

# Canadian Privacy Law Review

VOLUME 19, NUMBER 4

Cited as (2022), 19 C.P.L.R.

MARCH 2022

## • CANADIAN COURTS CONFIRM SIGNIFICANT LIMITS ON PRIVACY CLASS ACTIONS •

Mark Gelowitz, Partner, Céline Legendre, Partner, Robert Carson, Partner, W. David Rankin, Partner,  
Emily MacKinnon, Associate, and Lauren Harper, Associate, Osler, Hoskin & Harcourt LLP  
© Osler, Hoskin & Harcourt LLP, Toronto, Montreal, and Vancouver



**Mark Gelowitz**



**Céline Legendre**



**Robert Carson**



**W. David Rankin**

### • In This Issue •

#### CANADIAN COURTS CONFIRM SIGNIFICANT LIMITS ON PRIVACY CLASS ACTIONS

*Mark Gelowitz, Céline Legendre, Robert Carson,  
W. David Rankin, Emily MacKinnon and  
Lauren Harper* .....57

#### CANADA'S ANTI-SPAM LEGISLATION – 2021 YEAR IN REVIEW

*Bradley Freedman*.....62

#### CLEARVIEW AI ORDERED TO COMPLY WITH PROVINCIAL REGULATORS' PRIVACY RECOMMENDATIONS

*Kristen Pennington, Julia Loney, Robbie Grant  
and Kristen Shaw* .....64

#### THE OPC PUBLISHES ITS 2020-2021 ANNUAL REPORT – “PROJECTING OUR VALUES INTO LAWS: LAYING THE FOUNDATION FOR RESPONSIBLE INNOVATION”

*Amy Quackenbush and Theo Ling* .....66



**Emily MacKinnon**



**Lauren Harper**

**F**or businesses operating in Canada, 2021 brought welcome guidance: courts across the country repeatedly exercised their gatekeeping role to put a stop to privacy class actions that lack evidence of harm to the proposed class members. In other words, a class action should not automatically follow from a data breach or incident. Even when a class action does follow, defendants have a variety of tools to defend privacy claims or to resolve them early on.

## CANADIAN PRIVACY LAW REVIEW

**Canadian Privacy Law Review** is published monthly by LexisNexis Canada Inc., 111 Gordon Baker Road, Suite 900, Toronto ON M2H 3R1 by subscription only.

All rights reserved. No part of this publication may be reproduced or stored in any material form (including photocopying or storing it in any medium by electronic means and whether or not transiently or incidentally to some other use of this publication) without the written permission of the copyright holder except in accordance with the provisions of the *Copyright Act*. © LexisNexis Canada Inc. 2022

ISBN 0-433-44419-3 (print) ISSN 1708-5446

ISBN 0-433-44652-8 (PDF) ISSN 1708-5454

ISBN 0-433-44420-7 (print & PDF)

Subscription rates: \$395.00 per year (print or PDF)  
\$600.00 per year (print & PDF)

Please address all editorial inquiries to:

### General Editor

Professor Michael A. Geist  
Canada Research Chair in Internet and E-Commerce Law  
University of Ottawa, Faculty of Law  
E-mail: mgeist@uottawa.ca

### LexisNexis Canada Inc.

Tel. (905) 479-2665  
Fax (905) 479-2826  
E-mail: cplr@lexisnexis.ca  
Web site: www.lexisnexis.ca

## ADVISORY BOARD

• Ann Cavoukian, former Information and Privacy Commissioner of Ontario, Toronto • David Flaherty, Privacy Consultant, Victoria • Elizabeth Judge, University of Ottawa • Christopher Kuner, Hunton & Williams, Brussels • Suzanne Morin, Sun Life, Montreal • Bill Munson, Toronto • Stephanie Perrin, Service Canada, Integrity Risk Management and Operations, Gatineau • Patricia Wilson, Osler, Hoskin & Harcourt LLP, Ottawa

**Note:** This review solicits manuscripts for consideration by the Editors, who reserves the right to reject any manuscript or to publish it in revised form. The articles included in the *Canadian Privacy Law Review* reflect the views of the individual authors and do not necessarily reflect the views of the advisory board members. This review is not intended to provide legal or other professional advice and readers should not act on the information contained in this review without seeking specific independent advice on the particular matters with which they are concerned.



