Canadian Journal of Law and Technology

Volume 21 | Number 1 Article 1

7-2023

The Future of Data Protection Enforcement in Canada: Lessons from the GDPR

Guilda Rostama
Independent Researcher

Teresa Scassa
University of Ottawa, Canada Research Chair in Information Law and Policy

The Future of Data Protection Enforcement in Canada: Lessons from the GDPR

Guilda Rostama[*] *& Teresa Scassa*[**]

1. INTRODUCTION

Imagine a not-too-distant scenario in which a private sector organization in Canada is investigated by the Privacy Commissioner of Canada jointly with the Commissioners of Quebec, British Columbia ("BC"), and Alberta in relation to complaints that it shared massive quantities of personal data with third parties contrary to its stated practices in its privacy policies. Imagine also that each of the commissioners is empowered under newly amended data protection legislation to issue substantial Administrative Monetary Penalties ("AMPs"). If each of the commissioners finds that its respective laws were breached, should the organization be subject to four different AMPs, or just one? This is a central question that this article seeks to answer.

Canada's private sector data protection statute, the *Personal Information Protection and Electronic Documents Act* ("PIPEDA"),[1] applies to the collection, use, or disclosure of personal information in the course of commercial activity. It applies to all such activity where there are interprovincial or international data flows; it also applies to all commercial activity in those provinces that have not enacted private sector data protection laws that are judged to be "substantially similar." Three provinces — Quebec, BC, and Alberta — have substantially similar private sector laws. Although the initial concept may have been to neatly divide jurisdiction between the relevant commissioners based upon the intra- or inter-provincial nature of any activity, the situation has evolved to one in which federal and provincial commissioners treat their jurisdiction as overlapping in some cases (where the same set of facts has inter- and intra-provincial dimensions that attract the application of both PIPEDA and the relevant provincial statute) and possibly even concurrent (where both PIPEDA and the relevant provincial statute are considered to apply to the same facts).[2] As we move to a new era of

---

[*] Privacy law and GDPR specialist, independent researcher.

[**] Canada Research Chair in Information Law and Policy, University of Ottawa. We are grateful for the helpful anonymous peer review comments we received.

[1] SC 2000, c 5.

[2] Examples of recent investigations carried out by all four commissioners include the following: Office of the Privacy Commissioner of Canada, "Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta," PIPEDA Findings #2021-001, (2 February 2021), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-

data protection law in which commissioners' enforcement powers are substantially increased, this concurrent and/or overlapping jurisdiction raises important questions about the co-ordination of what might be multiple enforcement measures with respect to the same breach.

There is no doubt that Canadian private sector data protection law is in need of a significant overhaul. PIPEDA was first enacted in 2000, at a time when building trust in emerging e-commerce was the main preoccupation. By 2020, the data-driven economy and the burgeoning artificial intelligence ("AI") sector had created significant new data protection challenges. These included the widespread and often continuous collection of significant volumes of data, as well as uses that included profiling, artificial intelligence innovation, and automated decision-making. The increasing volume and changing nature of cross-border data flows also made it necessary to take into account the potential for data breaches on a global scale. Calls for reform of PIPEDA included demands for much stronger enforcement of what had initially been conceived of as an ombuds-style soft-compliance model. In November 2020, Canada's federal government introduced into Parliament Bill C-11, its long-awaited bill to reform Canada's aging private sector data protection law, which would replace PIPEDA with the *Canadian Privacy Protection Act* ("CPPA").[3] Bill C-11 contained enhanced enforcement measures, including the power to levy substantial AMPs for certain breaches of the statute. Many elements of Bill C-11 were controversial,[4] and the bill died on the order paper when a federal election was called in 2021. In June 2022, a revised version of Bill C-11 — now renumbered as Bill C-27[5] — was introduced in Parliament.

001/ > [Joint Investigation of Clearview AI]; and Office of the Privacy Commissioner of Canada, "Joint investigation into location tracking by the Tim Hortons App," PIPEDA Findings #2022-001 (1 June 2022), online: < www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-001/ > [Joint Investigation of Tim Hortons]. An example of a joint investigation between the federal, BC, and Alberta commissioners is the following: Office of the Information and Privacy Commissioner for British Columbia, "Joint investigation of The Cadillac Fairview Corporation Limited by the Privacy Commissioner of Canada, the Information and Privacy Commissioner of Alberta, and the Information and Privacy Commissioner for British Columbia, Office of the Information and Privacy Commissioner for British Columbia, 2020 CanLIIDocs 3393" (29 October 2020), online: < canlii.ca/t/t0bj > .

3 Bill C-11, *An Act to enact the Consumer Privacy Protection Act and the Personal Information and Data Protection Tribunal Act and to make consequential and related amendments to other Acts*, 2nd Sess, 43rd Parl, 2020 (first reading 17 November 2020; second reading never took place).

4 See, for example, the trenchant critique of the Bill by then Privacy Commissioner Daniel Therrien: Office of the Privacy Commissioner of Canada, "Submission of the Office of the Privacy Commissioner of Canada on Bill C-11, the Digital Charter Implementation Act, 2020" (May 2021), online: < www.priv.gc.ca/en/opc-actions-and-decisions/submissions-to-consultations/sub_ethi_c11_2105/ > .

5 Bill C-27, *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make*

Like Bill C-11, Bill C-27 proposes new enforcement powers for the federal Commissioner, including order-making powers and the ability to recommend AMPs to a new Data Tribunal. Indeed, until now, PIPEDA and its provincial equivalents have largely taken a soft-touch approach to enforcement. Commissioners may conduct audits or investigate complaints under their statutes, but remedial powers have been limited to making orders (in the case of the provinces) or recommendations (in the case of PIPEDA). The commissioners were not empowered to award damages or impose monetary penalties.

Changes to this approach have already begun. Quebec's recent reform of its public and private sector data protection laws added AMPs to the commissioner's suite of powers. Once a new federal bill is passed, it is expected that BC, and Alberta will amend their own private sector data protection laws in order to maintain their substantial similarity. In BC, a special committee of the legislature has already made recommendations for the reform of BC's law,[6] and Alberta has held consultations on amendments to its *Personal Information Protection Act*.[7] It is anticipated that both provinces will consider adding AMPs to the enforcement powers in the upcoming reform of their statutes.[8]

In this article, we consider the impending shift in Canada from a soft-compliance model of private sector data protection to one in which commissioners in three provinces and at the federal level will likely wield significant new enforcement powers. Interestingly, based on recent experience, provincial and federal commissioners may exercise their respective powers concurrently in cases that involve cross-border flows of data. Indeed, recognizing that "[d]omestic and international enforcement cooperation in the area of privacy law is increasingly critical in a digitized world," the privacy guardians signed a collaboration agreement in May 2022, allowing them to "share information, consult on enforcement matters of mutual interest, discuss policy and develop public education and compliance documents."[9]

We explore the implications for the enforcement of data protection laws in Canada once the anticipated reforms take place. If three provincial

---

consequential and related amendments to other Acts, 1st Sess, 44th Parl, 2022 (first reading 16 June 2022).

