Bill C-2 Backgrounder: New Search Powers in the Strong Borders Act and Their Charter Compliance

Robert Diab, Faculty of Law, Thompson Rivers University | September 2025

Criminal Law Quarterly, Vol 73(3) 2025

Abstract:

Bill C-2, tabled in June of 2025, will bring about the most significant expansion of investigative search powers in Canada in over a decade, along with a long sought after lawful access regime for compelling assistance from electronic service providers. This article provides a concise overview of these powers, places them in context by noting how they expand or amend existing authority, and comments on their constitutional validity. Powers in Bill C-2 are canvassed here in three groups: those relating cross-border traffic, domestic investigations, and technical assistance with access to data.

Introduction

The Liberal government's first substantive bill, C-2, tabled on June 5, 2025, contains the most significant expansion of investigative search powers in Canada in over a decade, along with a lawful access regime for compelling assistance from electronic service providers.[1] This article provides a concise overview of these powers, places them in context by noting how they expand or amend existing authority, and comments on their constitutional validity. Powers in the bill are canvassed here in three groups: those relating cross-border traffic, domestic investigations, and technical assistance with access to data.

The first part of this paper discusses changes in the areas relating to customs and immigration enforcement, coastal patrol, Canada Post, financial crimes, and the sex offender registry. The second part considers the bill's introduction of new 'information demand' and production order powers, along with amendments to computer search warrants, exigent search provisions, foreign entity requests and mutual legal assistance. It sheds light on the meaning of new declaratory and indemnification provisions that are brief but complex in application. The third part places the proposed *Supporting Authorized Access to Information Act* in Part 14 of the bill in the context of comparable legislation in other Five-Eye nations, and surveys its powers to compel technical assistance, its confidentiality provisions, and its inspection powers.

Bill C-2 will likely be revised before it is passed, or it may not be passed at all. There is, however, a good chance at this point that the bill will pass in substantially the same form as currently tabled—or that Parliament will attempt to pass some if not most of these powers in the near future.

To lend context to what follows, I note that the investigative powers in the bill engage a host of rights under the *Canadian Charter of Rights and Freedoms*,[2] including under sections 7, 8, 11(c), and 13. The focus in this article is on the constitutionality of the bill's investigative powers under section 8 of the *Charter*, guaranteeing "[e]veryone has the right to be secure against unreasonable search or seizure." A reasonable search under section 8 is one that is authorized by a reasonable law and carried out reasonably.[3] One question arising under the bill is whether a new power authorizes what amounts to a search or seizure under section 8. The test for this is whether a power authorizes a

---

[1] 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 (first reading) [Bill C-2].

[2] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (UK), 1982, c 11 [*Charter*].

[3] *R v Collins*, [1987] 1 SCR 26, p. 278.

state agent, acting for an investigative purpose, to do something that interferes with a reasonable expectation of privacy a person has over a place or thing.[4]

The main question throughout this article, however, will be whether new laws in Bill C-2 that do authorize a search or seizure under section 8 are likely to be upheld as a "reasonable law." Courts assess this by asking whether a power strikes an appropriate balance between law enforcement and privacy interests at issue. To keep this overview concise, I will not explore the balance question for each power discussed here in detail. But the reader might keep in mind that the Supreme Court of Canada has considered four factors in assessing this: whether the power relates to a criminal or regulatory offence; the state or law enforcement interest at issue; the impact on personal privacy; and the oversight and accountability safeguards.[5]

Part 1: Powers related to cross-border traffic

Customs Act

Part 1 of the bill amends the *Customs Act* to expand inspection powers in relation to goods being exported. Currently, the Act requires that "all goods that are exported" be reported to officers of the Canada Border Services Agency (CBSA), with certain exceptions.[6] CBSA officers can also "examine any goods that are to be exported" and may, without grounds, open containers or packages to do so.[7] Bill C-2 would add new sections to the *Customs Act* that would compel warehouse operators and "every person who transports" goods to give CBSA "free access to… any goods destined for export" that are loaded or stored in a place and, without grounds, "open any package or container".[8]

The *Customs Act* defines "goods" to include "any document in any form," which courts have interpreted to include data on a phone or laptop.[9] But the wording of the new provisions would not provide CBSA power to search devices a person may carry on departure since goods stored on a

---

[4] *R v Bykovets*, 2024 SCC 6 at para 31, *R v Evans*, [1996] 1 SCR 8 at para 11.

[5] See *Goodwin v British Columbia (Superintendent of Motor Vehicles)*, 2015 SCC 46 at para 57 [*Goodwin*], and the considerations set out in the dissenting reasons of Strayer J in *Del Zotto v Canada*, [1997] 3 FC 40 (CA) [Del Zotto FC], adopted in *Del Zotto v Canada* [1999] 1 SCR 3. See also Robert Diab & Chris D.L. Hunt, *Search and Seizure* (Toronto: Irwin Law, 2023), chapter 7.

[6] *Customs Act*, RSC 1985, c 1 (2nd Supp), s 99, s 95(1) and (1.1) [*Customs Act*].

[7] *Ibid*, s 99(1)(c).

[8] Bill C-2, s 4, adding new ss 97.01 and 97.02 to the *Customs Act*.

[9] *R v Whittaker*, 2010 NBPC 32; *R v Moroz*, 2012 ONSC 5642 at para 20; *R v Saikaley*, 2012 ONSC 6794 at para 82; *R v Buss*, 2014 BCPC 16 at paras 25–32; *R v Gibson*, 2017 BCPC 237 at para 201; *R v Singh*, 2019 OCJ 453 at paras 64-65.

device would not be "goods destined for export".[10] This can be inferred from the different phrasing used in the existing section 99(1)(c) and the proposed export inspection powers. The former speak of "goods to be exported"; the latter "goods destined for export… loaded…or stored" or in a "warehouse." Notably, the government has not taken the opportunity in Bill C-2 to amend section 99(1) in response to appellate decisions finding the use of this provision for device search at the border on no grounds to be unreasonable.[11]

Are the new powers that authorize CBSA to gain "free access" to places where items "destined for export" are held—a transport truck or warehouse—and to "open any package or container" unreasonable under section 8 of the *Charter*? Probably not. They constitute a search because the inspection of items at issue may interfere with a reasonable privacy interest. But the Supreme Court of Canada in *Simmons*,[12] a case involving a strip search of a suspected drug importer, held the state interest in search at the border to be high and a person's privacy interest to be low.[13] Relying on *Simmons*, courts have found reasonable under section 8 searches conducted by CBSA officers under *Customs Act* powers to open packages and examine goods on no grounds—even where they resulted in charges under the *Criminal Code* and the *Controlled Drugs and Substances Act*.[14] The new powers here are analogous.

