill, Bill C-8,[1] which reintroduces Bill C-26 from the previous Parliament (with minor tweaks),[2] could lead to a re-evaluation of the European Commission's adequacy decision concerning Canada's data protection laws. As such, the bill could push Canada to the brink of a disruption in the framework governing cross-border data flows between the two jurisdictions. Such a scenario would create tremendous uncertainty for actors in the digital economy who routinely process Europeans' personal data, such as airlines, financial institutions, information management service providers, cloud and data storage companies, and e-commerce platforms.

Historically, the European Commission has recognized Canada with adequacy decisions as a safe harbour for Europeans' personal data.[3] These decisions have served as a key legal basis for cross-border data flows from the European Union to Canadian commercial enterprises. Bill C-8, however, which is likely to become law in due course,[4] endows the federal government with new security-related order-making and information-collecting powers. These kinds of powers have historically drawn scrutiny from European regulators and courts — and even led to the annulment of the European Commission's adequacy decisions for other jurisdictions in the past. Canadian decision makers should anticipate that these new powers may attract similar scrutiny from European authorities, while European decision makers should contemplate the consequences and impact of these new powers. This paper argues that the Canadian federal government should proactively address these concerns by strengthening privacy and data protection rights to avoid potential disruptions in cross-border data flows between Europe and Canada.

Background on EU Adequacy Decisions and Surveillance Concerns

Europe plays a significant role as a norm-setting power in international governance, especially in the area of privacy and data protection law. One of the clearest examples of this soft power is the European Commission's ability to issue, amend or revoke adequacy decisions, which lay a critical foundation for cross-border data flows.[5] Under EU law,[6] the transfer of Europeans' personal data may take place only subject to certain safeguards, such as binding corporate rules,[7] codes of conduct,[8] standard contractual clauses[9] or explicit consent. However, the most convenient framework is an adequacy decision — a decision by the European Commission that data transfers to foreign jurisdictions writ large are permissible because those jurisdictions ensure "an adequate level of [data] protection" for Europeans' personal data, matching protections enjoyed in the European Union.[10] Notably, the framework of the Charter of Fundamental Rights of the European Union (the Charter) ensures not only a right to private life, but "the right to the protection of personal data" and concomitant rights to the processing of data "for specified purposes and on the basis of the consent of the person" in a manner "subject to control by an independent authority," with the right to an effective remedy and a fair trial.[11]

According to Directive 95/46/EC, the first comprehensive legal framework within the European Union for data protection, these determinations were taken on the basis of "all the circumstances surrounding a data transfer operation or set of data transfer operations."[12] Directive 95/46/EC outlined the goals and principles governing the lawful processing of personal data of Europeans, and required EU member states

to incorporate these principles into their domestic laws. In 2018, Directive 95/46/EC was repealed and replaced by the General Data Protection Regulation (GDPR), which is now directly binding on EU member states and governs "the processing of personal data and rules relating to the free movement of personal data."[13] Like Directive 95/46/EC, the GDPR allows for the transfer of personal data from Europe to foreign jurisdictions without specific authorizations only if those jurisdictions ensure "an adequate level of protection."[14] This multifaceted assessment considers factors such as the nature of the legal regime (in particular, "effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred"[15]), the existence of an independent supervisory body "with responsibility for ensuring and enforcing compliance with the data protection rules,"[16] and the existence of binding conventions or instruments that bolster respect for the protection of personal data.[17]

The *Schrems* cases, launched by Austrian activist Max Schrems against Facebook, demonstrate just how seriously the Europeans take this legal framework. In 2000, the European Commission rendered an adequacy decision on the "Safe Harbour Principles" pursuant to Directive 95/46/EC, which allowed for block transfers of Europeans' personal data to the United States; however, in 2015, in its *Schrems I* decision regarding Schrems' complaint against Facebook — largely focused on American surveillance programs "involving the large-scale collection and processing of personal data" that accessed data collected by Facebook — the Court of Justice of the European Union (CJEU), the highest court on EU law, invalidated that framework.[18] Then, in 2016, the European Commission adopted its "privacy shield" adequacy decision to replace it. But in its *Schrems II* decision, in which Schrems revived concerns about American surveillance programs collecting personal information via Facebook, the CJEU invalidated that framework, too.