6 Special Committee to Review the Personal Information Protection Act (BC), "Modernizing British Columbia's Private Sector Privacy Law" (December 2021), online (pdf): < www.leg.bc.ca/content/CommitteeDocuments/42nd-parliament/2nd-session/pipa/report/SCPIPA-Report_2021-12-06.pdf > [BC Special Committee].

7 Government of Alberta, "Privacy Protection Engagement" (27 October 27 2021), online: < www.alberta.ca/privacy-protection-engagement.aspx > .

8 BC Special Committee, *supra* note 6 at 43.

9 British Columbia Office of the Information and Privacy Commissioner, "News Release: Privacy guardians sign collaboration agreement" (10 May 2022), online: < www.oipc.bc.ca/news-releases/3668 > .

commissioners and the federal commissioner have overlapping or concurrent jurisdiction over the actions of an organization and each has the power to levy AMPs, we ask how breach investigations should be conducted and how determinations should be made about who should levy an AMP, knowing that there is the potential for multiple AMPs to be imposed with respect to the same breach of data protection law. We also consider the importance of the concept of substantial similarity to the issue of harmonized enforcement. In considering the evolving Canadian context, we draw upon the European Union ("EU") experience under the *General Data Protection Regulation* ("GDPR")[10] with the one-stop-shop model for enforcement in cases where more than one jurisdiction is affected by the actions of an organization. Although there are important differences between the EU and Canada in terms of data protection, there are already informal efforts to harmonize approaches in Canada. AMPs change the enforcement landscape for data protection law, and the EU experience can offer useful insights for Canadian approaches where multiple commissioners have concurrent or overlapping jurisdiction. Indeed, the creation of a cooperation mechanism for 27 different countries within the EU is a notable achievement and one from which we might learn.

Our analysis begins with a discussion of constitutional jurisdiction over private sector data protection in Canada. We then look at the substantial similarity framework established in PIPEDA and carried over with some modifications into Bill C-27, and we discuss how this framework leads to overlaps in jurisdiction. We next consider the need for harmonization of enforcement, using the EU's one-stop-shop model under its GDPR as a basis for comparison. We next look at whether a one-stop-shop model might be suitable in Canada and what might be required to make it work.

2. CONSTITUTIONAL JURISDICTION OVER PRIVATE SECTOR DATA PROTECTION IN CANADA

The division of powers between federal and provincial governments in the *Constitution Act, 1867*[11] has sometimes posed challenges for national regulation of key economic areas. Although the federal government has jurisdiction over "the regulation of trade and commerce" under s 91(2), the provinces retain jurisdiction over "property and civil rights" (s 92(13)) and "matters of a merely local or private nature" (s 92(16)). Contracts and torts — essentially, private law — fall under the category of "property and civil rights." This can create constitutional tension between the federal and provincial governments in the commercial context. In the case of data protection, it is generally assumed that

---

[10] EU General Data Protection Regulation (GDPR): Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

[11] *The Constitution Act, 1867* (UK), 30 & 31 Vict, c 3, ss 91, 92.

the provinces have jurisdiction to enact laws governing how personal data are collected, used and disclosed in the province, including in the course of intra-provincial commercial transactions. The federal government would have jurisdiction over the collection, use, and disclosure of personal data in federally regulated sectors, such as banking, and in relation to interprovincial or cross-border transactions. What is less clear is the extent of federal jurisdiction to set a national standard and to have it apply to all commercial activity in the country.

Over the years, the federal "trade and commerce" power has been interpreted to include a category of "general trade and commerce" that "authorizes laws where the national interest is engaged in a manner that is qualitatively different from provincial concerns."[12] The general trade and commerce power is distinct from the power of the federal government to regulate interprovincial and international trade.[13] Canada's trademark registration scheme is an example of the successful reliance upon the "general trade and commerce" power. The Supreme Court of Canada has ruled that the *Trademarks Act* is validly enacted federal legislation that is supported by the general trade and commerce power, notwithstanding the fact that unregistered trademarks are also governed by provincial law.[14] A key feature of the federal statute — and one that was important from the perspective of its constitutional justification — was the presence of a national registration scheme for trademarks and the possibility that this created for a national scope for the recognition and protection of trademarks.[15] A matter does not fall within federal jurisdiction simply because it would be easier to deal with at that level.[16]

---

[12] *General Motors of Canada Ltd. v. City National Leasing*, 1989 CarswellOnt 956, 1989 CarswellOnt 125 (S.C.C.); *Reference re Securities Act (Canada)*, 2011 SCC 66, 2011 CarswellNat 5243, 2011 CarswellNat 5244 (S.C.C.) at para. 46 [*Securities Reference 2011*].

[13] The Supreme Court of Canada has cautioned against an overly broad interpretation of the general trade and commerce power on the basis that such an interpretation would "upset the constitutional balance" by permitting "federal duplication (and, in cases of conflict, evisceration) of the provincial powers over large aspects of property and civil rights and local matters." As a result, according to the Court, "the trade and commerce power has been confined to matters that are genuinely national in scope and qualitatively distinct from those falling under provincial heads of power relating to local matters and property and civil rights." See *Securities Reference 2011*, *supra* note 12 at para 70.

[14] *Kirkbi AG v. Ritvik Holdings Inc. / Gestions Ritvik Inc.*, 2005 SCC 65, 2005 CarswellNat 3631, 2005 CarswellNat 3632 (S.C.C.).