Immigration and citizenship information sharing

Part 6 of the Bill C-2 would amend the *Department of Citizenship and Immigration Act* (*DCIA*) and *Immigration and Refugee Protection Act* to allow officials under each act to share information about a person's immigration or citizenship status to (in the case of *DCIA* powers) other agencies of the federal or provincial governments (and, in the case of *IRPA*, to other federal agencies) for the purpose of enforcing law in the jurisdiction at issue.[15] This can include the content of a document issued to a person.[16] Some of this information might attract a privacy interest, such as addresses, or

---

[10] Bill C-2, s 4, adding new ss 97.01 to the *Customs Act*.

[11] *R v Pike*, 2024 ONCA 608; *R v Canfield*, 2020 ABCA 383.

[12] *R v Simmons*, [1988] 2 SCR 495 at para 49 [*Simmons*].

[13] *Ibid* at para 49.

[14] See the application of s 99(1)(a) of the *Customs Act* in *R v Lapple*, 2016 ONCA 289; *R v Sekhon*, 2009 BCCA 187; and *R v McKay*, 1992 CanLII 6192 (AB KB); *Criminal Code*, RSC 1985, c C-46 [*Criminal Code* or *Code*] and the *Controlled Drugs and Substances Act*, SC 1996, c 19.

[15] Bill C-2, s 33, adding new ss 5.2-5.7 to the *Department of Citizenship and Immigration Act*, SC 1994, c 31 [*DCIA*], and Bill C-2, s 36 adding a new s 6.1(1) to the *Immigration and Refugee Protection Act*, SC 2001, c 27, s 3 [*IRPA*].

[16] Bill C-2, s 33, the proposed s. 5.5(1)(c) to the *DCIA.*

reasons for entry or refusal of a visa. The provisions thus allow for private information to be shared without grounds.

However, they do not violate section 8 of the *Charter* because the form in which information sharing would unfold here does not constitute a search or seizure under section 8. The provisions authorize ministry disclosure of information—with a host of safeguards, including conditions limiting use by the recipient—but they do not authorize a *demand* for disclosure, which would constitute a search or seizure under section 8.[17] In *R v Spencer*,[18] the Supreme Court of Canada applied this analysis to the Crown's attempt to rely on a provision that authorized disclosure to police in the *Personal Information Protection and Electronic Documents Act*, declining to find that it authorized a police demand for the subscriber information at issue, which did constitute a search.[19]

A point worth clarifying about the information sharing provisions in Bill C-2 (there are more below) is why disclosure in itself does not constitute a search or seizure under section 8. Police conduct a search or a seizure when they examine or take something over which a person has a reasonable privacy interest and they do so for an investigative purpose.[20] Where a state actor, without having been asked, provides law enforcement with incriminating evidence (a blood sample, a computer) that engages a privacy interest, the Supreme Court of Canada has held that police receipt of it can constitute a search or seizure.[21] And for this, law enforcement receiving the evidence would need authority to render its reception (for an investigative purpose) reasonable under section 8. The Supreme Court has not, however, rendered a majority decision in a case involving state agents sharing private information to facilitate an investigation.[22] But arguably, once police begin examining the information or decide to keep hold of it for an investigative purpose, they engage

---

[17] Conditions are to be imposed in Bill C-2, s 33, in the new ss. 5.5 to 5.7 of the *DCIA*.

[18] 2010 SCC 43 [*Spencer*].

[19] Section 7(3)(c.1) of the *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5 (*PIPEDA*), permitting disclosure without consent to a government agency where it has identified its lawful authority to obtain the information.

[20] As Cromwell J put it in *Spencer*, *supra* note 21 at para 67, "Where a police officer requests disclosure of information relating to a suspect from a third party, whether there is a search depends on whether, in light of the totality of the circumstances, the suspect has a reasonable expectation of privacy in that information".

[21] *R v Dyment*, [1988] 2 SCR 417 [*Dyment*]; *R v Colarusso*, [1994] 1 SCR 20 [*Colarusso*]; *R v Cole*, 2012 SCC 53 [*Cole*].

[22] In *Wakeling v United States of America*, 2014 SCC 72, 3 of 7 judges held that s 193(2)(e) of the *Criminal Code*, allowing for information obtained from a wiretap to be shared with US law enforcement, constituted a reasonable law since it included reasonable measures for the continuing seizure of private information. In *Quebec (Attorney General) v. Laroche*, 2002 SCC 72, provincial vehicle inspectors turned over to police information about cars at a dealership, but the entire Court held this not to be private information.

section 8 and require authority.[23] These new disclosure provisions do not authorize a search or seizure.

Canada Post Corporation Act

Currently mail can be searched or seized under the *Canada Post Corporation Act* pursuant to powers in the Act,[24] the *Canadian Security Intelligence Service Act*,[25] the *Customs Act*,[26] and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*.[27] The bill would amend the *CPCA* to allow search and seizure of mail under any act of Parliament, which would include the *Criminal Code* powers to search with a warrant or in exigent circumstances.[28] The bill would also amend the corporation's power to open mail under the current section 41(1) of the *CPCA*.[29] Currently that section allows officials to open mail, other than letter mail, on reasonable suspicion that mail is "non-mailable matter" (which includes "any item transmitted by post in contravention of an Act or regulation of Canada").[30] The new provision would allow for opening letter mail on the same grounds.

Section 41(1) was amended in 2023 to include the requirement for reasonable suspicion before opening non-letter mail in response to the holding in *R v Gorman*,[31] which held the provision to violate section 8 without this. The new power—expanding search on reasonable suspicion of 'non-mailable matter' to letter mail—raises the question of whether this measure strikes a reasonable balance between the greater privacy interest in letter mail and law enforcement or public safety interests in warrantless access. Should it be necessary that officials think a piece of mail probably contains contraband rather than only possibly containing it? Does a reasonable possibility that a letter contains a substance that might seriously harm postal officials change the equation? And would a court necessarily agree that the privacy interest in letter mail today remains high? These will be the questions if and when the provision is challenged in a criminal case.

---

[23] This would follow from principles set out in *Dyment*, *Colarusso*, and *Cole*, *supra* note 24, and the way the Supreme Court has defined what constitutes a search or seizure, also canvassed in these cases.

[24] *Canada Post Corporation Act*, RSC 1985, c C-10, s 41 [*CPCA*].