At the core of these decisions were concerns about American surveillance activities and practices, such as the explosive disclosures of whistleblower Edward Snowden. Of particular concern was Section 702 of the Foreign Intelligence Surveillance Act, which effectively authorizes the warrantless targeting of "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[19] Similarly, Executive Order 12333 has been viewed as a wide permit for law enforcement and intelligence agencies to engage in sweeping data collection and surveillance practices.[20] In *Schrems II*, these instruments garnered particular scrutiny, with the CJEU concluding that they did not provide for any limitations on the powers conferred to surveillance authorities.[21] These instruments deprived individuals of actionable rights before courts to address their concerns about the treatment of their personal data.[22] This lack of redress was not fixed by an ombudsperson position specifically created to address European concerns.[23]

For its part, Canada has largely sidestepped similar scrutiny. This is somewhat surprising, given that Canadian academic authorities on privacy have long warned that the current (and proposed) Canadian privacy law is arguably inadequate under the terms of the GDPR.[24] Although Canada has repeatedly failed to update its privacy legislation,[25] its main privacy legislation for the private sector was nevertheless recognized by the European Commission in 2002 in an adequacy decision for transfers of Europeans' personal data.[26] This decision has been repeatedly renewed, most recently in January 2024, with the

European Commission noting "the Canadian legal system provides effective oversight and redress mechanisms."[27] This renewal also placed emphasis on "ongoing legislative reform" of Canadian federal privacy law, which has since been stalled. The European Commission noted it would "closely monitor future developments in this area."[28] There are, of course, some notable exceptions. Perhaps the most important is the decision regarding *EU-Canada Passenger Name Records*, the agreement that governed the transfer of passenger name record data from the European Union to Canada, which the CJEU held was incompatible with the privacy provisions of the Charter.[29] That decision threw Canada into a years-long negotiation for a replacement agreement. Nevertheless, in the main, the European Commission has shown a lighter touch vis-à-vis Canada than the United States in its willingness to grant adequacy decisions.

One particular item worth highlighting about the European Commission's renewal of its adequacy decision for Canada in 2024 is a subsequent response letter issued by the European Data Protection Board (EDPB), the regulatory agency charged with ensuring consistency in the GDPR among member states. That letter highlighted the EDPB's concern — "while not questioning the substance" of the Commission's final decision to renew the adequacy decision — that the renewal decision "did not provide a full description of the laws and practices" of Canada and other countries.[30] In other words, the EDPB has raised concerns about the comprehensiveness of the Commission's review. The EDPB then noted its own wish to see the Commissioner provide "a more detailed overview of the intelligence landscape," because "government access for law enforcement and national security purposes […] require[s] particular attention and monitoring in the future."[31]

Concerning Surveillance Provisions of the New Canadian Law

A new bill — virtually assured passage into law — may set the stage for a reversal of the European Commission's view of Canadian privacy and data protection law. Introduced by the federal government in summer 2025, Bill C-8, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts, has two main components. First, it amends the national Telecommunications Act to elevate security as an objective of Canadian telecommunications policy and creates powers ostensibly related to cyber security in that and other legislation. Second, it creates a new law, the Critical Cyber Systems Protection Act, a bill that mirrors an evolving legislative pattern observed in peer states.[32]

While the bill is well-intentioned and contains many necessary components,[33] it also contains provisions that unquestionably endow the federal government with unchecked order-making and information-collecting powers vis-à-vis telecommunications service providers and designated operators of critical cyber systems. Telecommunications service providers alone collect reams of sensitive personal information (e.g., name, address, email address, phone number, product subscriptions, service usage details, such as call records or data usage, account information, and potentially other information if it is provided), as do operators of critical cyber systems.[34] In Part I, section 15.4 allows the federal government to "require any person" at "any time and subject to any conditions that the Minister of Industry may specify" to provide the minister with "any information that the Minister believes on reasonable grounds is relevant for the

purpose of making, amending or revoking orders" under the law that allow the minister to restrict telecommunications services for security reasons.[35] This power adheres only to a subjective standard, whereby many of those orders require only the minister's opinion that an order is "necessary [...] to secure the Canadian telecommunications system."[36] Moreover, the Act is silent on how this information might be repurposed; the federal institution most likely to obtain it, the Communications Security Establishment (CSE), has mandates for both foreign intelligence collection and cyber security and information assistance.[37] Its enabling legislation does not limit it from repurposing information collected under one mandate to serve another.[38] Other order-making powers in Part I under section 15.2 have been critiqued by The Citizen Lab: "all telecom providers in Canada would be compellable through secret orders to install backdoors inside Canada's networks by weakening encryption or network equipment."[39] They note specifically: "[T]he broad language in subsections 15.2(2)(c), (l), and (m) could be used to order Canadian telecommunications companies to install lawful-access related measures in encrypted components of Canada's telecommunication networks."[40] Measures in Bill C-2, An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures, exacerbate the concerns about legitimizing access to sensitive personal information.[41]