[15] In *General Motors of Canada Ltd. v. City National Leasing*, 1989 CarswellOnt 956, 1989 CarswellOnt 125 (S.C.C.) at 661-662, the Supreme Court of Canada relied upon the five indicia of federal competence under the general trade and commerce power set out in the earlier *General Motors* decision: "(1) whether the impugned law is part of a general regulatory scheme; (2) whether the scheme is under the oversight of a regulatory agency; (3) whether the legislation is concerned with trade as a whole rather than with a particular industry; (4) whether it is of such a nature that provinces, acting alone or in concert, would be constitutionally incapable of enacting it; and (5) whether the legislative scheme

This, then, is the delicate constitutional footing on which PIPEDA and Bill C-27 rest. In its early days, PIPEDA faced at least two constitutional challenges that were never ultimately decided by the courts.[17] Bill C-27 treads cautiously in some areas, no doubt seeking to avoid jurisdictional controversies.[18] It is unclear whether the significant problems with Canada's digital and data law and policy infrastructure that were laid bare during the COVID-19 pandemic[19] will support

---

is such that the failure to include one or more provinces or localities in the scheme would jeopardize its successful operation in other parts of the country." PIPEDA to some extent maps onto this framework. Private sector data protection is part of a regulatory scheme overseen by the Privacy Commissioner of Canada, an independent agent of Parliament. Its application is to commercial activity broadly, and there is an argument that without a national standard, data protection would be significantly undermined. The "substantial similarity" framework in PIPEDA carves out space for provincial action that is complementary to the federal scheme. In the first *Securities Reference*, the Supreme Court of Canada ruled that the establishment by the federal government of a national securities regulator did not fall within its general trade and commerce power, while at the same time acknowledging the challenges that this might create. The Court urged cooperation, stating, "[t]he common ground that emerges is that each level of government has jurisdiction over some aspects of the regulation of securities and each can work in collaboration with the other to carry out its responsibilities" (*Securities Reference 2011*, *supra* note 12 at para 131). The second Securities Reference case found that a modified version of the legislation was constitutional because it "addresse[d] a matter of genuine national importance and scope going to trade as a whole in a way that [was] distinct and different from provincial concerns" (*Reference re Pan-Canadian Securities Regulation*, 2018 SCC 48, 2018 CarswellQue 9836, 2018 CarswellQue 9837 (S.C.C.) at para. 102, citing *Securities Reference 2011*, *supra* note 12 at para 124).

16 *Securities Reference 2011*, *supra* note 12 at para 90, the Supreme Court of Canada cautioned that "one should not confuse what is optimum as a matter of policy and what is constitutionally permissible." The Court noted that "references in past cases to promoting fair and effective commerce should be understood as referring to constitutional powers that, because they are essential in the national interest, transcend provincial interests and are truly national in importance and scope. Canada must identify a federal aspect distinct from that on which the provincial legislation is grounded. The courts do not have the power to declare legislation constitutional simply because they conclude that it may be the best option from the point of view of policy. The test is not which jurisdiction — federal or provincial — is thought to be best placed to legislate regarding the matter in question. The inquiry into constitutional powers under ss. 91 and 92 of the Constitution Act, 1867 focuses on legislative competence, not policy."

17 On December 17, 2003, the Quebec government issued a decree setting out its intention to pursue a reference case before the Quebec Court of Appeal to challenge the constitutionality of PIPEDA (Gouvernement du Québec, Décret 1368-2003). This challenge was not ultimately pursued. Constitutional issues were also raised in *State Farm Mutual Automobile Insurance Co. v. Canada (Privacy Commissioner)*, 2010 FC 736, 2010 CarswellNat 3689, 2010 CarswellNat 2225 (F.C.), although the Federal Court resolved the dispute without deciding the constitutional issues.

18 For example, Bill C-27 refers to minors but avoids defining an age limit, as the age of majority is traditionally a matter of provincial jurisdiction.

19 See e.g. Amir Attaran & Adam R. Houston, "Pandemic Data Sharing: How the Canadian Constitution Has Turned into a Suicide Pact" in Colleen M Flood et al, eds,

greater federal activity in this area, or whether they will simply fuel more calls for enhanced federal-provincial cooperation.

3. SUBSTANTIAL SIMILARITY AND OVERLAPPING OR CONCURRENT JURISDICTION

The delicate constitutional footing on which PIPEDA rests explains why it contains a provision that allows the Governor in Council to make an order recognizing that a provincial private sector data protection law is "substantially similar" to PIPEDA.[20] Under s 26(2)(b) of PIPEDA, if the Governor in Council is satisfied that a provincial law that is substantially similar to PIPEDA "applies to an organization, a class of organizations, an activity or a class of activities," it can, by Order, "exempt the organization, activity or class from the application of this Part in respect of the collection, use or disclosure of personal information that occurs within that province."

Quebec, BC, and Alberta have their own private sector data protection statutes. Quebec's original private sector data protection law predated PIPEDA. Although this law was declared substantially similar, it was clearly not based on PIPEDA, nor was PIPEDA modelled on the Quebec statute. Quebec has recently enacted its own revised data protection law,[21] significantly changing its regime in advance of any action by the federal government. BC and Alberta both drafted their own *Personal Information Protection Acts* after PIPEDA was enacted, and overt similarities are more evident in those statutes.

The current framework means that if an Alberta resident has a complaint about a breach of their data protection rights with respect to the actions of an Alberta-based company, their complaint will be received and addressed by the Alberta Information and Privacy Commissioner under Alberta's *Personal Information Protection Act*,[22] whereas if the complaint is directed against a federally regulated organization (such as a bank, for example) or one based in another province or country, they must direct their complaint to the federal Privacy Commissioner. For the provinces and territories that have chosen not to enact their own private sector data protection laws, any data protection issue is directed to the federal Privacy Commissioner under PIPEDA.

Bill C-27 reproduces the substantial similarity approach found in PIPEDA, although with some modifications. For example, Bill C-27 provides for regulations that will set out the criteria for making a substantial similarity determination. Regulations will also provide for a process for reconsideration of such a finding and will lay out criteria for any reconsideration. Under PIPEDA,

---

Vulnerable: The Law, Policy and Ethics of COVID-19 (Ottawa: University of Ottawa Press, 2020) 91.

[20] PIPEDA, *supra* note 1, s 26(2).

[21] *An Act to modernize legislative provisions as regards the protection of personal information*, SQ 2021, c 25.

[22] SA 2003, c P-6.5.

there was no provision for reconsideration of substantial similarity once it was accorded; under Bill C-27, provincial laws can be reassessed if they do not keep up with changes to the federal statute.