[25] *Canadian Security Intelligence Service Act*, RSC 1985, c C-23 [*CSIS Act*].

[26] *Supra* note 6.

[27] *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 [*PCMLTFA*].

[28] *Code*, *supra* note 14, ss 487 and 489.

[29] Bill C-2, s 27, proposing a change to s 41(1) of the *CPCA*, *supra* note 27.

[30] Section s 41(1) of the *CPCA*, *supra* note 27, and s. 4(d) of the *Non-mailable Matter Regulations*, SOR/90-10.

[31] 2022 NLSC 3.

Oceans Act

Bill C-2 would amend the *Oceans Act* to expand the coast guard's mandate to include conducting "security patrols" and the "the collection, analysis and disclosure of information or intelligence."[32] The government's *Charter* statement on the bill suggests that the powers to gather or disclose information here could engage privacy interests under section 8 but would be limited to the purposes of the Act, which pertain primarily to "the safe movement of ships in Canadian waters and marine pollution response".[33] Suffice it to note that the disclosure powers here do not create authority to search under section 8. If police or another agency investigating an offence were to ask the coast guard to disclose information that engages a privacy interest, for the reasons noted above (canvassed in *Spencer*), the demand would constitute a search and the disclosure power here would not authorize that demand.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act

Part 10 of Bill C-2 would make various changes to the *PCMLTFA*, including one that would oblige the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to disclose information to the Commissioner of Canada Elections, on a reasonable suspicion that the information would be relevant to an investigation of an offence or violation under the *Canada Elections Act.*[34] The disclosure here would neither constitute a search nor authorize one, for reasons noted above. The requirement for reasonable suspicion here is a measure intended to protect private information held under the *PCMLTFA* akin to a condition on the use of information disclosed under some of the other disclosure provisions in C-2.

Sex Offender Information Registration Act

The amendments to the *SOIRA* regime in Part 13 of Bill C-2 are so extensive as to merit an entire article in itself. Briefly, the bill will expand powers of the Royal Canadian Mounted Police to share information with foreign and domestic agencies by reducing the threshold from it being "necessary" to do so to there being "reasonable grounds to believe it would assist" in investigating or preventing

---

[32] Bill C-2, s 30(2), amending s 41(2) of the *Oceans Act*, SC 1996, c 31, s 35.

[33] Canada, Department of Justice, "Charter Statement – 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" (19 June 2025), online: Department of Justice https://www.justice.gc.ca/eng/csj-sjc/pl/charter-charte/c2_2.html..

[34] Bill C-2, ss 94 and 95, amending ss 55(3) and 55.1(1) of the *Canada Elections Act*, SC 2000, c 9, cite. I omit discussion of new powers in s 62 of Bill C-2 for inspections on probable grounds to enforce compliance with the *PCMLTFA*'s new reporting requirements; these contemplate standard grounds for regulatory searches, including the requirement for a warrant if the inspection involves a dwelling house.

a sex offence.[35] *SOIRA* currently has provisions that compel an offender to be photographed and to have their identifying physical characteristics noted; the bill would clarify that this includes a power to record "any tattoos or distinguishing marks".[36] It would shorten the time-frame that offenders must report changes to their vehicle information, from a year to a number of days.[37] It would permit CBSA agents to disclose more specific travel details about offenders to other law enforcement (than currently under *SOIRA*), including documents used; date, time, and place of destination and arrival; along with flight numbers.[38] And the bill would authorize CBSA agents to consult the *SOIRA* database to gather information to assist in fulfilling their duties under law.[39]

The new information sharing provisions would not constitute authority for a search or seizure under section 8, for reasons canvassed above (about sharing provisions generally). The new information collection powers, however, would appear to authorize a search since they allow private information to be collected for an investigative purpose. Yet soon after *SOIRA* was enacted, at least one court in Canada undertook a careful consideration of whether its existing powers to collect information about offenders authorized a form of search and were thus reasonable search laws.[40] The court found that they did not constitute a search, since sex offenders do not have a reasonable privacy interest in the information at issue. The court arrived at this conclusion by considering the collection powers in *SOIRA* to be closely analogous to those in the DNA provisions of the *Criminal Code* and by relying on the Supreme Court of Canada's assessment of them in *R v Rodgers*.[41] In *Rodgers*, the Court held that offenders have no privacy interest in their DNA being sampled in the same way that offenders have no privacy over their fingerprints or photographs being taken under the *Identification of Criminals Act*.[42]

Given the close parallels between *SOIRA*'s collection powers and the DNA *Code* provisions—in terms of purpose and function—and the holding in *Rodgers*, new collection powers added to *SOIRA* in Bill C-2 are not likely to offend section 8 of the *Charter.*

---

[35] Bill C-2, s 151, amending s 16(4)(c) of the *Sex Offender Information Registration Act*, SC 2004, c 10 [*SOIRA*].

[36] Bill C-2, s 148, amending s 5(3) of *SOIRA*.

[37] Bill C-2, s 147, amending s 4.1(1) of *SOIRA*.

[38] Bill C-2, s 150, adding a new s 15.3 to *SOIRA*; current disclosure powers of CBSA agents are in the existing s 15.2 of *SOIRA.*

[39] Bill C-2, s 151, adding a new s 16(2)(c.1) to *SOIRA*.

[40] *P.S.C. v. British Columbia (Attorney General)*, 2007 BCSC 895.

[41] *Ibid* at paras 139-147, citing *Rodgers*, 2006 SCC 15 [*Rodgers*].

[42] *Rodgers*, *ibid* at para 43; *Identification of Criminals Act*, RSC 1985, c I-1.

Part 2: Domestic investigative powers

Computer searches

Part 14 of Bill C-2 makes various amendments to the *Criminal Code*, beginning with slight changes to warrant provisions in section 487. These are mostly cosmetic, making the computer search provisions more reader friendly, but they include three notable changes. A new section 487(2.4) allows for a warrant to search "computer data" on a "computer system" that is "in the possession of" police on reasonable grounds—something for which police currently seek an additional 487 warrant (if they come into possession of a computer pursuant to a warrant under 487 that did not specify they could search a computer found in a place).[43] Section 487(2.5) to be added would allow a judge to impose a limit on the examination of computer data under this new warrant to a stipulated class of data, and for this to be done by "a person whose only role in the investigation of the commission of the offence set out in the warrant is to extract computer data." A further provision would compel the person conducting the data extraction not to share with other investigating officers data falling outside of the stipulated class of searchable data.[44] Judges have long been in a position to include these conditions in a warrant, but will likely do so with more frequency given their codification.