## THE “SOME BASIS IN FACT” REQUIREMENT IS A MEANINGFUL SCREENING DEVICE

Several decisions reinforced that certification is meant to be a meaningful screening device in privacy class actions:

- In *Simpson v. Facebook, Inc.*,<sup>1</sup> the plaintiff alleged that a third party named Cambridge Analytica had obtained information about Facebook users from a third-party application developer. The Ontario Superior Court of Justice dismissed the plaintiff’s certification motion on the basis that there was no evidence that any Canadian user’s data was shared with Cambridge Analytica (and therefore no justification for a class proceeding). Justice Belobaba emphasized the Court’s gatekeeping role, stating, “The dismissal of this certification motion is simply a reminder to class counsel that while certification remains a low hurdle it is nonetheless a hurdle.” Similarly, in *Kish v. Facebook, Inc.*,<sup>2</sup> the Court of Queen’s Bench for Saskatchewan dismissed another application for class certification that was premised on allegations related to Cambridge Analytica. Justice Keene built on the growing trend of cases emphasizing the Court’s gatekeeping role at the certification stage, including *Simpson* and *Setoguchi v. Uber* (discussed below). Osler acted for Facebook in both cases. Further information is set out in our Osler Updates on these two certification decisions, Ontario Superior Court denies certification of Cambridge Analytica class action and Another Canadian court denies certification of Cambridge Analytica class action.<sup>3</sup>
- Similarly, in *Beaulieu c. Facebook Inc.*,<sup>4</sup> the Québec Superior Court held that the plaintiff did not satisfy her burden at the authorization stage (Québec’s equivalent of the certification stage) to establish an “arguable case.” Justice Courchesne found that the plaintiff’s allegations – that Facebook’s tools allowed employers and companies to illegally exclude certain users from employment and housing opportunities – were

“hypothetical and speculative.” Osler acted for Facebook in this case as well.

In all three cases, the plaintiffs launched, or sought to launch, appeals. In *Kish*, however, the Court of Appeal for Saskatchewan recently dismissed the plaintiff’s motion seeking leave to appeal, finding that the plaintiff’s proposed appeal lacked sufficient merit to be heard by a panel of the Court of Appeal. The appeal decisions in the other two cases will likely be released in 2022.

#### PLAINTIFFS MUST SHOW SOME EVIDENCE OF HARM

Other decisions confirmed that plaintiffs must show evidence of actual harm in order to obtain certification and to succeed on the merits of a proceeding alleging privacy violations. This requirement presented a serious hurdle for plaintiffs in data breach class actions:

- In *Setoguchi v. Uber*,<sup>5</sup> the Court of Queen’s Bench of Alberta denied certification of a proposed class action arising out of an alleged data breach involving Uber. There was no evidence that the hacker used any personal data obtained in the breach to anyone’s detriment. Justice Rooke found no evidence of any real (not *de minimis*) harm; there was only “speculation about a **future possibility** of loss or harm” (emphasis in original). The court also distinguished “minor and transient upset” from “compensable injury.” Justice Rooke observed that without evidence of compensable loss, “a class proceeding could be a mere ‘fishing trip’ based on speculation, without any evidence of fish being present.”
- In March 2021, the Québec Superior Court released its decision in the first privacy class action in Canada to be determined (and dismissed) on the merits. In *Lamoureux v. IIROC*,<sup>6</sup> the plaintiff alleged that an inspector working at the Investment Industry Regulatory Organization of Canada (IIROC) lost a laptop containing information about thousands of Canadians. The

laptop was never found. Justice Lucas dismissed the action finding that, while it is not necessary for class members to have actually fallen victim to identity theft in order to recover, injury beyond general inconvenience must be proven. Given the lack of documentary or medical evidence proving the extent of the damages, the Court categorized the class members’ fears and worries as general inconveniences. Justice Lucas also dismissed the claim for punitive damages, finding that IIROC acted diligently and implemented appropriate response measures when the loss came to light. The focus on the absence of compensable harm aligns with recent authority from the common law provinces, including *Setoguchi*. Further information is set out in our blog post First merits decision dismissing privacy class action in Canada on the *Lamoureux* decision.<sup>7</sup>