In addition to applying to intra-provincial matters where no substantially similar legislation exists, PIPEDA also applies to interprovincial and international data flows.[23] However, nothing in PIPEDA expressly precludes the application of substantially similar provincial laws to interprovincial and international data flows where there is a "real and substantial connection" with the province and the possibility of concurrent jurisdiction exists. In other words, if there is a breach of privacy that affects individuals across Canada, the law of reference would be PIPEDA, but the commissioners in provinces that have their own private sector data protection laws could, at least in theory, also assume jurisdiction. BC's *Personal Information Protection Act* ("PIPA") is the apparent exception. It specifically provides that if PIPEDA applies to a matter, PIPA does not.[24] However, the Quebec and Alberta laws contain no such provision. In Quebec, the Commission de l'accès à l'information has explicitly asserted concurrent jurisdiction.[25]

In addition to concurrent jurisdiction, it is also possible to have overlapping jurisdiction where federal and provincial statutes apply to the same set of facts. This might arise where some parts of a company's activities have cross-border dimensions, whereas others are interprovincial. For example, an organization might collect data from residents of BC (along with residents of other provinces), triggering the application of BC's PIPA, but those data may be stored on servers outside BC that are hacked by actors also outside BC. In such circumstances, the BC commissioner might assert jurisdiction over the collection and use of the personal data of BC residents by the organization, whereas the federal commissioner would have jurisdiction by virtue of the interprovincial dimensions of the organization's activities and the breach. This might explain why the BC Commissioner has participated in joint investigations notwithstanding section 3(1)(c) of PIPA, which provides that where PIPEDA applies, BC's PIPA does not.

---

[23] This jurisdiction was presumed under PIPEDA: see Office of the Privacy Commissioner of Canada, "PIPEDA in brief" (May 2019), online: <www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#_h1-2>, which states: "All businesses that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province or territory in which they are based (including provinces with substantially similar legislation." The assumption of jurisdiction is made explicit in Bill C-27, *supra* note 5, s 6(2)(a).

[24] *Personal Information Protection Act*, SBC 2003, c 63, s 3(1)(c).

[25] See e.g., *X. c. Rogers Communications Inc.* (September 29, 2014), Doc. 111310 (Commission d'accès à l'information), online: <decisions.cai.gouv.qc.ca/cai/ss/fr/item/357046/index.do>.

The joint investigations carried out by the federal and provincial commissioners in cases involving companies whose actions span provincial or national borders also suggest a recognition of concurrent jurisdiction, even in BC. The federal privacy commissioner and the commissioners of Alberta, BC, and Quebec have collaborated increasingly closely on data protection issues over the last number of years. It is now common for high-profile and high-impact data protection issues with national dimensions to be the subject of joint investigations by this group of commissioners. Noteworthy recent joint investigations include those into Clearview AI[26] and Tim Hortons.[27] These investigations have included findings that the data protection law of each of the commissioners' respective jurisdictions was breached. Following joint findings of breaches of the law, each commissioner remains free to pursue whatever measures are provided for under their respective enabling laws. For example, in the Clearview AI case, the commissioners of Quebec, BC, and Alberta have each issued orders.[28]

Although it directly addresses the issue of applicable law rather than of concurrent jurisdiction, the Office of the Privacy Commissioner of Canada ("OPC") recognizes the potential for overlapping jurisdiction by stating the following:

> If you operate in more than one province, you may have to comply with more than one statute, depending on the jurisdiction (. . .) If your organization operates in a province with substantially similar provincial legislation (B.C., Alberta and Quebec) and has to follow that law, PIPEDA only applies to interprovincial and international transaction (. . .) One part of a transaction (e.g. collection) may be subject to a provincial privacy law while another part of the transaction (disclosure) may be subject to PIPEDA.[29]

It seems possible, therefore that there may be both concurrent and overlapping jurisdiction for private sector data protection, at least in BC, Alberta, and Quebec.

---

[26] See Joint Investigation of Clearview AI, *supra* note 2.

[27] See Joint Investigation of Tim Hortons, *supra* note 2.

[28] See Office of the Information and Privacy Commissioner (BC), Order P21-08, Clearview AI, Inc (14 December 2021), online: < www.oipc.bc.ca/orders/3610 > ; Office of the Information and Privacy Commissioner (Alberta), Order P2021-12 (7 December 2021), online: < oipc.ab.ca/wp-content/uploads/2022/01/Order-P2021-12.pdf > ; Commission d'accès à l'information du Québec, Clearview AI, Inc, 1023158-S (14 December 2021), online: < decisions.cai.gouv.qc.ca/cai/ss/fr/item/518218/index.do > .

[29] Office of the Privacy Commissioner of Canada, "Questions and Answers regarding the application of PIPEDA, Alberta and British Columbia's Personal Information Protection Acts" (November 2004), online: < www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/r_o_p/02_05_d_26/ > .

Both concurrent and overlapping jurisdiction can be challenging and unpredictable for organizations. Organizations must consider how to build a privacy program on the basis of several laws that, even if deemed substantially similar, could contain different requirements in similar situations. In its document on overlapping jurisdiction, the OPC recommends that organizations look at the differences between the laws, stating that "[i]f you follow the more stringent requirement all the time, you will very likely comply with both laws."[30]

With respect to which privacy commissioner would be competent, an approximate answer is given:

> In answering this question, the substance of the transaction and the subject of the complaint would be considered. From the customer's perspective, the transaction takes place in the province. The customer is likely not even aware of the trans-border data flow that took place electronically (. . .) Commissioners' offices will coordinate their activities to reduce duplication of effort on the part of the complainant and organization. They are working to develop a harmonized approach to dealing with privacy complaints in the private sector.[31]

The OPC also attempts to provide guidance to individuals so that they can determine which privacy commissioner should receive their complaint:

> In order to determine the privacy office to which you should direct your complaint, the following factors may be considered:
>
> a) Which practice do you object to (e.g., collection, use, refusal of access to your personal information, disclosure, safeguarding, etc.)? If you are concerned about the organization disclosing your information, then the privacy office that oversees the organization doing the disclosure should receive your complaint.
>
> b) Is one of the organizations on contract to the other? If so, the primary organization is probably the one responsible for the information practices of the other. The complainant may be best to complain to the Privacy Office with jurisdiction for the contract.[32]

In other words, it is up to the individual to determine which privacy commissioner will be competent to take their complaints, knowing that if a mistake is made, "the office that originally looked into [their] case will return to [them] all the information [they] provided to it. Or, with consent, the original privacy office will forward these materials to the appropriate privacy office on [their] behalf."[33] By and large, this system has worked under PIPEDA.

---

[30] *Ibid.*

[31] *Ibid.*

[32] *Ibid.*

[33] *Ibid.*

Both BC and Alberta will likely look with interest to Bill C-27 should it be passed into law. It is to be expected that substantial similarity will be an objective in both provinces, although this does not mean that the reform bills in those jurisdictions will be simple copies of what is done at the federal level. Canada's largest province, Ontario, published a White Paper in 2021[34] that called for comment on its proposal for a private sector data protection law for Ontario, although momentum has since faded for any action in this area. Although the White Paper clearly used Bill C-11 as a model for many of its proposed provisions, it did recommend taking different approaches on some issues. For example, the report explicitly recommended taking a human rights-based approach to privacy and proposed more detailed protections for the privacy of children and youth.