Information demand

Among the most controversial new powers in Bill C-2 is the proposed 'information demand' power to be added to the *Code* in a new section 487.0121.[45] This would allow police to make a written demand to "a person who provides services to the public" to indicate whether they have "provided services" to a "subscriber or client," or an "account or other identifier"—and if so, whether they have "transmission data" in relation to that person (all 'yes or no' questions); the province and municipality in Canada where they provided service or the country and municipality outside of Canada where they did so; and the time period in which they provided services or, if they still do, when they began to do so.[46] The provision also allows police to demand whether a provider knows of "any other person who provides services to the public and who provides or has provided services" to the target.[47] To make a demand under this section, police need only "reasonable grounds to suspect"

---

[43] Bill C-2, s 156, amending s 487 of the *Code* by adding s 487(2.4).

[44] Bill C-2, s 156, adding the *Code* a new s 487(2.6).

[45] Bill C-2, s 158.

[46] *Ibid*, to become s 487.0121(1)(a) to (d) of the *Code*.

[47] *Ibid*, s 487.0121(1)(e).

that a federal offence has been or will be committed and that the information "will assist in the investigation of the offence."[48] The timing to comply with a demand can be as little as 24 hours, and police may not make a demand to a person under investigation for the offence at issue.[49]

Early assessments of the provision raise several concerns. It allows police to gain too much private information on grounds that are too low: without a warrant, on reasonable suspicion alone. It allows police to impose a confidentiality condition lasting up to a year.[50] A person to whom a demand is made may seek review of it before a judge but has only five days to file an application to do so and must give notice to the officer involved.[51] A judge may then revoke or vary the demand if it is "unreasonable in the circumstances" or would "disclose information that is privileged or otherwise protected from disclosure by law."[52] But the bill places the onus on the recipient of a demand to act quickly to avoid a potential penalty of a summary conviction and a fine of up to $5,000.[53]

The bill adds substantially the same 'information demand' power to the *Canadian Security Intelligence Service Act*,[54] with similar provisions to challenge it.[55] But there are two important differences. Unlike the new demand power to be added to the *Criminal Code*, which requires police to have reasonable suspicion of an offence, CSIS agents can make an 'information demand' without grounds. And CSIS can only make the demand "[f]or the purpose of performing its duties and functions under section 12 or 16".[56] Section 12 permits the Service to collect information "to the extent that is strictly necessary" relating to "activities that may on reasonable grounds be suspected of constituting threats to the security of Canada". Section 16 authorizes the Service to collect information relating to the "defence of Canada or the conduct of the international affairs of Canada" involving "any person other than" a Canadian citizen, permanent resident, or a company incorporated in Canada. This would appear to limit CSIS to making an 'information demand' of only

---

[48] *Ibid*, s 487.0121(2).

[49] *Ibid*, ss 487.0121(4) and 487.0121(3).

[50] *Ibid*, s 487.0121(5).

[51] *Ibid*, s 487.0121(7).

[52] *Ibid*, s 487.0121(10).

[53] Bill C-2, s 165, amending *Code* s 487.0197.

[54] Bill C-2, s 185, adding a new s 20.21 to the *CSIS Act*, *supra* note 28.

[55] Bill C-2, s 185, adding a new s 20.22 to the *CSIS Act*, *supra* note 28.

[56] Bill C-2, s 185, opening phrase of the proposed s 20.21(1) of the *CSIS Act*, *supra* note 28.

a narrow class of targets. But at the time they make the demand—having only an Internet Protocol address or account name—how will they know if the target is not a citizen or permanent resident?

Production order for subscriber information

Bill C-2 also introduces a new production order specifically for subscriber information attaching to an account for services. Currently, police seek this using the 'general production order' in section 487.014 of the *Code* on reasonable grounds to believe a federal offence has been or will be committed and that a "document or data" in a person's possession will afford evidence of the offence. The bill would add a new section 487.0142, which would allow police to obtain an order for "all subscriber information" on reasonable suspicion, and also adds to the *Code* a definition of "subscriber information" that is expansive.[57] It goes beyond the name and address attached to an account to include "types of services provided," devices used, and other billing information—and it applies not only to providers of an electronic service but to "any client of a person who provides services to the public".

The Supreme Court in *Spencer* affirmed that a demand for and seizure of subscriber information engages significant interests in privacy and anonymity, but did not rule on what would constitute a reasonable law to authorize this.[58] A majority of the Court in *Bykovets* suggested that using a production order (for transmission data) on reasonable suspicion offered police a viable and reasonable means of obtaining an Internet Protocol address.[59] Since an IP address attracts a lesser privacy interest than subscriber information (because further steps must be taken to link an IP address to a person), one might infer that the Court will be inclined to find reasonable suspicion for subscriber information too low a standard to make for a reasonable law under section 8. However, the Court in *Bykovets* was divided 5-4 on *whether* an IP address attracts a reasonable privacy interest at all. A slim majority may well find that a production order for subscriber information on reasonable suspicion is reasonable.

A further concern courts will consider here in deciding the reasonableness of this new power is whether it contains further effective safeguards in addition to a warrant requirement. The bill shortens the time limit for a recipient to seek review of a production order (*i.e.*, for subscriber

---

[57] Bill C-2, s 159 and 157(1) respectively, adding to the *Code* a new s 487.0142 and definition of subscriber information to s 487.011. See also Bill C-2, s 174, adding to the *Code* a new s 492.2(5.2), which allows a judge issuing a warrant for transmission data (under s 492.2(1), on reasonable suspicion) to also obtain from the person—if they provide services to the public—subscriber information relating to the transmission data.

[58] *Spencer*, *supra* note 21 at paras 22-67 and paras 73-74.

[59] *R v Bykovets*, 2024 SCC 6 at para 85 [*Bykovets*].

information, but also for other production orders in the *Code*) from 30 days to 5 days.[60] Here too, the recipient of the order must give notice to the officer named in the order.[61] One might argue that in practical terms, this review mechanism will often not provide an effective further safeguard against improper searches, leaving the only real safeguard here to be a judge's assessment of reasonable suspicion.

Request of a foreign entity

Bill C-2 would add a new section allowing a peace or public officer to ask a judge to authorize them to make a "request to a foreign entity that provides telecommunication services" to produce a document with transmission data or subscriber information in their possession or control.[62] The officer must establish a reasonable suspicion that a federal offence has been or will be committed and the evidence at issue will assist in the investigation. If granted, the officer has 30 days to make the request.