#### LIMITS ON INTRUSION UPON SECLUSION CLAIMS AGAINST DATABASE DEFENDANTS

In 2021, the Ontario Divisional Court held that a necessary element of the tort of intrusion upon seclusion is that the defendant itself *committed* the intrusion. The tort does not apply where a defendant merely failed to prevent an intrusion by a third party. In *Owsianik v. Equifax Canada Co.*,<sup>8</sup> the plaintiff alleged that a third-party hacker infiltrated Equifax’s database exposing personal information about thousands of consumers. A class action was initially certified. However, on appeal, a majority of the Divisional Court held that a claim for intrusion upon seclusion could not succeed against Equifax since *an intrusion* is “the central element of the tort” and Equifax did not intrude.

The Divisional Court’s decision marks an important development in Canadian privacy law and reaffirms that certification judges should refuse to certify causes of action that are bound to fail. (A further appeal is being pursued by the plaintiff to the Court of Appeal and will be monitored with interest.)

## PRE-CERTIFICATION MOTIONS IN PRIVACY CASES

Recent decisions have also confirmed that pre-certification motions may be appropriate to resolve privacy actions on their merits. In *Schmidt v. LinkedIn Corporation*,<sup>9</sup> the B.C. Supreme Court granted leave for the defendant to have its summary trial application determined in advance of certification. The plaintiff alleged that LinkedIn's iOS app surreptitiously read and stored the contents of users' clipboards. But the plaintiff presented no evidence supporting those allegations. LinkedIn sought, and the Court granted, an opportunity to disprove these speculative factual allegations at a pre-certification summary trial. Likewise, in *Cronk v. LinkedIn Corporation*,<sup>10</sup> the B.C. Supreme Court accepted LinkedIn's argument that the defendant's summary trial application should be heard concurrently with certification. The plaintiff alleged that LinkedIn violated privacy legislation by showing users their own names and profile pictures in customized "dynamic ads." LinkedIn sought to defend the case on its merits at an early stage, including on the basis that showing someone their own name and photo is not a breach of privacy. The Court agreed that a summary trial had the potential to conclusively determine the core issues in the case at an early stage. Osler acted for LinkedIn in both cases.

Both *Schmidt* and *Cronk* were B.C. cases and therefore did not address recent amendments to the *Class Proceedings Act, 1992*<sup>11</sup> in Ontario, which expressly encourage pre-certification motions that could promptly resolve, or significantly narrow, putative class proceedings. Both cases are consistent with the B.C. Court of Appeal's subsequent decision in *British Columbia v. The Jean Coutu Group (PJC) Inc.*<sup>12</sup> The Court of Appeal rejected older case law that established a presumption that certification should be the first procedural matter to be heard. The Court's new framework for sequencing pre-certification applications will likely expand the opportunities for defendants in privacy cases to argue summary trial applications either before or

concurrently with certification, thereby providing a means for finally disposing of the action at an early stage.

## CONCLUSIONS

It remains critical for businesses to respond quickly and effectively when data incidents occur; however, businesses should be heartened by this year's developments. Despite the proliferation of privacy class action filings over the last decade, courts across Canada are making it clear that certification is not a rubber stamp. And courts have confirmed that businesses facing privacy class actions have a range of effective tools to defend privacy claims. Osler is at the forefront of these developments and will continue to report as the law regarding privacy class actions matures.