This raises the real possibility that personal information justifiably collected through Bill C-8 to support making cyber security orders could be repurposed toward other objectives of the CSE, such as foreign intelligence collection. Moreover, Bill C-8 permits the federal government to disclose this information to nearly anyone it wants, including foreign governments such as the United States.[42] Given Canada's commitments to sharing foreign intelligence through the Five Eyes, it is plausible this information is likely to circulate beyond Canadian institutions.[43] The Privacy Commissioner of Canada previously warned Parliament that Bill C-26 would "grant certain regulators with warrantless search powers," and added: "Notably Bill C-26 does not limit the collection of personal information, nor does it contain safeguards to ensure that regulators (or their delegates) who carry out warrantless searches have done so reasonably."[44] But the CSE has pushed back on that. As a representative from the CSE told Parliament in the study of Bill C-26: "Any limitation would also reduce the CSE's collaboration with our Five Eyes partners."[45] This raises the likely possibility that the information will be shared, intentionally or accidentally, with the US government, among others, for purposes such as intelligence collection or national security investigations; this has happened in the past.[46] As the Privacy Commissioner of Canada has noted: "These broad powers could lead to far-reaching and persistent information-sharing, without individuals' awareness or consent."[47]

In Part II, Bill C-8 also creates a new "cyber security direction" power that enables the government to order designated operators of critical infrastructure systems "to comply with any measure set out in the direction for the purpose of protecting a critical cyber system."[48] The designated operators are identified by the government from among services and systems deemed "vital." Unlike the CSE's enabling legislation, which requires pre-approval for the CSE's spying activities that contravene federal law or interfere with the reasonable expectation of privacy of individuals in Canada,[49] there is no similar oversight mechanism in this law — a serious worry if the CSE operates under the "technical and operational assistance" prong of its mandate by helping the Minister of Public Safety and Emergency

Preparedness.[50] Indeed, the law is specifically exempt from provisions of the Statutory Instruments Act that would require publication and provide review.[51]

Designated operators receiving cyber security directions cannot even disclose their existence, except to the extent necessary to implement them.[52] The only oversight of these powers is a requirement, after an order has been made, to notify two review bodies, the National Security and Intelligence Committee of Parliamentarians and the National Security and Intelligence Review Agency (NSIRA). However, the CSE has a demonstrated history of failing to provide these review bodies with documents as part of their work,[53] in addition to having other problems with transparency, such as compliance with the Access to Information Act.[54] In its most recent annual report, NSIRA reiterated that the CSE was consistently requesting ministerial authority necessary to engage in cybersecurity and information assurance that "did not fully reflect its activities in practice,"[55] and failed to provide statistics on information related to Canadians or persons located in Canada, to which the CSE refused to respond.[56] The CSE's respect for the Privacy Act is also broadly questionable, as the CSE follows its own internal (and currently undisclosed) privacy policies that interpret this Act, creating uncertainty about the nature of the 139 "privacy incidents" identified in a recent annual report and whether these incidents accurately reflect respect for Canadians' privacy rights under that legislation.[57]

Bill C-26 initially contained a judicial review mechanism to review these powers, but it has been superseded by a new mechanism created in Bill C-70, An Act respecting countering foreign interference. Bill C-70 was rushed through Parliament in summer 2024 with unanimous support from all parties, with the main objective of creating a foreign agent registry (still not established more than a year later) and defining new criminal offences for foreign interference. Bill C-70 also created a new judicial mechanism in the Canadian Evidence Act called Secure Administrative Review Proceedings (SARP), which will be used in judicial reviews of the orders made under the powers created by Bill C-8. One reason this is particularly concerning is that SARP, unlike traditional judicial reviews, deprives parties of the right to a lawyer by allowing representation only through the appointment of a Special Counsel protecting their interests — not in an attorney-client relationship.[58] It also allows for withholding evidence from affected parties. The SARP mechanism was shoehorned into the law after the Privacy Commissioner of Canada had already warned that "individuals whose personal information may have been collected by the government and used to support a direction or order that affects them, may never know."[59]