This new 'foreign entity request' power is a response to concerns raised about the British Columbia Court of Appeal's 2018 decision in *Brecknell*.[63] The court in that case overturned lower court rulings which held that police lacked jurisdiction to make a demand of Craigslist in California to disclose transmission data on the basis that the *Criminal Code*'s production order provisions had no extra-territorial effect. The Court of Appeal's decision was criticized as erroneous in the absence of a clear indication in the *Code* that Parliament intended such an effect.[64] The new foreign entity request power addresses this concern by making clear an intention that police can act beyond Canada's border in seeking this kind of evidence, and it finesses issues of comity and respect for foreign sovereignty by framing the power here not as an "order" but as a "request."

Tracking and transmission data powers

The *Criminal Code* currently allows police to seek warrants to track a person's location.[65] The standard required depends on whether police seek to track something "usually worn by the individual" or a thing such as a vehicle. Tracking a device worn requires reasonable belief that

---

[60] Bill C-2, s 163, amending s 487.0193(1) and (2) of the *Code.*

[61] *Ibid*, s 487.0193(2).

[62] Bill C-2, s 160, adding to the *Code* s 487.0181. The term 'peace officer' is presently defined in section 2 of the *Code*. The bill will move (but not change) the definition of 'public officer' out of the warrant provisions of the *Code*, where it is currently defined, and place it in section 2.

[63] *British Columbia (Attorney General) v. Brecknell*, 2018 BCCA 5.

[64] David Fraser, "Case Comment: *British Columbia (Attorney General) v Brecknell*" 18 Can. J. L. & Tech. 135.

[65] *Code*, s 492.1.

tracking would assist in an investigation; tracking a vehicle or other thing requires reasonable suspicion.[66] A new provision states that where a judge authorizes a tracking warrant for a device a person usually wears, they can also stipulate that police may track the location of "any similar thing that is unknown at the time the warrant is issued" on a reasonable suspicion that the person might "use, carry or wear that similar thing."[67] The key requirement here is that a judge has already decided there are probable grounds to believe that a tracking warrant for personal movement would assist in the investigation. The effect of the extension here is slight and likely to be found reasonable.

The *Code* currently contains an analogous provision for obtaining a warrant for transmission data on reasonable suspicion.[68] The Bill amends this to allow a judge to include a condition permitting seizure of transmission data involving "any means of telecommunication that is unknown at the time the warrant is issued but that is of a similar type" as that set out in the warrant—on reasonable suspicion the person might use this other means of communication.[69] This is not likely to be challenged given that the same standard is required for the warrant itself (and courts have found that standard reasonable given the lower privacy interest in transmission data itself).[70]

Declaratory and indemnity provisions

The *Criminal Code* currently includes a provision stating that "[f]or greater certainty," police do not need a production order or other authorization to "ask a person to… voluntarily provide a document to the officer that the person is not prohibited by law from disclosing."[71] Bill C-2 adds another declaratory provision that makes a similar assertion about police not needing authority to ask a person to voluntarily provide "information" within the ambit of the new 'information demand' power.[72] And the bill adds a further provision stating that police do not need authority to "receive any information… and to act" on it, if a person volunteers it to police without being asked.[73]

---

[66] *Ibid*, s 492.1(1).

[67] Bill C-2, s 173, adding to the *Code* a new s 492.1(2.1).

[68] *Code*, s 492.2(1).

[69] Bill C-2, s 174, adding to the *Code* a new s 492.2(1.1).

[70] *R v Mahmood*, 2011 ONCA 693 at paras 96-98; and *R. v Nicholson*, 2015 BCSC 2429 at para 41.

[71] *Code*, s 487.0195(1).

[72] Bill C-2, s 164, adding to the *Code* a new 478.0195(1.1), (3), and (4).

[73] *Ibid*, s 478.0195(3)

Notably, these new declaratory provisions refer not to a document that a person is "not prohibited by law from disclosing" but instead to "information" the person "is lawfully in possession of".[74]

A plain reading of these new provisions might lead one to interpret them to mean: police do not need to make a formal 'information demand' to ask Shaw or Telus for details about a person's account if those companies are willing to provide it voluntarily. Nor do they need authority to receive and examine a document containing private data—subscriber information or even an email or a chat—if they did not ask for it. With respect to section 8 of the *Charter*, the first proposition is incorrect; the second is unclear at this time.

The Supreme Court of Canada in *Spencer* considered an earlier version of the declaratory provision that is currently in the *Code* (stating that police do not need a production order or other authorization to "ask a person to… voluntarily provide a document").[75] Justice Cromwell, for the Court, rejected the Crown's attempt to rely on it as authority for police to request subscriber information about a suspect from Shaw, or as a provision that made it unnecessary for police to have authority in law to make a request.[76] Put another way, this provision did not create a new search power or determine whether a police request for subscriber information constituted a search.[77] That turns strictly on whether what police are asking for is private. And a declaratory provision could not decide that question. The Court held that subscriber information is private; asking for it constitutes a search under section 8; and therefore, police need authority in law to ask for it. The current section 487.0195(1)—stating that police do not need a production order to "ask a person to… voluntarily provide a document"—is not true *if the document contains private information.* That is the thrust of *Spencer.* The same qualification would apply to the new declaratory provision pertaining to information within the ambit of an 'information demand.'[78] It is not true that "no information demand is necessary" for police to ask for it if the information engages a reasonable privacy interest under section 8 of the *Charter*. Asking for it would constitute a search without lawful authority.

The assertion in the other new declaratory provision in the bill pertaining to police *receipt* of information falls into a legal grey area at present. As noted earlier, the Supreme Court of Canada has held that police conduct a search or seizure under section 8 when a state agent provides police with evidence that engages a reasonable privacy interest and police receive it for an investigative

---

[74] *Ibid*, ss 487.0195(1.1) and (3).

[75] *Spencer*, *supra* note 28, at paras 69-73, considering an earlier version of what is now s 487.0195(1) of the Code.

[76] *Spencer*, *supra* note 28 at para 73.

[77] *Ibid.*

[78] Bill C-2, s 164, adding to the *Code* s 478.0195(1.1).

purpose.[79] The Supreme Court has considered the possibility that police also conduct a search or seizure when they receive from a civilian evidence engaging a suspect's privacy interest.[80] The new declaratory provision here asserts that no order, warrant, or information demand is necessary to receive and act on information voluntarily provided.[81] At present, this is only indisputably correct in certain cases.