*[Mark Gelowitz is a key contact for the firm's Corporate and Securities Litigation Group. Mark has a business-focused civil and securities litigation, appellate and international commercial arbitration practice. His practice covers a wide variety of issues in corporate and commercial law including mergers and acquisitions litigation, director and officer liability, corporate governance, shareholder disputes, oppression, privacy, libel and slander, real estate lease disputes, mining litigation and class actions.]*

*Céline Legendre is a partner in the firm's National Litigation group, based in Montréal. Céline's practice focuses on civil and commercial litigation, including class actions, privacy, product liability, corporate and securities litigation, directors' and officers' litigation, shareholders' remedies and professional liability. Céline also advises clients on competition and antitrust issues relating to deceptive marketing and alleged cartel activity, internal investigations and wrongful disclosure.*

*Robert Carson has a broad litigation practice with particular emphasis on corporate and securities litigation and class action defence. Robert has experience defending securities, consumer, competition and product liability class actions. His*

practice also includes mergers and acquisitions litigation, director and officer liability, shareholder disputes, valuation proceedings, oppression claims, Ontario Securities Commission proceedings, and insolvency and restructuring matters.

**W. David Rankin** carries on a general commercial litigation practice which includes appellate litigation, administrative and constitutional litigation, class actions, employment/wrongful dismissal litigation, and other general civil litigation. David has appeared as counsel before the Supreme Court of Canada on ten separate occasions. David is a co-author of *Sopinka and Gelowitz on the Conduct of an Appeal*, 4th Edition, a leading resource for litigators and judges on appellate practice and procedure.

**Emily MacKinnon** is a litigator in Vancouver, BC. Her practice includes high-level commercial disputes as well as constitutional and public law matters. An experienced oral advocate, Emily has argued at the Supreme Court of Canada and at all levels of court in British Columbia, Manitoba, Alberta, and Ontario. As a trusted advisor to her clients, Emily provides practical advice on company law disputes and regulatory matters.

**Lauren Harper** is an associate in Osler's Litigation Group. She maintains a general civil and commercial litigation practice. Lauren obtained her J.D. at the University of Toronto. Prior to law school, she received her Bachelor of Science (Honours) in Life

Sciences with a minor in Psychology from Queen's University.]

- <sup>1</sup> [2021] O.J. No. 726, 2021 ONSC 968 (Ont. S.C.).
- <sup>2</sup> [2021] S.J. No. 339, 2021 SKQB 198 (Sask. Q.B.).
- <sup>3</sup> Mark Gelowitz, Robert Carson, and Lauren Harper, "Ontario Superior Court Denies Certification of Cambridge Analytica Class Action" (18 February 2021), online: Osler <<https://www.osler.com/en/resources/critical-situations/2021/ontario-superior-court-denies-certification-of-cambridge-analytica-class-action>>; Mark Gelowitz, Robert Carson, and Lauren Harper, "Another Canadian Court Denies Certification of Cambridge Analytica Class Action (21 July 2021), online: Osler <<https://www.osler.com/en/resources/regulations/2021/another-canadian-court-denies-certification-of-cambridge-analytica-class-action>>.
- <sup>4</sup> [2021] Q.J. No. 8599, 2021 QCCS 3206 (Qu. S.C.).
- <sup>5</sup> [2021] A.J. No. 22, 2021 ABQB 18 (Alta. Q.B.).
- <sup>6</sup> [2021] J.Q. No. 27662021 QCCS 1093 (Qu. S.C.).
- <sup>7</sup> Deborah Glendinning, Lauren Tomasich, and Jessica Harding, "First Merits Decision Dismissing Privacy Class Action in Canada" (19 April 2021), online: Osler <<https://www.osler.com/en/blogs/classactions/april-2021/first-merits-decision-dismissing-privacy-class-action-in-canada>>.
- <sup>8</sup> [2021] O.J. No. 3171, 2021 ONSC 4112 (Ont. S.C.).
- <sup>9</sup> [2021] B.C.J. No. 845, 2021 BCSC 739 (B.C.S.C.).
- <sup>10</sup> [2021] B.C.J. No. 844, 2021 BCSC 738 (B.C.S.C.).
- <sup>11</sup> S.O. 1992, c. 6.
- <sup>12</sup> [2021] B.C.J. No. 1202, 2021 BCCA 219 (B.C.C.A.).