Potential EU Concerns Regarding Bill C-8

The GDPR requires the European Commission to monitor legal developments in foreign jurisdictions that could affect adequacy decisions,[60] and subjects adequacy decisions to a review every four years.[61] When a review indicates that a third-party country or organization "no longer ensures an adequate level of protection," the European Commission is required to "repeal, amend or suspend" the adequacy decision permitting the transfer of European personal data to that jurisdiction.[62] When that occurs, the European Commission is required to consult with that jurisdiction to remedy the situation.[63] Bill C-8 will likely attract European regulatory scrutiny when Canada's data protection regime comes up for review. The Privacy Commissioner of Canada warned Parliament in February 2024 that the powers contained in Bill

C-26 may attract such scrutiny by the European Commission, opining that "[t]he thresholds authorizing the collection of information in Bill C-26 fall short of a necessity and proportionality standard and may attract scrutiny of Canada's adequacy status which will be reviewed every four years."[64]

The main concern that Bill C-8 is likely to raise is the vulnerability of Europeans' personal data for collection, use and disclosure under the CSE's foreign intelligence collection mandate. While the CSE is prohibited from directing its activities against Canadians or persons in Canada, nothing prohibits it from targeting Europeans located outside of Canada.[65] This concern will directly affect European customers and users to whom Canadian telecommunications service providers or designated operators of critical cyber systems are offering services that collect personal data. For example, a Canadian telecommunications service provider might have European customers who subscribe to an international roaming plan or access virtual private networks through Canada; they might work with a European company to provide cloud-based communication tools or data centre hosting, involving the processing of personal data for employees or customers of the European company; or they may collect data on European users' browsing behaviour, location or preferences through their web presences. The order-making and information-collecting powers under Bill C-8 could allow the CSE to direct telecommunications service providers in possession of such European personal data to provide that information to them — at which point nothing in Bill C-8 prevents the repurposing of that information toward its other mandates, including foreign intelligence. These practices are subject to little real oversight and no meaningful independent review. These issues complement concerns now arising in Bill C-4 (An Act respecting certain affordability measures for Canadians and another measure), which amends the Canada Elections Act. That bill removes almost all meaningful guardrails on how Canadian political parties process personal information.[66] This is a particularly high-risk area, given the GDPR considers personal data revealing "political opinions" to be a special category of sensitive data.[67]

Under *Schrems II*, the CJEU expressed concern with the extraterritorial effect of American surveillance practices, in particular Facebook's collection of data that was then accessible by American authorities. These practices interfered, the CJEU held, with fundamental rights guaranteed in the Charter by failing to comply with the specified regime established in the GDPR. The CJEU noted that any inference with privacy rights in the Charter "must lay down clear and precise rules governing the scope and application of the measure in question and imposing minimum safeguards" to ensure against any risk of abuse, namely by indicating "in what circumstances and under which conditions a measure providing for the processing of such data may be adopted, thereby ensuring that the interference is limited to what is strictly necessary."[68] Due to Section 702 and EO 12333's lack of limitations imposed on the ability to collect, purpose and repurpose data collection against non-US persons — combined with a lack of actionable rights — the court held that the adequacy decisions in question could not ensure an equivalent level of protection.[69]

Bill C-8 presents many of the same concerns. Under Part I of Bill C-8, the information-collecting powers of the federal government are basically unrestrained. As the Privacy Commissioner of Canada has noted about the predecessor bill, these powers "grant certain regulators with warrantless search powers" in the context of a highly subjective standard where the minister need only believe that the information-

collecting activity might be "relevant" to making orders.[70] Moreover, once this information is collected, Bill C-8 does not restrain the CSE from repurposing that information for other mandates — a concern the Privacy Commissioner of Canada has flagged.[71] These defects in the bill resemble Section 702 and EO 12333 by neglecting to cabin the data collection in scope and purpose. Part I of Bill C-8 also raises questions about the powers described above, which, in theory, could require telecommunications service providers to undermine encryption standards. A recent European Court of Human Rights decision, *Podchasov v Russia*, aimed squarely at a recent Russian law that imposed a requirement to decrypt encrypted communications "on a generalised basis and without sufficient safeguards" as a contravention of the Charter.[72] Some have opined that this decision may entail "a European right to end-to-end encryption."[73]