If a person communicated private *information* about a suspect to police—without police having asked—this would not constitute a search or seizure, since in this case, the person is merely sharing their *knowledge* of private details. But if they provide a *document*, such as the copy of a chat, an email, or photo that engages a suspect's privacy interest, police receipt and examination of it may constitute a search or seizure (because police are receiving it for an investigative purpose and the thing itself engages a suspect's privacy).[82] This new declaratory provision is thus true for the disclosure of *some* information, but for a document engaging a privacy interest, police would arguably need authority.

The two new declaratory provisions point to a further point of potential confusion. What is the practical import of the use of different phrasing here ("a document …that the person is not prohibited by law from disclosing" in contrast to "information" the person is "in lawful possession of")? It relates to an amendment that Bill C-2 will make to the indemnity provision in the current section 487.0195(2).

As noted above, Bill C-2 does not remove or amend the existing declaratory provision, section 487.0195(1); the new declaratory provisions address only information within the ambit of the new 'information demand' and police receipt of information voluntarily disclosed. The current indemnity provision in 487.0195(2) shields a person from civil or criminal liability for voluntarily providing a "document" to police, when asked, if they were "not prohibited by law from disclosing" it. One prohibition can be found in *PIPEDA*, which prohibits companies like Shaw or Telus from disclosing private customer information to law enforcement when asked, unless police have a warrant or lawful authority to ask for it.[83] (By contrast, in British Columbia, Alberta, and Quebec,

---

[79] *Dyment*, *Colarusso*, and *Cole*, *supra* note 24.

[80] *R v Marakah*, 2017 SCC 59 at para 50.

[81] Bill C-2, s 164, adding to the *Code* s 478.0195(3).

[82] Robert Diab, "'Must the Police Refuse to Look?' Resolving the Emerging Conflict in Search and Seizure Over Civilian Disclosure of Digital Evidence" (2023) 68:4 McGill Law Journal 369.

[83] *PIPEDA*, *supra* note 22, ss 7(3)(c) and (c.1).

provincial privacy law permits a party to disclose private customer information on a mere request from law enforcement.[84])

The bill amends section 487.0195(2) to also indemnify a person for voluntary disclosures of "information" within the ambit of an 'information demand' in the "circumstances" set out in the new declaratory provision about this, which refers to information a person lawfully possesses.[85] The revised indemnity provision thus contemplates a scenario where police ask for information without making a formal 'information demand'; Shaw or Telus disclose it; it happens to be private information under *PIPEDA*; the voluntary disclosure is prohibited under the Act, since police asked for it without lawful authority (i.e., a formal demand)—and Shaw or Telus are indemnified for violating the Act. What incentive, some have asked, do Shaw or Telus have to insist that police make a formal demand?

Shaw or Telus may have no incentive to insist on a formal demand, but police have an incentive under the *Charter*. If police ask Shaw or Telus for information that engages a reasonable privacy interest under section 8, the new indemnity provision might shield the company from liability for the disclosure, but the police request would constitute a search without authority and thus an unreasonable search, possibly resulting in the exclusion of evidence.

Exigent circumstances

Bill C-2 would amend the existing provision in the *Code* authorizing search without a warrant in exigent circumstances to allow for seizure of subscriber information, transmission, or tracking data without a production order.[86] But the requirement here is the same: police are authorized to carry out these warrantless seizures "if the conditions for obtaining an order exist but by reason of exigent circumstances it would be impracticable to obtain an order." This amendment merely codifies a power police had at common law to make a warrantless seizure for the same information in exigent circumstances.[87]

---

[84] *Personal Information Protection Act*, SBC 2003, c 63., s 18(1)(j); *Personal Information Protection Act*, SA 2003, c P-6.5., s 20(f); *Act respecting the protection of personal information in the private sector,* CQLR, c P-39.1, s 18(3). Section 26(2) of *PIPEDA* provides authority for the federal government to exempt organizations and activities from *PIPEDA* where a province has enacted a private-sector privacy law that is substantially similar to *PIPEDA*, and regulations have been passed to this effect for these three provinces: SOR/2004-220; SOR/2004-219; and SOR/2003-374.

[85] Bill C-2 does not extend indemnity to persons who make voluntary disclosures of information to police that police did not request, i.e., corresponding to the new declaratory provision about police receipt of information: s 478.0195(3).

[86] Bill C-2, s 167, amending the *Code* s 487.11.

[87] See, e.g., *R v Chaudhry*, 2021 ONSC 394, at paras 116-121, surveying common law on point and holding that exigent circumstances in that case authorized police to seize taxi records that would otherwise have required a production order.

Mutual Legal Assistance in Criminal Matters Act

Bill C-2 adds provisions to the *MLACMA* that fulfill part of the mandate of international agreements, which Canada has yet to finalize or ratify,[88] to provide for a more expeditious process for enforcing foreign production orders for subscriber information and transmission data.[89] New provisions will oblige the Minister of Justice to "make arrangements for the enforcement" of a foreign order through an *ex parte* process that results in the issuance of a production order for subscriber information or a production order for transmission data if the test for those orders in the *Code* is met.[90]

Criminal detection powers under the PCMLTFA

Bill C-2 amends the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* to allow banks and other institutions to which the Act applies to "collect an individual's personal information without the individual's knowledge or consent" if the RCMP or other police (or prescribed) agency discloses it to them.[91] The bank or other entity may then use it "for the purpose of detecting or deterring a contravention of the laws of Canada or a province that relates to money laundering, terrorist activity financing or sanctions evasion."[92] The police or other agency in this case must state in writing that it is making the disclosure "for the purpose of detecting or deterring" one of these kinds of contraventions under federal or provincial law, and that doing so with the individual's knowledge or consent "would compromise the ability to detect or deter" the contravention at issue.[93]

If a bank or other agency receives personal information from the police and takes investigative steps that intrude on a person's privacy, this could constitute a search or seizure under section 8, because the bank or other receiving entity in this case would act as an agent of the police—extending the latter's investigative purposes.[94] The power given here to banks and other entities to

---

[88] These agreements include those contemplated under the *Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence*, 12 May 2022, CETS No 224, and the US 'Cloud Act', or the *Clarifying Lawful Overseas Use of Data Act*, Pub L No 115–141, div V, 132 Stat 348 (enacted 23 March 2018), codified at 18 USC §§ 2523, 2713.

[89] Bill C-2, s 183, adding to the *Mutual Legal Assistance in Criminal Matters Act*, RSC 1985, c 30 (4th Supp) s 22.07.

[90] *Ibid*, the new section 22.07(3), referring to conditions in the proposed *Code* s 487.0142(2), noted above, and the current *Code* s 487.016(2).