The issue of concurrent and overlapping jurisdiction becomes even more challenging in the context of the shift in the Canadian enforcement model. Bill C-27 proposes giving the Privacy Commissioner of Canada the power to recommend the imposition of substantial AMPs in certain circumstances. Quebec's new legislation already includes such powers for the Commission d'accès à l'information. The BC Special Legislative Committee has also recommended that a revised provincial statute should include the power to impose AMPs.[35] In all likelihood, Alberta will follow suit. Ontario's White Paper recommended that the Ontario Commissioner be given powers to levy substantial AMPs for certain categories of breach.[36] It is clear that Canada is shifting, overall, from a soft-compliance approach to data protection to one where there can be substantial penalties imposed for breaches of legal obligations. Particularly because of the potential for exercise of concurrent or overlapping jurisdiction, there will need to be harmonization of enforcement approaches.

4. HARMONIZATION OF ENFORCEMENT

Up to this point we have explained how it has arisen that privacy commissioners in Quebec, BC, and Alberta have sometimes asserted either concurrent or overlapping jurisdiction with the federal privacy commissioner in data protection matters that have national impact. If, as seems likely, Canada, BC, and Alberta join Quebec in adding AMPs to the enforcement powers under

---

[34] Ministry of Government and Consumer Services (ON), "Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy" (17 June 2021), online: < www.ontariocanada.com/registry/view.do?postingId = 37468 > ["Modernizing Privacy in Ontario"].

[35] BC Special Committee, *supra* note 6 at 7.

[36] See "Modernizing Privacy in Ontario," *supra* note 34 at 34-35. Note that the province of Ontario has already provided for AMPs in reforms to its Personal Health Information Protection Act, SO 2004, c 3, Sch A, s 61.1, although those have still not come into effect and are awaiting regulations.

the provinces' respective data protection laws, there will be a new need to harmonize enforcement approaches.

Currently, where findings of breaches are made in joint investigations, each of the provincial commissioners can order the respondent organization to cease the offending practices or to take any other measures necessary to correct the breach (such as destroying improperly collected personal data).[37] The federal commissioner can recommend such actions and can apply to Federal Court for an order.[38] For the most part, the orders will be very similar. The provincial orders might relate only to the personal data of the residents of the particular province, but, taken collectively, the orders will require the organization to address the problem on a nation-wide basis.

Federal-provincial cooperation on the interpretation and application of data protection laws through joint investigations has considerable merit in terms of creating shared national expectations around data protection obligations. However, as we move toward a future in which commissioners across the country have new enforcement powers, the nature of this federal-provincial cooperation may need to change. And, even absent a joint investigation, the exercise of concurrent jurisdiction over the same dispute by two or more commissioners could raise serious issues regarding enforcement.

This is because if there is either a joint investigation or concurrent investigations by federal and provincial commissioners into a breach of data protection law involving cross-border data flows, and if the federal and provincial laws have been amended to allow the imposition of AMPs, there is the potential for multiple AMPs to be imposed with respect to the same breach. To make matters more complicated, while notionally the provincial commissioners will be assessing AMPs with respect to the impact of the breach in their respective jurisdictions, the federal legislation will apply nationally, thus creating the potential for AMPs that overlap with provincially imposed AMPs. As a result, although some may argue that we should not be too concerned that the egregious breaches for which AMPs were meant to provide a penalty are met with up to four different AMPs, there are reasons to address such overlaps. Not only does such a system create the potential for problematic divergences in approach, but it is arguably unfair for an organization to be financially penalized multiple times for the same fault in the same country. This is particularly the case where the provincial commissioners exercise concurrent jurisdiction with the federal commissioner on the same set of facts. We suggest that there may need to be explicit legislative attention paid to the interrelationship of these different regimes.

To address these issues, we draw upon the experience under the EU's GDPR with the one-stop-shop mechanism, i.e., the procedures put in place to address

---

[37] An example of this can be found in the orders issued respectively by the Commissioners of BC, Alberta, and Quebec following the Joint Investigation of Clearview AI, *supra* note 2.

[38] PIPEDA, *supra* note 1, s 15.

cross-border GDPR-breaches that impact multiple jurisdictions. We do so in order to identify challenges and issues in the Canadian context and to make recommendations for legislative change.

(a) What is the One-Stop-Shop?

The one-stop-shop is a procedure put in place by the GDPR that aims to harmonize at the European level the decisions of data protection authorities concerning cross-border processing. Cross-border processing is a processing of personal data which involves several Member States, either because the organization:

a) processes personal data in the context of activities carried out in establishments in several EU Member States; or
b) processes personal data in a single establishment that materially affects individuals in different countries in the EU.

Before the GDPR came into force, organizations that deployed cross-border processing activities were potentially subject to rulings of 27 different regulators for the same breach of privacy. This was cumbersome and time consuming for organizations, and it prevented a uniform application of European rules.[39] To resolve these difficulties, the GDPR established the "one-stop-shop" mechanism, which is based on the following three principles:

a) This mechanism is only available for companies established in the EU;[40]
b) There is a single point of contact for organizations: this is the "lead" authority, that is to say the data protection authority of the country where the main establishment of the business is located.
c) The organization is subject to one decision that is valid throughout the EU: any decision made by the lead authority is taken with the validation of all the other concerned EU regulators.[41]

---

[39] The first proposal of the European Commission in 2011 highlighted the need for consistency several times. For example: "When personal data moves across borders it may put at increased risk the ability of individuals to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information. At the same time, supervisory authorities may find that they are unable to pursue complaints or conduct investigations relating to the activities outside their borders. Their efforts to work together in the cross-border context may also be hampered by insufficient preventative or remedial powers, inconsistent legal regimes, and practical obstacles like resource constraints. Therefore, there is a need to promote closer co-operation among data protection supervisory authorities to help them exchange information and carry out investigations with their international counterparts." (*Proposal for a Regulation of the European Parliament and the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)*, COM/2012/011 final at para 91, online: < eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52012PC0011 >.)

[40] To be established in the EU, a foreign-based company must have an "establishment" in one of the EU Member States, which, according to Recital 22, implies the effective and real exercise of activity through stable arrangements.

[41] GDPR, *supra* note 10, art 60.