Under Part II of Bill C-8, these concerns become even more pronounced, since it is not clear how SARP proceedings will even take place with respect to cyber security directions. Designated operators receiving a cyber security direction cannot disclose its existence, except to the extent necessary to implement it.[74] This total blackout of information means that information collected under Part I of Bill C-8 might be used for the purpose of issuing a cyber security direction under Part II, which parties may never know about. This defect raises concerns about whether the legal regimes maintain "effective and enforceable data subject rights and effective administrative and judicial redress for the data subjects whose personal data are being transferred."[75] Presumably, this problem is less likely to present under sections 15.1 and 15.2 of Part I of Bill C-8, since any orders taken under these provisions are far more likely to garner public attention (e.g., disconnecting a party's connection to a telecommunications service provider). It is already a significant problem in the legislation that there is no pre-approval oversight process for the issuance of these directions, such as by the Intelligence Commissioner. Directions need only have "the purpose of protecting a critical cyber system" and be based only on "reasonable grounds that it is necessary to make the order for that purpose,"[76] with only the weakest requirements for notification after the fact.[77]

Recommendations and Conclusions

Bill C-8 is ostensibly a cyber security bill. However, several of the order-making provisions it contains — under section 15 of Part I and section 20 of Part II — go far beyond what is necessary for cyber security and information assurance. Indeed, section 15.4 of Part I and section 20 of Part II seem like unconcealed efforts to thwart the oversight mechanisms established in the Communications Security Establishment Act, which provide that the agency must obtain approval from the Office of the Intelligence Commissioner when the CSE's spying activities contravene federal law or interfere with the reasonable expectation of the privacy of individuals in Canada.[78] Indeed, as Intelligence Commissioner Simon Noël warned the Senate Standing Committee on National Security, Defence and Veterans Affairs in its study of Bill C-26:

> There are two areas I want to highlight for your consideration. First, the proposed section 15.4 of the *Telecommunications Act* allows the minister to compel the production of any information in support of the orders. This information could include personal information, which, under broad

> exceptions, could then be widely disclosed. Second, […] [Part II of Bill C-26] allows for the regulators to carry out unwarranted searches where, again, personal information could be collected. Who is missing in this big picture? It is the Canadian public.[79]

Strangely, the Intelligence Commissioner's oversight powers under the Communications Security Establishment Act were highlighted to the European Commission in the Canadian federal government's most recent "Update Report" for the purposes of reviewing the renewal of the adequacy decision. Now, those same powers are being suddenly diminished in Bill C-8. When the time comes for European regulators to look once again at the state of Canadian privacy and data protection law, the legacy of Bill C-8 is almost certain to garner scrutiny (as will the ongoing reform of Canadian private sector privacy legislation, which is currently stalled).[80]

If Canada does not act to fix these problems, the passage of Bill C-8 (as well as Bill C-2 and Bill C-4) may present a "backdoor" for privacy and human rights activists to turn to European law to challenge not only Bill C-8 but also, more broadly, the current state of privacy law in Canada — namely, by using the concerning provisions in Bill C-8 as an opportunity to challenge the "adequacy" determination currently given to Canada. In the event the European Union were to find Canada's privacy framework lacking, this could upend the foundation upon which cross-border data flows between the two blocs now occur. In turn, that could create enormous uncertainty for Canadian actors in the digital economy who collect, use and disclose personal data. This situation could mirror the uncertainty after the CJEU invalidated the *EU-Canada Passenger Name Records*[81]— a decision that precipitated years of negotiation for an appropriate replacement.

Acknowledgements

The author thanks Adam Richert, Nicole Langlois, and Saad Hammadi for their editing assistance, as well as three anonymous reviewers for their very helpful feedback. This article elaborates on comments made on two occasions: an appearance on November 4, 2024, at the Senate Standing Committee on National Security, Defence and Veterans Affairs during its study of Bill C-26; and a panel at the Balsillie School of International Affairs on November 5, 2024, on the topic of "Rethinking Canada's Digital Future," featuring Vass Bednar, David Skok, Benjamin Revcolevschi and the author, and moderated by Ann Fitz-Gerald.