[91] Bill C-2, s 196, adding to the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, SC 2000, c 17 [*PCMLTFA*], a new ss 11.71. The term "personal information" is not defined in the *PCMLTFA* and Bill C-2 does not include a definition.

[92] *Ibid*, adding a new s 11.72.

[93] *Ibid*, s. 11.71(1)(b)(iii).

[94] The agency test under the *Charter*, in an investigative context, is whether the third-party would have taken steps at issue but for police involvement: *R v Broyles*, [1991] 3 SCR 595; *R v M.(M.R.)*, [1998] 3 SCR 393.

"use" personal information to "detect or deter" a crime could be challenged as an unreasonable law under section 8 since it does not come with any safeguards, aside from requiring the entity to be investigating money laundering, terrorism financing, or evading sanctions . For example, police might provide a bank with information from an anonymous tip and the bank might begin making inquiries and gathering information about a person's activities, turning over a dossier to law enforcement. The bank will have conducted an invasive search on behalf of police without oversight or any standard applied to whether the privacy interference was reasonable.

The bill prohibits a bank or other entity from using the information police disclose to it "with the intent to prejudice a criminal investigation"—which is to say, from tipping off a person of interest.[95] The bill also grants civil and criminal immunity to "a person or entity" that collects or uses information here "in good faith."[96]

Part 3: Supporting Authorized Access to Information Act

Part 15 of Bill C-2 contains a whole new statute, the *Supporting Authorized Access to Information Act*, that compels "electronic service providers" to make technical modifications to equipment to provide police and CSIS personnel with immediate access to private data.[97] The Act is modeled after legislation in Britain, Australia, and New Zealand,[98] which sets out similar powers to order specific companies or classes of them to take certain steps—in distinction to the 1994 *Communications Assistance for Law Enforcement Act* in the United States,[99] which sets out general requirements for how to design systems to ensure that law enforcement can access data where authorized. Canada's Parliament has considered similar 'lawful access' bills over the past decade to keep in step with other

---

[95] Bill C-2 s 196, adding the proposed s. 11.72(2) to the *PCMLTFA*.

[96] *Ibid*, a new s 11.73. It seems unlikely that this provision extends immunity to misuses of information in the hands of FINTRAC—the government entity under the *PCMLTFA* to which banks and entities are required to report information about transactions—since the provision limits indemnity to the collection or use of personal information "under this Part." Part 1.2 in its entirety is new with Bill C-2 and the collection or use of personal information in the new s 11.71 here pertains to a person or entity referred to in s 5 of the Act, which does not include FINTRAC. This is not to say, however, that personal information provided to FINTRAC to conduct what amounts to a search might be challenged in a criminal case as unreasonable under section 8.

[97] Bill C-2, s 194.

[98] *Investigatory Powers Act 2016 (UK)*, 2016, c 25; *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (Cth)*, No 148, 2018 (Aus) [*Assistance and Access Act*]; *Search and Surveillance Act 2012 (NZ)*, 2012, No 24.

[99] *Clarifying Lawful Overseas Use of Data Act*, Pub L No 115-141, Div V, 132 Stat 348 (2018).

Five-Eye partners.[100] The data-sharing agreements noted above that Canada is currently negotiating may serve as a further impetus for including this Act in the bill.[101]

The scope and purpose of the Act are broad, but it contains important limitations. The purpose of the Act is to "ensure that electronic service providers can facilitate the exercise of authorities to access information that are conferred on authorized persons."[102] The Act defines the term 'access' "in relation to information" to mean "access by any means that may be authorized under the *Criminal Code* or the *Canadian Security Intelligence Service Act*," including "obtaining a document containing information" or "intercepting [a] communication."[103] "Authorized persons" are only those "having authority… to access information" under the *Criminal Code* or *CSIS Act*.[104] "Information" is any "information, intelligence, or data to which access may be authorized" under either of those statutes.[105] Given the many references here to 'authorization,' the Act would presumably only permit peace or public officers under the *Code* acting with a warrant, requisite grounds, or exigent circumstances—or CSIS agents conducting a national security investigation not targeting a Canadian citizen or permanent resident—to gain access to private data through the technical modifications compelled under the Act.

The parties compellable under the Act are also broad in scope and the ambit of what they can be compelled to do is broad. The Act applies to an "electronic service provider" (ESP), which is anyone who provides an "electronic service" to "persons in Canada" or while carrying on part of its business activities here.[106] An "electronic service" is any service that involves creating, storing, transmitting, or making available information in electronic or digital form—which could be anything from a website offering a *service* to a platform like Signal, iCloud, or Gmail that facilitates communication or stores files.[107] The Minister of Public Safety and Emergency Preparedness can define, by regulation, a sub-class of ESPs to be a "core provider." Core providers can be compelled, by regulation, to implement technical capabilities or to install, maintain, or test "any device,

---

[100] David Fraser, "Past Canadian 'lawful access' attempts, both by Liberal and Conservative governments" (26 June 2025), online (blog): https://blog.privacylawyer.ca/2025/06/past-canadian-lawful-access-attempts.html.

[101] See the agreements *supra* note 88.

[102] Bill C-2, s 194; s 3 of the proposed Act.

[103] *Ibid*, s 2.

[104] *Ibid.*

[105] *Ibid.*

[106] *Ibid.*

[107] *Ibid.*

equipment, or other thing that may enable an authorized person to access information".[108] The Minister can compel an ESP to do these same things or take other steps, but only for a period of time.[109] The Minister, in this case, must take factors into account, including benefits to law enforcement or intelligence, feasibility, costs, and impact on persons receiving a service.[110] Ministerial orders against ESPs are subject to mandatory review before they can be extended.[111] The Minister is not obliged to consider similar factors in crafting regulations that would apply to core providers, but the latter can apply for an exemption to a regulation.[112]

No one can be compelled to do anything if compliance would "introduce a systematic vulnerability" in protections related to a service at issue or "prevent the provider from rectifying such a vulnerability."[113] Comparable Australian legislation defines "systematic vulnerability" as "a vulnerability that affects a whole class of technology" rather than only "a particular person."[114] Canada's Act instead gives the Minister the power to define, by regulation, "the meaning of any term or expression for the purposes of this Act, including 'authentication', 'encryption' and 'systemic vulnerability'."[115] This is an attempt to have one's cake and eat it. The government can appear to be banning back doors to encryption, like Australia and unlike Britain (where legislation does not include a ban).[116] But allowing the Minister to decide what constitutes encryption or an unacceptable systematic vulnerability is, in practical terms, tantamount to not ruling out a back door at all.

