C-26 Q&A

1. Do the privacy and reporting safeguards in C-26 apply to Section 15.4?

Privacy

• The privacy safeguards of C-26 do apply to 15.4, which governs information gathering to support orders made pursuant to sections 15.1 and 15.2.

• As an example of how S. 15.4 may be used, the Minister could ask for technical details on a network architecture, or what actions an operator has taken to implement an order.

- OK, fair hypothetical. But despite covenants from government officials at the CSE that the type of information that would be collected pertains largely to "technical information," an amendment to restrict the data collection specifically to "technical information" was explicitly rejected in Parliament.[1] As a representative from the CSE told Parliament: "Any limitation would also reduce the CSE's collaboration with our Five Eyes partners."[2] This raises the likely possibility that the information will be shared with the United States government, among others. 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."[3]

• S. 15.4 is not intended to capture personal information nor does it allow for surveillance; the focus is on networks, not on consumers.

- That might be the intention, but the ambit of the legislative text is much, much wider : "The Minister may require any person to provide to the Minister or any person designated by the Minister, within any time and subject to any conditions that the Minister may specify, **any information** that the Minister believes on reasonable grounds is relevant for the purpose of making, amending or revoking an order under section 15.1 or 15.2." This clearly includes personal information.
- This power is cabined by only a subjective standard, whereby many of those orders (under 15.1 and 15.2) require only the Minister's opinion that an order is "necessary [...] to secure the Canadian telecommunications system."

• It is limited by the policy objectives of the act, which include protecting the telecommunications system, but don't include general security objectives like law enforcement. It is also limited by the various other privacy safeguards in the bill, including definitions of personal and deidentified information, a prohibition on sharing any confidential information internationally or for criminal matters, as well as the Privacy Act and the Charter protections against unreasonable search and seizure.

- The issues of the definition of personal information and "de-identified" information -- which can be deemed "confidential information" by a provider -- is a red herring. The real concern is the real possibility that personal information collected through Bill C-26 to support order-making relevant to the security of the telecommunication sector may serve as a vector for information collection supporting foreign intelligence collection. Moreover, Bill C-26 permits the federal government to disclose this information to nearly anyone it wants, including foreign governments like the United States.[4] Given Canada's commitments to sharing foreign intelligence through the Five Eyes, it is plausible this information is likely to circulate beyond Canadian institutions.[5]

---

[1] House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 44-1, No 101 (8 April 2024) at 1540 (Steve Bolton). In any case, the Supreme Court of Canada has recently acknowledged that even technical information can be personal information. *See R. v. Bykovets*, 2024 SCC 6.

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

[3] Office of the Privacy Commisioner 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/>.

[4] *Blll C-26*, Part I, s 15.7.

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

• Furthermore, section 15.4 is modelled after an existing authority in the Telecommunications Act (s. 37) to collect information from regulated entities that has been in existence for over thirty years on general telecommunications matters. It has been consistently used to collect commercial information.

- There is certainly an analogy with section 37, but the difference here is with whom that information can be shared (Bill C-26, Part I, s 15.6) and the ability of organizations like CSE to repurpose this information towards its other mandates, like foreign intelligence. Despite covenants from government officials at the CSE that the type of information that would be collected pertains largely to "technical information," an amendment to restrict the data collection specifically to "technical information" was rejected in Parliament.[6] Efforts to cabin the use of the information were also specifically rejected.

Reporting

• Under s. 15.21, the Minister is required to table an annual report. That report must include certain specific information including the number of orders made, their nature, a description of compliance, and an explanation of the necessity, reasonableness, and utility of the orders.

- This is somewhat heartening, but there remain concerns. What happens if they don't provide the information? What is the penalty or mode of redress if the gov't institution is not forthcoming? Exactly as has happened in the past with CSE refusing to give information to NSIRA and NSICOP? Moreover, this annual report obligation only concerns orders under sections 15.1 and 15.2. How will the public learn about how the information collecting powers are being utilized under section 15.4?

• Section 15.4 can only be used for the purpose of making, amending or revoking an order or regulation, and for verifying compliance.