Endnotes

[1] Bill C-8, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 45th Parl, 2025 (as introduced by the House of Commons 18 June 2025) [Bill C-8].

[2] Bill C-26, *An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts*, 1st Sess, 44th Parl, 2024 (as passed by the House of Commons 19 June 2024) [Bill C-26].

[3] See e.g. EC, *Commission Decision No 087/ 2002 EEA of 20 December 2001 pursuant to Directive 95/46/EC on the adequate protection of personal data provided by the Canadian Personal Information and Electronic Documents Act* [2002] OJ, L 002/0013 at 13–16. See also EC, *Report from the Commission to the European Parliament and the Council on the first review of the functioning of the adequacy decisions adopted pursuant to Article 25(6) of Directive 95/46/EC*, COM/2024/7.

[4] The predecessor bill, Bill C-26, finished third reading in the Senate with minor proposed amendments and sent back to the House of Commons on December 5, 2024. However, the fall of the Trudeau government shortly thereafter prevented the bill from passing.

[5] Laurent Cohen-Tanugi, "Europe as an international normative power: state of play and perspectives," *Groupes d'études géopolitiques*, December 2021, https://geopolitique.eu/en/articles/europe-as-an-international-normative-power-state-of-play-and-perspectives/.

[6] EC, *General Data Protection Regulation*, [2016], OJ L 127, art 45(1) [*GDPR*].

[7] *Ibid*, art 47.

[8] *Ibid*, art 40.

[9] *Ibid*, art 46(3).

[10] EC, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] OJ, L 281 [*Directive 95/46/EC*]. Article 25 of Directive 95/46/EC was later reprised in article 45(1) of the GDPR. Under article 45(3) of the GDPR, these adequacy decisions are subject to review at least every four years.

[11] EC, *Charter of Fundamental Rights of the European Union*, [2000] OJ, C 364/01, arts 7, 8, 47 [*Charter*].

[12] *Directive 95/46/EC*, *supra* note 10.

[13] *GDPR*, *supra* note 6, art 1.

[14] *Ibid*, art 45(1).

[15] *Ibid*, art 45(2)(a).

[16] *Ibid*, art 45(2)(b). Likewise, article 52(1) of the GDPR requires that supervisory authorities for privacy and data protection act "with complete independence in performing [their] tasks and exercising [their] powers in accordance with [the GDPR]."

[17] *GDPR*, *supra* note 6, art 45(2)(c).

[18] *Maximillian Schrems v Data Protection Commissioner* [2015] CJEU Case 362/14.

[19] *FISA Amendments Act of 2008*, 50 USC § 1881a (2008) ("Procedures for targeting certain persons outside the United States other than United States persons"). The provision has been consistently renewed. See *FISA Amendments Act Reauthorization Act of 2012* (2012) at 112, and *FISA Amendments Act Reauthorization Act of 2017* (2017) s 139. "FISA Section 702 Reauthorized for 2 years," *Lawfare* (30 April 2024), online: <https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years>.

[20] US, *Executive Order 12333* of Dec. 4, 1981, appearing at 46 FR 59941, 3 CFR, 1981 Comp., p 200, unless otherwise noted.

[21] *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems*, [2020] ECHR Case 311/18 at para 63 [*Schrems II*].

[22] *Ibid* at paras 180–82.

[23] *Ibid* at para 197.

[24] See Colin Bennett, "The 'Adequacy' Test: Canada's Privacy Protection Regime Passes, but the Exam Is Still On," Centre for International Governance Innovation (April 3, 2024), online: <https://www.cigionline.org/articles/the-adequacy-test-canadas-privacy-protection-regime-passes-but-the-exam-is-still-on/>; Colin Bennett, "Submission on Bill C-27, Digital Charter Implementation Act to House of Commons Standing Committee on Industry and Technology, October 26, 2023," online: <https://www.colinbennett.ca/blog/submission-on-bill-c-27-digital-charter-implementation-act-to-house-of-commons-standing-committee-on-industry-and-technology-october-26-2023/>.

[25] LEGISinfo, "Overview 44th parliament, 1st session" (22 November 2021), online: <https://www.parl.ca/legisinfo/en/overview>.