Early commentary on the Act has been especially critical of its confidentiality provisions. The Act prohibits an ESP from disclosing that it is subject to a ministerial order to install, modify, or test equipment, and a core provider cannot disclose the fact of being exempt from a requirement to do these things under a regulation.[117] Nor can these parties disclose details about applications for

---

[108] *Ibid*, s 5.

[109] *Ibid*, s 7(1).

[110] *Ibid*, s 7(2).

[111] Ibid, s 11.

[112] Ibid, s 6.

[113] *Ibid*, ss 5(3) and 7(4).

[114] *Assistance and Access Act*, *supra* note x, s 317B; the full definition reads: "systemic vulnerability means a vulnerability that affects a whole class of technology, but does not include a vulnerability that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified."

[115] Bill C-2, s 194; s 46(1)(c) of the proposed Act.

[116] The *Assistance and Access Act* (Australia) and the *Investigatory Powers Act* (UK), *supra* note 101.

[117] Bill C-2, s 194; s 15 of the proposed Act.

exemptions or submissions made or received in the course of a ministerial review of orders.[118] ESPs are also prohibited from disclosing "information related to a systemic vulnerability" or the potential for one—thus preventing companies from proactively warning others when vulnerabilities are detected.

The confidentiality provisions are relevant to concerns under section 8 of the *Charter* for posing a likely impediment to holding police or CSIS agents accountable for searches conducted that do not result in criminal charges or for inspections under the Act (discussed below) that do not result in contraventions. One such concern is that any modification or device an ESP is compelled make or install might be one that gives police real-time access to data, for which they would need an interception warrant under Part VI of the *Criminal Code* but which they may not have (or be aware that they should have) at the time they begin accessing and inspecting private data.[119]

The Act also gives police and CSIS agents the power to make a "request" to an ESP to "provide all reasonable assistance" in the testing of a device or other thing that may enable an authorized person to access information.[120] ESPs are subject to inspections by persons the Minister may delegate for the purpose of "verifying compliance or preventing non-compliance" with the Act.[121] A "designated person" may "enter any place if they have reasonable grounds to believe that anything relevant to that verification or prevention, including any document or electronic data, is located in that place".[122] The Act grants sweeping search powers to "examine anything found in the place, including any document or electronic data," to make copies, remove any document, or use any computer or equipment.[123] Owners or "persons in charge" must give "all assistance that is reasonably required" to allow the designated person to fulfill their function under these provisions.[124] A search in a dwelling house requires a warrant on reasonable grounds—*not* to believe that an offence or

---

[118] *Ibid*.

[119] See *R v TELUS Communications Co.,* 2013 SCC 16 on the need for an interception warrant for police to compel production of future text messages sent by a service provider's customers.

[120] Bill C-2, s 194; s 14 of the proposed Act.

[121] *Ibid*, s 19(1).

[122] *Ibid*.

[123] *Ibid*, s 19(3).

[124] *Ibid*, s 19(5).

contravention has been or will be committed and evidence of it is likely to be found, the standard formulation—but grounds to believe that consent is likely to be refused.[125]

The Supreme Court has affirmed that in regulatory contexts, businesses and individuals enjoy a lesser privacy interest and that invasive searches on lower grounds are reasonable.[126] The sweeping nature of these search powers, however, combined with the lack of safeguards attaching to them raises a doubt about the likelihood of their being found reasonable. The designated person here who might access documents or make copies of them need not be acting with authorization under the *Code* or the *CSIS Act*. Yet, they could readily interfere with significant personal privacy interests. They would not be doing so to investigate persons other than the ESPs being inspected, but a court might consider the powers here unreasonable under section 8 for allowing searches that are too broad in scope without adequate safeguards of personal privacy in a broad sense.[127]

The Act sets out powers to audit ESPs for compliance and for designated persons to issue a "compliance order" to "take any measure necessary" to rectify a compliance issue.[128] An "administrative monetary penalty" of up to $250,000 can be imposed for a "violation" of the Act, with the due diligence and other common law defences available.[129] The Act makes a series acts an offence on summary conviction, with a penalty of up to $500,000, including ESP non-compliance with a ministerial order; failure to provide reasonable assistance to an authorized person to access information or a designated person conducting an inspection; breach of the confidentiality provisions, and breach of a compliance order.[130] Due diligence is a codified defence here.[131] The Act also makes obstructing a designated or authorized person in the course of an inspection or an attempt

---

[125] However, using the likelihood of consent being refused as a standard is not uncommon in the regulatory context in relation dwelling houses: see, e.g., the *Food and Drugs Act* (R.S.C., 1985, c. F-27) s 23(10); *College of Immigration and Citizenship Consultants Act* (S.C. 2019, c. 29, s. 292) s 52(2).

[126] *Goodwin*, *supra* note 5 at para 60; *British Columbia Securities Commission v Branch*, [1995] 2 SCR 3 at para 52; *R v McKinlay Transport Ltd*, [1990] 1 SCR 627 at 647.

[127] A further case to consider here would be a search that a designated person might begin for the purpose of a (regulatory) inspection under Act which becomes at some point a search to investigate a possible crime. Inspection powers here would not authorize a search for the latter purpose or be reasonable if they did (for lacking adequate safeguards). On how and when a search crosses the line from regulatory to criminal, see *R v Jarvis*, [2002] 3 SCR 757, paras 85-99 and *R v Nolet*, 2010 SCC 24 at paras 38-40.

[128] Bill C-2, s 194; ss 21 & 23 of the proposed Act.

[129] *Ibid*, s 27 & 28.

[130] *Ibid*, s 40(1) & (2).

[131] *Ibid*, s 40(4).

to gain access to information, or knowingly making a false statement to them, carrying a fine in each case (up to $50,00 and $250,000 respectively).[132]

The penalty provisions in the Act are relevant to section 8 of the *Charter* when assessing whether powers to search or seize things in an investigation of a contravention or offence under the Act are reasonable. Given the absence of a jail sentence and relatively low monetary penalties, the broad sweep of the powers meant for regulatory purposes could be found to be reasonable, despite there being few safeguards (i.e., a warrant for dwelling houses). But a court may be reluctant to construe these search powers for violations or offences under the Act in such narrow terms. A court might consider the real possibility that through the use of these powers, an inspector or designated person could access customer data of an ESP engaging a high privacy interest, and therefore that these powers cannot be considered strictly regulatory in nature. They may require more safeguards of client or customer information to be held reasonable.

[132] *Ibid*, ss 43 & 44.