- True. But this is a very broad power with loose and subjective standards. The Minister only needs to have "reasonable grounds" that the information they are seeking to collect is "relevant" to "making, amending, or revoking" the orders (which they can make when they "believes on reasonable grounds that it is necessary to do so").
- Not just me speaking here. As the Privacy Commissioner of Canada has noted, these powers "grant certain regulators with warrantless search powers"[7] in the context of a highly subjective standard where the Minister need only believe that the information collecting activity might be "relevant" when they are "making, amending, or revoking" one of the orders to secure the telecommunications system,[8] for orders that they can make in cases they believe are "necessary [...] to secure the Canadian telecommunications system."[9]
- Moreover, once this information is collected, Bill C-26 does not restrain the CSE from repurposing that information for other mandates, like foreign intelligence—a concern the Privacy Commissioner of Canada has flagged.[10]

• While ss. 15.21 and 15.4 don't reference each other directly, they're linked by the fact that they both apply to orders issued under ss. 15.1 and 15.2.

- OK.

• The text of s. 15.21 was put forward by the NDP and they based it on a proposal by civil liberties groups. See the discussion regarding NDP-7 and the associated stakeholder submission at page 16.

- It should remain. I just wonder what happens when/if federal gov't institutions don't heed it. Look at NSIRA's latest annual report and the number of times CSE responded that the information sought "remains classified and cannot be published."

---

[6] House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 44-1, No 101 (8 April 2024) at 1540 (Steve Bolton). In any case, the Supreme Court of Canada has recently acknowledged that even technical information can be personal information. *See R. v. Bykovets*, 2024 SCC 6.

[7] Office of the Privacy Commisioner 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/> ("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.")

[8] *Bill C-26*, Part 1, s 15-4.

[9] *Bill C-26*, Part I, ss 15.1 and 15.2.

[10] Office of the Privacy Commisioner 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/> ("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.")

2. Does C-26 allow the government to gain warrantless access to private information, with no limits on how that information can be used?

• No. Bill C-26 is not intended for the collection of private information, and safeguards to prevent misuse exist in both parts of the legislation as well as in other privacy protection regimes that already exist in Canadian law.

- Intention is a misnomer; we should be looking at what the law permits. Section 15.4 clearly permits the collection of private information, and it lacks safeguards on repurposing the information. Therefore, the answer to this question ("Does C-26 allow the government to gain warrantless access to private information, with no limits on how that information can be used?") is obviously yes.

Part I: Telecommunications Act Amendments

• The scope of Part 1 is limited to the telecommunications system rather than broader law enforcement issues. It contains explicit provisions to protect the confidentiality of information, and the Minister is not permitted to order a telecommunications service provider to intercept a private communication.

- Section 15.2(2) clearly states the Minister can order a TSP to use "any product or service, or any product or service provided by a specified person, including a telecommunications service provider"; "implement specified standards in relation to its telecommunications services, telecommunications networks or telecommunications facilities"; or "do a specified thing or refrain from doing a specified thing". These are very, very broad powers.
- Also arguably, section 15.4 provides a backdoor for intercepting private communications under the pretext of potentially making orders under sections 15.1 or 15.2.

• Numerous legislative and judicial guardrails exist to prevent warrantless access to private information, and these apply to Bill C-26. Section 8 of the Canadian Charter of Rights and Freedom protects against unreasonable searches and seizures, and subsection 184(1) of the Criminal Code makes it illegal to intercept private communications.

- Indeed, I suspect the provisions under Part I will be the subject of a *Charter* challenge at some point.
- Section 184 prohibits unlawful interception -- irrelevant if the interception is lawful.

Part 2: Critical Cyber Systems Protection Act

• Part 2 of Bill C-26 authorizes the government to obtain information in two ways. Section 17 requires designated operators to report cyber security incidents above a certain threshold to the Communications Security Establishment (CSE). And subsection 23(1) permits the collection and exchange of information by certain government entities for the purpose of making, amending or revoking cyber security directions, if the Governor in Council believes on reasonable grounds that it is necessary to do so to protect a critical cyber system.

- Section 17 is needed.
- Section 23(1) is about information collection and exchange from and among government parties. Not really an issue.

• information required to protect these critical cyber systems would be related to the technical operation of the cyber system. As a result, it would be unlikely to contain personal information.

- Even technical information can be personal information, as the Hon. Simon Noel pointed out regarding the Supreme Court's *Bykovets* decision. However, I'm not particularly concerned about the information collecting powers under Part II. The bigger issues are the transparency issues (sections 24 and 25).

• Should any personal information be collected incidentally, it would be handled with the privacy protections of all applicable laws, including the Canadian Charter of Rights and Freedoms, the Personal Information Protection and Electronics Documents Act (PIPEDA) and the Privacy Act.

- Yes, but I suspect the anti-transparency provisions and the SARP elements will be subject to challenge in their own right.