[26] See *Personal Information Protection and Electronic Documents Act*, SC 2000, c 5. The adequacy decisions from the European Commission (2002/2/EC) were carried out under the auspices of Directive 95/46/EC, *supra* note 10.

[27] *Report from the Commission to the European Parliament and the Council*, *supra* note 3.

[28] *Ibid.*

[29] *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, Opinion 1/15 at para 232.

[30] Ana Talus Letter to Michael McGrath, "EDPB letter to the European Commission on its review of its eleven adequacy decisions adopted under Directive 95/46/EC," online: <https://www.edpb.europa.eu/system/files/2024-12/edpb_letter_20241205_european-commission-review-of-11-existing-adequacy-decisions_en.pdf>.

[31] *Ibid.*

[32] CIRCIA in the US (https://www.congress.gov/bill/117th-congress/house-bill/2471/text); US, *Consolidated Appropriations Act, 2022,* 136 Stat 49; Australia, *Security of Critical Infrastructure Act 2018*, compilation No 2023/6, online: <https://www.legislation.gov.au/Series/C2018A00029>; and NIS2 in the EU (https://eur-lex.europa.eu/eli/dir/2022/2555), *Directive (EU) 2022/2555 of the European Parliament and the Council of 14 December 2022*, OJ L 333 27.12.2022, at 80.

[33] *FISA Amendments Act Reauthorization Act of 2012*, *supra* note 19 at 112. Although the following articles discuss Bill C-26, they remain relevant to C-8. See Matt Malone, "As Drafted, Canada's New Cybersecurity Law Opts for Secrecy over Security," Centre for International Governance Innovation (26 August 2024), online: <https://www.cigionline.org/articles/as-drafted-canadas-new-cybersecurity-law-opts-for-secrecy-over-security/>; Matt Malone and Russell Walton, "Canada's Proposed Cybersecurity Law Is Flawed, but Can Be Salvaged," Centre for International Governance Innovation (23 April 2023), online: <https://www.cigionline.org/articles/canadas-proposed-cybersecurity-law-is-flawed-but-can-be-salvaged/>.

[34] For an illustrative example, see the privacy policy for the largest telecommunications service provider in Canada: Bell Canada, "Personal information and your privacy," online: <https://www.bell.ca/Security_and_privacy/How_we_collect_and_use_data#personalInfoSection>.

[35] Bill C-8, *supra* note 1, Part 1, s 15.4. This power to compel the provision of information supports other order-making powers under Bill C-8, Part 1, ss 15.1, 15.2.

[36] *Ibid*, Part 1, s 15.1.

[37] *Communications Security Establishment Act*, SC 2019, c 13, s 76, s 15(1) [*CSE Act*].

[38] As the director general of Strategic Policy for the CSE told the House of Commons during its study of Bill C-26: "Information collected by CSE pursuant to one aspect of its mandate can be used by CSE under another aspect of the mandate."

House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 44-1, No 101 (8 April 2024) at 1540 (Steve Bolton).

[39] The Citizen Lab (Kate Robertson), "Submission to the Senate Standing Committee on National Security, Defence and Veterans Affairs: Study of Bill C-26, An Act respecting cyber security, amending the Telecommunications Act and making consequential amendments to other Acts," at para 35, online: <https://sencanada.ca/Content/Sen/Committee/441/SECD/briefs/Brief_CitizenLab_AMENDED_e.pdf>.

[40] *Ibid.*

[41] Bill C-2, *An Act respecting certain measures relating to the security of the border between Canada and the United States and respecting other related security measures,* 1st Sess, 45th Parl, 2025 (as introduced by the House of Commons 3 June 2025).

[42] Bill C-8, *supra* note 1, Part I, s 15.7.

[43] Stephanie Hogan, "What are the 'Five Eyes'? As Canada accuses India, what you need to know about the intelligence alliance", *CBC* (21 Sept 2023), online: <https://www.cbc.ca/news/canada/five-eyes-canada-india-1.6972210>.

[44] Office of the Privacy Commissioner of Canada, "Issue sheets on Bill C-26" (14 June 2024), online: <https://www.priv.gc.ca/en/privacy-and-transparency-at-the-opc/proactive-disclosure/opc-parl-bp/secu_20240212/is_20240212/>.

[45] Standing Committee on Public Safety and National Security, *supra* note 38.