Therefore, the one-stop-shop facilitates the enforcement of the GDPR without impacting individuals: their national data protection authority remains their only point of contact. For example, individuals residing in France can continue to address their complaints to the Commission nationale de l'informatique et des libertés ("CNIL"), even if the latter is not the lead authority with regard to enforcement.

(b) How Does the One-Stop-Shop Mechanism Work?

When an EU regulator receives a complaint, it must inform all other EU regulators in order to determine who the lead supervisory authority is and which other EU regulators may be concerned by the complaint (either because the organization in question has an establishment in their territory, or because there are individuals that are affected by the data processing deployed by the organization). Once the lead authority has been identified, it is in charge of leading the case and must coordinate with its EU counterparts. In other words, it must lead the investigation, prepare the draft decision, and circulate the draft among the other relevant data protection authorities. It must then collect and take into account their observations, with the aim of reaching a rapid and consensual decision between the authorities. In the event of a persistent disagreement between the authorities concerned, the lead authority must refer the draft decision to the European Data Protection Committee for a decision. The committee, which brings together all the data protection authorities of the European Union, will then have to adopt a binding decision for the lead authority. The resultant decision therefore represents the common interpretation of the European authorities concerning the cross-border processing in respect of which the decision is taken.

The lead supervisory authority must inform the complainant of the decision taken with regard to the controller and must notify them of any decision to close or reject the complaint.

(c) Feedback on the One-Stop-Shop Four Years After the GDPR

Almost five years after the entry into force of the GDPR, some people choose to take the view that the one-stop-shop mechanism should be fundamentally revised because of the phenomenon of forum shopping.

For example, up until 2020, TikTok did not have any establishment in the EU, which meant that each supervisory authority in the EU was competent in its own jurisdiction (the one-stop-shop mechanism cannot be activated for an organization that does not have any presence in the EU). Thus, the French, Italian, and Dutch authorities had started their own investigations against TikTok and created a "TikTok taskforce" at the level of the European Data Protection Board ("EDPB") to "coordinate potential actions and to acquire a more comprehensive overview of TikTok's processing and practices across the

EU." [42] As Politico notes, "TikTok has been in the sights of the Italian regulator since at least January 2020, when it first called for an EU-wide task force to address the risks posed to children by the platform."[43] However, following the creation of this taskforce, TikTok decided to shift its key data protection functions to Dublin. This choice to create an establishment within the meaning of the GDPR in Dublin had the direct effect of stopping national investigations launched by national data protection authorities. The Dutch Data Protection Authority's Deputy Chair, Monique Verdier, remarked, "[w]e are now transferring several results of our investigation to the Irish Data Protection Commission. Initially TikTok did not have its head office in Europe, and we were able to look into this matter from the Netherlands, but in the course of our investigation, TikTok established operations in Ireland."[44] Therefore, the EDPB guidelines were followed,[45] and all pending proceedings were transferred to the Irish Data Protection Commission ("DPC"), which became the Lead Supervisory Authority for the investigations launched by other national authorities.

This example of forum-shopping is typical of what may occur with the one-stop-shop mechanism. As noted by some,

> Most Big Tech companies have their European headquarters in Ireland because of its tax system. As a result, the DPC is the leading Data Protection Authority to decide on GDPR breaches and privacy complaints against these tech giants. Critics argue that there might be a temptation for Ireland to downplay the enforcement of GDPR, as it is in its economic interest that the large tech corporation remain based in its territory.[46]

In addition, the DPC's budget requests were turned down many times by the Irish government,[47] which has a significant impact on the financial and human

---

[42] European Data Protection Board, "Thirty-first Plenary session: Establishment of a taskforce on TikTok, Response to MEPs on use of Clearview AI by law enforcement authorities, Response to ENISA Advisory Group, Response to Open Letter NYOB" (10 June 2020), online: < edpb.europa.eu/news/news/2020/thirty-first-plenary-session-establishment-taskforce-tiktok-response-meps-use_en > .

[43] Hannah Roberts & Giorgio Leali, "TikTok Is the Latest Target in Italy's Crusade against Big Tech" (1 February 2021), online: *Politico* < politico.eu/article/tiktok-latest-target-italy-privacy-regulator-crusade-against-big-tech/ > .

[44] European Data Protection Board, "Dutch DPA: TikTok Fined for Violating Children's Privacy" (22 July 2021), online: < edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en > .

[45] European Data Protection Board, "Opinion 8/2019 on the Competence of a Supervisory Authority in Case of a Change in Circumstances Relating to the Main or Single Establishment" (9 July 2019) at para 31, online (pdf): < edpb.europa.eu/sites/default/files/files/file1/edpb_opinion_201908_changeofmainorsingleestablishment.pdf > .

[46] Luca Bertuzzi, "MEPs Call for Infringement Procedure against Ireland" (27 May 2021), online: *Euractiv* < www.euractiv.com/section/data-protection/news/european-parliament-calls-for-infringement-procedure-against-ireland/ > .

resources that the authority can commit to investigations. In this context, the European Parliament even voted in May 2021 in favor of a resolution calling on the European Commission to open an infringement procedure against Ireland for failing to enforce the GDPR.[48] As some observe, "[t]ech companies have noticed the system's weaknesses and have tried to use them to their advantage."[49]

Nevertheless, one may wonder whether the underfunding of the DPC and the resulting lack of enforcement actions should lead to a condemnation of the one-stop-shop system in general. Indeed, the one-stop-shop system can also lead to very successful investigations. For example, it has resulted in a €746 million fine against Amazon.[50] In this case, a single decision was made, issued by Luxembourg's data protection authority, but reviewed, discussed and validated by all data protection authorities in the EU. Admittedly, the decision was made three years after the complaint was filed. However, the one-stop-shop mechanism not only resulted in a fine of a dissuasive amount, but it also allowed other data protection authorities, such as the CNIL, to directly contribute to the Luxembourg investigation and to reinforce the findings of the case.[51] In addition, because the number of individuals that are impacted in a one-stop-shop procedure is higher, the amount of the fine can be higher as well, which reinforces the dissuasive effect. For instance, the one-stop-shop cooperation has also led to Meta (Facebook) being fined more than €2 billion. By way of contrast, Clearview AI, which does not have a base of operations in the EU, has been fined separately by the Greek, Italian, and French regulators in the amount of €20 million each. These amounts, although large, do not have the same dissuasive impact. Finally, the one-stop-shop system facilitates the process for the organization, which must deal with one authority only, and not with multiple jurisdictions.