---



---

## ELECTRONIC VERSION AVAILABLE

**A PDF version of your print subscription is available for an additional charge.**

**A PDF file of each issue will be e-mailed directly to you 12 times per year, for internal distribution only.**

---



---

• CANADA’S ANTI-SPAM LEGISLATION – 2021 YEAR IN REVIEW •

Bradley Freedman, Partner, Borden Ladner Gervais LLP

© Borden Ladner Gervais LLP, Vancouver



**Bradley Freedman**

In 2021, the Supreme Court of Canada refused to hear a challenge to the constitutional validity of *Canada’s Anti-Spam Legislation*<sup>1</sup> (commonly known as “CASL”), and the Canadian Radio-television and Telecommunications Commission issued two CASL enforcement decisions.

CASL

CASL creates a comprehensive regime of offences, enforcement mechanisms and potentially severe penalties designed to prohibit the sending of unsolicited commercial electronic messages (CEMs), the unauthorized commercial installation and use of computer programs on another person’s computer system and other forms of online fraud. Following are some key aspects of CASL:

- CASL creates an opt-in regime that prohibits, subject to limited exceptions, the sending of a CEM unless the recipient has given consent (express or implied in limited circumstances) to receive the CEM and the CEM complies with prescribed formalities (e.g., information about the sender and an effective and promptly implemented unsubscribe mechanism).
- CASL also prohibits, subject to limited exceptions, the installation and use of a computer program on another person’s computer system, in the course of a commercial activity, without the express

consent of the owner or authorized user of the computer system.

- CASL imposes liability on organizations and individuals (including corporate directors and officers) for direct and indirect/vicarious CASL violations. CASL provides a due diligence defence.
- CASL violations can result in regulatory penalties of up to \$10 million per violation for an organization and \$1 million per violation for an individual. CASL includes a private right of action that is not in force.

The Canadian Radio-television and Telecommunications Commission (CRTC) enforces CASL’s rules regarding CEMs and computer programs. Since CASL came into force in 2014, the CRTC has taken enforcement action against organizations and individuals who have violated CASL and issued enforcement decisions and accepted voluntary undertakings (settlements).

SUPREME COURT OF CANADA DECISION – COMPUFINDER APPEAL

In March 2021, the Supreme Court of Canada declined<sup>2</sup> to hear an appeal by CompuFinder from a Federal Court of Appeal decision<sup>3</sup> confirming the constitutional validity of CASL and providing important guidance regarding the interpretation of CASL’s rules for sending CEMs.<sup>4</sup>

CRTC ENFORCEMENT

In March 2021, the CRTC announced<sup>5</sup> and published a notice of violation<sup>6</sup> imposing a \$75,000 penalty on an individual for conducting high-volume spam campaigns without consent in violation of CASL’s CEM rules. The \$75,000 penalty is the

largest penalty imposed to date on an individual spammer.<sup>7</sup>

In December 2021, the CRTC announced<sup>8</sup> and published an undertaking<sup>9</sup> by an international retailer to voluntarily settle alleged CASL violations regarding the sending of promotional emails without consent and in some instances without a CASL-compliant unsubscribe mechanism. As part of the undertaking, the retailer agreed to pay a \$200,000 penalty and implement a CASL compliance program.

[*Bradley Freedman focuses his practice on cybersecurity/data protection, privacy, information technology, intellectual property, internet/e-commerce and related matters. He is recognized as a leading lawyer in these areas of law by the foremost legal rankings publications. He advises clients in negotiating, structuring and documenting transactions and business arrangements, and acts as counsel in litigation, arbitration and mediation. He has appeared before the Supreme Court of British Columbia, the British Columbia Court of Appeal, the Federal Court of Canada, the Federal Court of Appeal, the Trademarks Opposition Board, and international commercial arbitration tribunals.*]

---

<sup>1</sup> *An Act to Promote the Efficiency and Adaptability of the Canadian Economy by Regulating Certain Activities that Discourage Reliance on Electronic Means of Carrying out Commercial Activities, and to Amend the Canadian Radio-television and Telecommunications Commission Act, the Competition Act, the Personal Information Protection and Electronic Documents Act and the Telecommunications Act*, S.C. 2010, c. 23.