• Moreover, at the request of several civil society organizations called as witnesses during the House study of Bill C-26, language was added to subsection 20(5) to make it explicit that the GIC is not permitted to order any designated operator to intercept a private communication.

- This is a good amendment.

3. Does C-26 create privacy gaps that will cause problems for Canada in the EU?

• No. Bill C-26 contains privacy safeguards and would be subject to existing Canadian privacy laws that the EU has recently examined.

- Incorrect. Part I sections 15.1, 15.2, and 15.2, and Part II section 20 create many type of powers that have normally concerned the Europeans. Look at the *Schrems* cases. At the core of these decisions were concerns about American surveillance activities. Of particular concern was Section 702 in the *Foreign Intelligence Surveillance Act*, which effectively authorized the warrantless targeting of "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[11] Similarly, Executive Order 12333, which was originally signed by President Ronald Reagan, has been viewed as a wide permit for law enforcement and intelligence agencies to engage in sweeping data collection and surveillance practices (it requires cooperation with the CIA's intelligence gathering requests).[12] In *Schrems II*, these instruments garnered particular scrutinty, with the EUCJ concluding that Section 702 and EO 12333 did not provide for any limitations on the powers conferred to surveillance authorities, including actionable rights before courts to affected data subjects.[13] When we consider all the ways in which CSE gains new powers through these bills to expand its mission to conduct SIGINT on foreigners -- including Europeans -- we should absolutely anticipate their concern about the lack of consent, the lack of redress, and the lack of independence of review bodies. Those are all aspects of the right to private life assured by the European Charter (see Articles 7, 8 and 47 of the *Charter of Fundamental Rights of The European Union*).

• A 15 January 2024 assessment by the European Commission reaffirmed its decision that Canada's private-sector privacy framework, the Personal Information Protection and Electronic Documents Act (PIPEDA), provides an adequate level of data protection. As a result, personal information can continue to flow freely from organizations in EU Member States to organizations in Canada without requiring Canadian organizations to adhere to additional data protection safeguards.

- OK, but consider that ISED's latest representations to the EU highlighted the role the Intelligence Commissioner – an office omitted from this law entirely.[14] And those representations from ISED date from 2020.

• The European Commission also extensively examined Canada's public-sector privacy law, the Privacy Act, in addition to law enforcement and national security and intelligence frameworks. It found that public authorities in Canada are subject to clear, precise and accessible rules governing the access and use of personal data for public interest objectives.

- This was a historic analysis based on the last submission of ISED to the EU (in 2020), with the decision rendered in January 2024. This *next* review will be a problem if Bill C-26 passes.

4. Does C-26 allow closed-court proceedings without safeguards?

• No. While C-26 allows for closed-court proceedings in cases involving sensitive information, there are several built-in safeguards to ensure due process and fairness. For example, only a judge – not the government – may decide to withhold certain information to prevent harm to international relations, national defence, national security, or the safety of individuals.

- SARP replaces the right to representation with "Special Counsel". And it is not even clear *how* someone affected by an oder under Part II section 20 will even know of its existence given sections 24 and 25 -- let alone have a proper way to challenge it.

• Importantly, should Bill C-26 receive Royal Assent, the relevant sections would be supplanted by Bill C-70, which sets out general procedures for Secure Administrative Review Proceedings. The protections in C-70 go even further than C-26, notably allowing for the appointment of a special counsel to protect an applicant's interests. Similar frameworks for secure proceedings exist in countries such as the U.S., U.K., and Australia.

---

[11] 50 U.S. Code § 1881a - FISA Amendments Act of 2008 ("Procedures for targeting certain persons outside the United States other than United States persons"). The provision has been consistently renewed. *See REAUTHORIZATION ACT OF 2012*, of 2 Aug 2012, p 112 (2012) and *FISA Amendments Reauthorization Act of 2017,* of 9 Jan 2018, s 139 (2017). "FISA Section 702 Reauthorized for 2 years", *Lawfare* (30 April 2024), online at: <https://www.lawfaremedia.org/article/fisa-section-702-reauthorized-for-two-years>.

[12] *Executive Order 12333* of 4 Dec, 1981, appearing at 46 FR 59941, 3 CFR, 1981 Comp., p 200, unless otherwise noted and Case 311/18 *Data Protection Commissioner v Schrems, Facebook Ireland Ltd*, [2020] ECHR at para 63 [*Schrems II*].

[13] *Schrems II* at paras 180-182.