It is relevant to note that the EU regulators decided in May 2022 to reinforce their close cooperation by identifying on a yearly basis a number of cross-border cases of strategic importance for which an action plan with a fixed timeline for cooperation is set. Even if some cases are not subject to the one-stop-shop (for example, if the organization does not have an EU establishment), the EU

---

47 Charlie Taylor, "Data Protection Commission 'Disappointed' at Budget Allocation" (9 October 2019), online: *Irish Times* < www.irishtimes.com/business/technology/data-protection-commission-disappointed-at-budget-allocation-1.4045248 > .

48 Bertuzzi, *supra* note 46.

49 Vincent Manancourt, "Why Europe's Hands Are Tied on TikTok" (2 September 2020), online: *Politico* < www.politico.eu/article/tiktok-europe-privacy-gdpr-complexity-ties-hands/ > .

50 Laura Kayali & Vincent Manancourt, "Amazon Fined €746M for Violating Privacy Rules" (30 July 2021), online: *Politico* < www.politico.eu/article/amazon-fined-e746m-for-violating-privacy-rules/ > .

51 Commission Nationale de l'Informatique et des Libertés (CNIL), « L'autorité luxembourgeoise de protection des données a prononcé à l'encontre d'Amazon Europe Core une amende de 746 millions d'euros » (3 August 2021), online: *CNIL* < www.cnil.fr/fr/lautorite-luxembourgeoise-de-protection-des-donnees-prononce-lencontre-damazon-europe-core-une > .

regulators may also decide to join forces on investigation and enforcement activities, and DPAs may share the work within these groups. Finally, when needed, an EDPB taskforce can be created.[52]

Finally, the European regulators also recently called upon the European Commission to develop harmonized provisions at the EU level. According to the EDPB, "this is necessary to iron out the differences in administrative procedures and practices which may have a detrimental impact on cross-border cooperation (. . .). To this end, the EDPB has drawn up a list of procedural aspects that could benefit from further harmonization at EU level. This list addresses inter alia: the status and rights of the parties to the administrative procedures; procedural deadlines; requirements for admissibility or dismissal of complaints; investigative powers of Supervisory Authorities; and the practical implementation of the cooperation procedure."[53]

Therefore, although some adjustments are needed, it is obvious that the one-stop-shop can be very beneficial for GDPR enforcement, and one may wonder whether it would be useful to import such a model of cooperation in Canada.

(d) Could the One-Stop-Shop be Implemented in Canada and, if so, What Form Would it Take?

One option for Canada as its federal and provincial private sector data protection laws move into a new era of more substantive enforcement is the adoption of some kind of one-stop-shop mechanism tailored to the Canadian context. Such a mechanism would apply to breaches that simultaneously affect multiple provinces in Canada. Thus, it would attempt to harmonize enforcement relating to the same breach that has a real and substantial connection to more than one province with its own private sector data protection law.

If the one-stop-shop were to be implemented, it could take different shapes.

(i) Option 1: A one-stop-shop mechanism similar to the GDPR

Under the GDPR, the concerned authorities are invited to express their opinions at the stage of the draft report, i.e., after the investigation has been carried out by the Lead Supervisory Authority.[54] This is probably because there are 27 European authorities, and, for the interest of the advancement of the investigation, it is preferable to let the lead supervisory authority carry out the investigation alone.

---

[52] European Data Protection Board, "DPAs Decide on Closer Cooperation for Strategic Files" (29 April 2022), online: < edpb.europa.eu/system/files/2022-10/edpb_letter_-out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf >.

[53] European Data Protection Board, Letter to Commissioner Didier Reynders (10 October 2022), online (pdf): < edpb.europa.eu/system/files/2022-10/edpb_letter_out2022-0069_to_the_eu_commission_on_procedural_aspects_en_0.pdf >.

[54] Indeed, art 60(3) of the GDPR, *supra* note 10, states that the lead supervisory authority "shall without delay submit a draft decision to the other supervisory authorities concerned for their opinion and take due account of their views."

In Canada, however, there are currently only three provincial commissioners with powers under private sector data protection laws, and the rest of the provinces are represented by the OPC. Therefore, every step of the investigation could be discussed and put to a vote. The common decisions that would need to be made would relate to (i) whether to investigate the breach, (ii) what the findings would be, and (iii) whether there should be a fine (and in what amount). Of course, insofar as not all provinces have relevant private sector legislation, the federal OPC could potentially have more voting powers, as it would act as the representative of the provinces that have no private sector legislation. If a pro-rated voting scheme were considered, attention would have to be paid to whether it would be based on the number of provinces and territories represented by the federal privacy commissioner under the CPPA, or the relative sizes of the populations. For example, the commissioners of each of Quebec, Alberta, and BC could have one vote compared to the federal commissioner's seven votes (if only provinces are counted) or ten votes (if territories are included). If population were considered, Quebec, BC, and Alberta collectively make up just short of 50% of the population of the country.[55] In cases where all commissioners were involved, each of the three provinces could have one vote, and the federal commissioner could have three. In either formula, however, the federal commissioner either has a majority of votes, or votes equal to those of the provincial commissioners combined.

Leaving aside for the moment the issue of how to weight votes, in this option, if a breach affected Canadians across different provinces, the commissioners of Quebec, BC, and Alberta would become "concerned commissioners" alongside the federal commissioner (i.e., authorities that have an interest in the outcome of the investigation because of their mission to protect the information and privacy rights of their residents).

The lead investigator (or the "lead commissioner") could be the commissioner of the province where the organization is established in Canada. The procedural law governing the case would be that of the lead commissioner's jurisdiction, and any judicial review or appeal would need to be submitted to the competent courts of that province. If the organization is headquartered in a province other than Quebec, BC, or Alberta, or is federally regulated,[56] then it

---

[55] Statistics Canada, *Population Estimates Quarterly*, Table: 17-10-0009-01 (formerly CANSIM 051-0005) (Ottawa: Statistics Canada, release date 21 December 2022), online: <www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1710000901>. https://www150.statcan.gc.ca/t1/tbl1/en/tv.action?pid=1710000901.

[56] The issue of federally regulated companies is an interesting one. These would include, for example, banks and airlines, among others. Although in theory only PIPEDA (or the CPPA) would apply to the collection, use, or disclosure of personal information by these companies, it is not inconceivable that a provincial commissioner would assert concurrent jurisdiction where the federally regulated company has collected, used, or disclosed personal information in that province. For example, in a 2014 decision, the Commission d'accès à l'information du Québec took jurisdiction over a complaint against federally regulated Rogers Communications on the basis that it was subject to the

would be the federal commissioner who would be the lead commissioner, and federal law would govern the procedure to follow.