<sup>2</sup> *3510395 Canada Inc. v. Attorney General of Canada*, [2020] S.C.C.A. No. 370 (S.C.C.).

<sup>3</sup> *3510395 Canada Inc. v. Canada (Attorney General)*, [2020] F.C.J. No. 674, 2020 FCA 103 (F.C.A.).

<sup>4</sup> For more information, see Bradley Freedman, “Federal Court of Appeal Rules CASL Constitutionally Valid and Provides Interpretive Guidance” (2 July 2020), online: Borden Ladner Gervais LLP <<https://www.blg.com/en/insights/2020/07/federal-court-of-appeal-rules-casl-constitutionally-valid-and-provides-interpretive-guidance>>.

<sup>5</sup> Canadian Radio-television and Telecommunications Commission, News Release, “CRTC Issues Largest Ever Penalty to an Individual for Sending Messages Without Consent” (29 March 2021) online: <<https://www.canada.ca/en/radio-television-telecommunications/news/2021/03/crtc-issues-largest-ever-penalty-to-an-individual-for-sending-messages-without-consent.html>>.

<sup>6</sup> Canadian Radio-television and Telecommunications Commission, Notice of Violation: Scott William Brewer, 9110-2018-00509 (29 March 2021) online: <<https://crtc.gc.ca/eng/archive/2021/vt210329.htm>>.

<sup>7</sup> For more information, see Bradley Freedman, “CASL Enforcement – \$75,000 Penalty Imposed on Individual Spammer” (31 March 2021), online: Borden Ladner Gervais LLP <<https://www.blg.com/en/insights/2021/03/casl-enforcement-75k-penalty-imposed-on-individual-spammer>>.

<sup>8</sup> Canadian Radio-television and Telecommunications Commission, News Release, “Gap Inc. Agrees to pay \$200,000 for Allegedly Violating Canada’s Anti-Spam Legislation” (8 December 2021) online: <<https://www.canada.ca/en/radio-television-telecommunications/news/2021/12/gap-inc-agrees-to-pay-200000-for-allegedly-violating-canadas-anti-spam-legislation.html>>.

<sup>9</sup> Canadian Radio-television and Telecommunications Commission, Undertaking: Gap Inc., **9110-2021-00605** (6 December 2021) online: <<https://crtc.gc.ca/eng/archive/2021/ut211206.htm>>.

• CLEARVIEW AI ORDERED TO COMPLY WITH PROVINCIAL REGULATORS’ PRIVACY RECOMMENDATIONS •

Kristen Pennington, Partner, Julia Loney, Partner, Robbie Grant, Associate, and Kristen Shaw, Articled Student, McMillan LLP

© McMillan LLP, Toronto, Calgary, and Vancouver



**Kristen Pennington**



**Julia Loney**



**Robbie Grant**



**Kristen Shaw**

**F**ollowing an investigation by privacy regulators in 2020,<sup>1</sup> Clearview AI (“Clearview”) has ceased offering its facial recognition services in Canada. However, it has not stopped collecting images of Canadians, nor has it deleted the images it already collected. Now, Canada’s provincial privacy regulators have issued legally binding orders against Clearview forcing it to do just that.

**BACKGROUND**

In February 2020, the federal Office of the Privacy Commissioner of Canada (the “OPC”) and the provincial privacy regulators in British Columbia, Alberta and Québec (collectively, the “Commissioners”) launched a joint investigation into a US-based technology company, Clearview.

Clearview has developed a program that gathers images of individuals from across the internet (including from public social media pages), analyzes the images for biometric data, and compiles them into its database. Clearview then markets a search tool that allows its users to search the database using an image of a face, and receive in return images of that face found from across the web. Clearview has sold its tool to law enforcement agencies, as well as private sector entities.