[14] See https://ised-isde.canada.ca/site/plans-reports/en/sixth-update-report-developments-data-protection-law-canada.

- I'm curious to see how and when SARP is challenged. These are not tested mechanisms.

5. Under C-26, could individuals be arrested if the companies they work for are victimized by a cyber incident?

Part I: Telecommunications Act Amendments

• Employees of telecommunications companies cannot be arrested under C-26 simply because a cyber incident occurs.

• Rather, individuals may face charges if they contravene certain orders or regulations under sections 15.1, 15.2, or paragraph 15.8(1)(a), meaning they refused to act despite being directed to do so.

• Individuals would not be convicted if they demonstrate that they exercised all due diligence to prevent the offence from occurring.

• In most cases, the Crown would likely focus on management if higher-level officials are believed to have directed that a government order not be implemented.

Part 2: Critical Cyber Systems Protection Act

• Employees of designated operators cannot be arrested under C-26 simply because a cyber incident occurs.

• Part 2 of Bill C-26 is intended to ensure that designated operators take steps to prevent cyber incidents from occurring and be prepared to mitigate and recover from cyber incidents that do occur. It only holds designated operators accountable for actions that are within their control.

• Individuals found to be in contravention of the Act for actions such as sharing confidential information or failing to implement a Cyber Security Direction would be subject to penalties.

• As with Part 1 of the Act, designated operators and individuals could rely on a due diligence defence.

6. What penalties are applicable under similar laws in other Five Eyes countries?

United States

• The United States has begun consultations on the Cybersecurity Incident Reporting for Critical Infrastructure Act. Penalties for non-compliance include significant fines and imprisonment for terms of up to five years.

• The Federal Communications Commission has broad authority to fine telecommunications companies for failing to implement sufficient cyber security measures. Notable examples include a US$350 million (C$485m) fine in August 2021 to T-Mobile.

United Kingdom

• The UK's Telecommunications (Security) Act 2021 is broadly similar to Bill C-26.

• It requires telecommunications service providers to have measures in place to identify and defend their networks from cyber threats. Swift action must be taken after a security compromise in order to limit, remedy, and mitigate the damage. If a provider does not comply with their security duties, they can be fined up to a maximum of ten percent of their revenue. In a Canadian context, that would be a fine of C$2.5 billion to Bell and C$1.9 billion to Rogers.

Australia

• Under Australia's Security of Critical Infrastructure Act, an entity responsible for a system of national significance can face a maximum fine of AUD 3.13 million if it fails to have an incident response plan for cybersecurity incidents.

EU

• Under the European Union's NIS-2 Directive, which takes effect in January 2025, fines for failure to implement a security plan are set at two percent of annual worldwide revenue or €10m, whichever is greater. In a Canadian context, that would allow fines of C$500m against Bell, or C$386m against Rogers.

- This is what we should following. The size-cap approach would be much more effective for compliance.

• Punitive measures are also available against executives, including forced removal from executive board positions.

- Worth retaining when we think about Solar Winds.

• The EU General Data Protection Regulation (GDPR) has also been used to fine organizations for lax cyber security practices. Meta/Facebook was fined US$1.3 billion in 2023, and Amazon was fined US$877 million in 2021.

7. Does Canada have other laws that allow for fines similar to those set out in Bill C-26?

• The fines allowed for by Bill C-26 are comparable to those set out in other legislation internationally and domestically.

• As noted above, comparable regimes in other countries allow for penalties in the hundreds of millions of dollars.

• In Canada, the Competition Act allows for penalties of up to 3% of global annual revenue and 14 years in prison. The Consumer Privacy Protection Act (CPPA) that would be created by Bill C-27 allows fines of up to $25 million or 5% of global revenue.

• Without the possibility of maximum penalties that will matter to companies with tens of billions of dollars in annual revenue, there is a substantial risk that some companies would not take compliance seriously.

8. Why did the House remove an amendment made at committee that sought to limit the period for which information could be retained?

• The House Public Safety Committee initially amended Part 2 of Bill C-26 such that information exchanged between government entities under s. 23 could be retained "only for as long as is necessary to make, amend or revoke an order under section 20, or to verify compliance or prevent non-compliance with such an order."

• That amendment was subsequently removed by the House at Report Stage.

• This requirement to destroy information immediately after using it could have created a conflict with s. 6 of the Privacy Act, which requires that personal information be retained for a period after its use "in order to ensure that the individual to whom it relates has a reasonable opportunity to obtain access to the information."