Unlike the GDPR, the provincial laws, although substantially similar, might have important differences with the CPPA. If the privacy laws of the different provinces involved contradicted each other, the law of the "lead commissioner" would prevail because this is the law on which the organization would have designed its compliance strategy and program. However, the main issue would be the following: because the decisions in each jurisdiction are subject to review by the courts (and the federal commissioner's decisions could be appealable to a newly created Data Tribunal[57]), it is possible that the tribunal or a court will impose a different definition of a key term in one jurisdiction that is not shared in the others, given the laws and their local interpretation may diverge.

Therefore, this type of one-stop-shop mechanism would be possible to implement at the commissioner level but could theoretically result in inconsistencies if the decisions were challenged in court or before any data tribunal created by Bill C-27. Nevertheless, consensus views of multiple commissioners should carry weight in any court interpretations of key terminology, as should any clearly established one-stop-shop approach.

(ii) Option 2: A one-stop-shop mechanism where the OPC would act as the "lead regulator"

In this situation, there would be no discussions that would require a majority vote by all concerned commissioners. There could be exchanges of ideas and of opinion between privacy commissioners, but the final say/decision would be that of the OPC.

This system would have the advantage of simplicity, where the procedural law would be federal law, the applicable law would be either PIPEDA or its successor, the *Consumer Privacy Protection Act* from Bill C-27, and any appeal would be taken to the competent federal courts.

However, provincial privacy commissioners may be reluctant to agree with the OPC's interpretation/decision when the organization is in their province and when they would have been solely competent if the breach had not been a cross-provincial breach. This might be the case, for example, if a company headquartered in Quebec were responsible for a data breach that affected residents of other provinces.

In addition, such a solution would require that one or more provincial commissioners subordinate their view to the OPC. However, the federal government could not enact a law that would subordinate the provincial commissioners with respect to matters within their own jurisdiction. Therefore,

---

Quebec legislation because it carried out business in Quebec. See *X. c. Rogers Communications Inc.* (September 29, 2014), Doc. 111310 (Commission d'accès à l'information), online: < decisions.cai.gouv.qc.ca/cai/ss/fr/item/357046/index.do > .

[57] Bill C-27, *supra* note 5, s 101.

the only way such a cooperation system could be implemented would be through coordinated legislative amendments or through negotiation, where a Memorandum of Understanding would be signed between the federal and provincial governments.

(iii) Option 3: No one-stop-shop mechanism and the exclusive competence of a single authority

During the negotiations on the GDPR, there were many discussions about the possibility of implementing a centralized model, where an ad hoc authority, other than Data Protection Authorities, would be competent for the investigation and for deciding on the fine.

If this model had been implemented in the EU, that ad hoc authority would have been the European Commission, and the process would have been similar to the one adopted for the enforcement of competition regulations: the national competition authorities pool information together and mutually assist one another, but it is the European Commission that is in charge of enforcing competition laws and fining organizations that violate these regulations across Member States.

This process has led to an efficient handling of cases. For example, in 2017, Google was found guilty of breaching antitrust rules and was fined €2.4 billion, which is the largest such antitrust fine issued by the European Commission. Of course, privacy and competition regulations are quite different (although interconnected). However, the mechanism for handling complaints and for enforcing fines has the advantage of being efficient and straightforward.

This option could be the most feasible given the context of Canadian constitutional law. If this approach were adopted in Canada, one could imagine that the federal Data Tribunal would be the centralized authority making AMP decisions, with the involvement of multiple laws/commissioners. However, the main drawback would be that privacy commissioners, despite their level of expertise, would only be assisting the ad hoc authority, and this could only be done if there were a negotiated agreement between the federal government and the provinces.

(e) When the Organization has no Establishment in Canada

If the organization is not established in Canada but there is a "real and substantial connection" to Canada,[58] then the following two possibilities would apply:

---

[58] Following the decisions in *Lawson v. Accusearch Inc.*, 2007 FC 125, 2007 CarswellNat 247, 2007 CarswellNat 853 (F.C.) and *T. (A.) v. Globe24h.com*, 2017 FC 114, 2017 CarswellNat 184, 2017 CarswellNat 904 (F.C.), it is clear that PIPEDA will apply where there is a "real and substantial connection" to Canada. For a discussion of jurisdiction in the case of provincial statutes, see the orders of the Quebec, BC, and Alberta Commissioners re: Clearview AI, *supra* note 28.

a) If the affected Canadians are situated in one province alone, the commissioner of that province would conduct the investigation; or
b) If the affected Canadians are in more than one province, then the "one-stop-shop" would be launched, or there would be the exclusive competence of an ad hoc authority.

Although none of the proposed solutions is perfect, Option 1 is, in our view, the most straightforward. It is similar to the approach adopted in the EU under the GDPR and would operate in a context in which forum-shopping would be much less of a concern.

5. CONCLUSION

Significant changes to data protection enforcement in Canada are on the horizon. These changes will move Canada from a soft enforcement ombuds model to one where there is the potential for significant fines to be imposed on those who breach the law. The current legislative framework, in which both federal and provincial private sector data protection laws may apply simultaneously in certain instances, raises the potential for conflict and uncertainty when it comes to the imposition of AMPs. In this article, we have raised and framed the issues and have looked to the GDPR to see how the EU has attempted to manage situations where breaches of data protection law impact multiple jurisdictions.

Although the EU's one-stop-shop approach has been tailored specifically to the European context, it does offer a model that could be adapted in Canada. Adaptation of this model could provide a solution for an efficient and coordinated enforcement strategy by privacy commissioners in Canada. Its adaptation could take into account the fact that forum-shopping (an important concern in Europe) would be less relevant in this country, given that the discrepancies between provinces regarding corporate taxation are less significant than those between EU Member States. The details of the functioning of the one-stop-shop would remain to be discussed, but this is an issue that the federal government and its counterparts in BC, Alberta, and Quebec should be prepared to tackle.

In the first place, providing a solution will be necessary to avoid the imposition of duplicate penalties for the same breach (a kind of double jeopardy). Secondly, as there is no harmonization of procedural rules across provincial and federal jurisdictions, attention will need to be paid to how joint investigations are conducted. Informal cooperative practices developed under statutes with limited enforcement powers may not be adequate to address the procedural challenges once the financial stakes of an investigation are significantly augmented. Finally, it is not written in stone that investigations need to be joint investigations. It is conceivable that different commissioners could independently conduct investigations with respect to the same conduct. If this is the case, then the potential burden on organizations of facing multiple

investigations following different rules and procedures and different penalties must be considered.