[46] Catharine Tunney, "Spy agency says it 'improperly' shared Canadians' data with international partners," *CBC* (21 June 2025), online: <https://www.cbc.ca/news/politics/cse-intelligence-commissioner-shared-information-1.7566777>.

[47] Office of the Privacy Commissioner of Canada, *supra* note 44.

[48] Bill C-8, *supra* note 1, Part II, s 20(1).

[49] *CSE Act*, *supra* note 37, c 13, s 76 at ss 26, 28.

[50] *Ibid*, c 13, s 20.

[51] Bill C-8, *supra* note 1, Part II, s 22(1).

[52] *Ibid*, Part II, s 25.

[53] Christopher Parson, "Don't give more powers to the CSE until it submits to effective review", *Policy Options* (9 November 2022), online: <https://policyoptions.irpp.org/magazines/november-2022/communications-security-establishment-review/>.

[54] Matt Malone, "Trudeau promised radical transparency. Instead, he has exacerbated closed government", *The Hub* (23 February 2024), online: <https://thehub.ca/2024/02/23/matt-malone-trudeau-promised-radical-transparency-instead-he-has-exacerbated-closed-government/>.

[55] National Security and Intelligence Review Agency, "2023 Annual Report" (26 Sept 2024) at 70.

[56] *Ibid* at 77 and 78.

[57] Communications Security Establishment Canada, "Communications Security Establishment Annual Report 2023/2024" (25 June 2024).

[58] Bill C-70, *An Act respecting countering foreign interference*, 1st Sess, 44th Parl, 2024 (assented to 20 June 2024) at 38.35(3).

[59] Office of the Privacy Commissioner of Canada, *supra* note 44.

[60] *GDPR*, *supra* note 6, art 45(4).

[61] *Ibid*, art 45(3).

[62] *Ibid*, art 45(5).

[63] *Ibid*, art 45(6).

[64] Office of the Privacy Commissioner of Canada, *supra* note 44.

[65] *CSE Act, supra* note 37, c 13, s 76, s 22(1).

[66] Bill C-4, *An Act respecting certain affordability measures for Canadians and another measure*, 1st Sess, 44th Parl, 2024 (introduced 5 June 2025).

[67] *GDPR, supra* note 6, art 9.

[68] *Schrems II*, *supra* note 21, at para 176; *Opinion 1/15 Data Protection Commissioner v Facebook Ireland Limited and Schrems,* [2017] ECLI at para 141.

[69] *Schrems II, supra* note 21, at paras 180–82.

[70] Bill C-8, *supra* note 1, Part 1, ss 15.1, 15.2, 15-4.

[71] Office of the Privacy Commissioner of Canada, *supra* note 44 ("Notably Bill C-26 does not limit the collection of personal information. Not does it contain safeguards to ensure that regulators (or their delegates) who carry out warrantless searches have done so reasonably").

[72] *Podchasov v Russia*, Application no 33696/19, ECHR (13 May 2024).

[73] Jessica Shurson, "A European right to end-to-end encryption" (2024) *Computer L & Security Rev* 55.

[74] Bill C-8, *supra* note 1, Part II, ss 24 and 25.

[75] *GDPR*, *supra* note 6, art 45(2)(a).

[76] Bill C-8, *supra* note 1, Part II, s 20(1).

[77] *Ibid,* Part II, s 20(4).

[78] *CSE Act*, *supra* note 37, c 13, s 76 at ss 26–28.

[79] Intelligence Commissioner of Canada, "Remarks to the Standing Senate Committee on National Security, Defence and Veterans," 18 November 2024.

[80] EC, *Report from the Commission to the European Parliament and the Council*, *supra* note 3.

[81] EC, *Re Draft Agreement Between Canada and the European Union*, *supra* note 29.

Matt Malone, Balsillie Scholar (September - December 2024), is the Samuelson-Glushko Assistant Professor at the University of Ottawa Faculty of Law. He is also the Founder of Open by Default. Matt's main research interest pertains to the various ways law protects secret information, especially in the context of trade secrecy, confidential information, access to information, privacy, data protection, and cybersecurity. He also maintains a broad interest in legal issues pertinent to modern workplaces, in particular workplace investigations.

BALSILLIE PAPERS

balsilliepapers.ca

ISSN 2563-674X
doi:10.51644/BAP74