In February 2021, the Commissioners issued a report (the “Report”) finding that Clearview breached

federal and provincial private sector privacy laws by collecting online images of individuals in Canada without their knowledge or consent. More information on the Report can be found here.<sup>2</sup>

The Report included non-binding recommendations that Clearview:

- a. stop offering its facial recognition services in Canada;
- b. stop collecting, using, and disclosing images and biometric information of Canadians; and
- c. delete images and biometric facial information collected from Canadians

(collectively, the “Recommendations”).

**THE ORDERS**

Clearview advised the Commissioners that it had complied with the first recommendation in July 2020. However, as of December 2021, Clearview had not deleted or stopped processing the images and biometric information of Canadians.

Accordingly, the Commissioners (with the exception of the OPC) have now ordered Clearview to comply with the Recommendations as they relate to British Columbia, Alberta and Québec.<sup>3</sup>

The Office of the Information and Privacy Commissioner of Alberta provided a timeline, stating



that Clearview must report on its good faith steps to comply with the Recommendations within 50 days of the order.<sup>4</sup> Similarly, the Commission d'accès à l'information du Québec ordered that Clearview destroy all images and biometric identifiers collected without consent within 90 days of the order.<sup>5</sup>

Clearview can seek judicial review, meaning it can ask the appropriate provincial court(s) to reconsider and overturn the order(s). However, if the orders are not overturned on review, Clearview could be subject to monetary penalties for non-compliance.

### WHAT DOES THIS MEAN?

The orders highlight the active role the Commissioners are willing to take in following up on reports and investigations. If the Commissioners are ultimately granted broader enforcement mechanisms by proposed legislative changes, this role is likely to expand.

The OPC took this announcement as an opportunity to comment on the gaps in existing federal privacy legislation, noting that it currently does not have order-making powers under the *Personal Information Protection and Electronic Documents Act* ("PIPEDA") and must instead refer evidence of the commission of an offence to the Attorney General of Canada, who is responsible for any prosecution. The result is that individuals in provinces other than British Columbia, Alberta and Québec are not protected by the provincial regulators' orders to Clearview. The OPC therefore called for amendments to strengthen the enforcement mechanisms in PIPEDA, including by providing the OPC the ability to issue orders and impose monetary penalties, noting that similar recommendations have been proposed in British Columbia, and Ontario, and adopted in Québec.<sup>6</sup>

Finally, the investigation into Clearview AI's services, and the resulting Recommendations and orders, speak to the importance of assessing the privacy law implications of new products, services and initiatives early in their development and prior to their implementation. Failure to design and implement offerings in a manner that complies with Canada's patchwork of privacy legislation can lead to privacy

regulators' intervention and/or civil liability, as well as the costs of redesigning or scrapping offerings that are found not to be privacy compliant.

### A CAUTIONARY NOTE

The foregoing provides only an overview and does not constitute legal advice. Readers are cautioned against making any decisions based on this material alone. Rather, specific legal advice should be obtained.

*[Kristen Pennington is a Partner in the Privacy & Data Protection Group of McMillan LLP. Kristen counsels clients on the privacy law implications of new products, technologies, initiatives and corporate transactions. She also helps organizations develop privacy compliance programs and drafts privacy policies and privacy and data protection terms in an array of commercial agreements. She can be reached at Kristen.Pennington@mcmillan.ca.]*

*Julia Loney is a Partner in the Regulatory Group with McMillan LLP in Calgary, with a focus on commercial arrangements and transactions, corporate governance and compliance, and regulatory issues in project development. She provides strategic regulatory advice on consumer issues, and Alberta and Saskatchewan privacy matters, including access requests, legal requirements and risk assessments, and developing compliance programs and policies and consent forms. She can be reached at Julia.loney@mcmillan.ca.]*

*Robbie Grant is an Associate in the Regulatory Group with McMillan LLP in Toronto, with a focus on privacy and data protection. He frequently assists in drafting and reviewing privacy policies, responding to data breaches, and advising on the privacy law dimension of business practices and transactions. He can be reached at Robbie.grant@mcmillan.ca.]*

*Kristen Shaw is an Articled Student in the Vancouver office of McMillan LLP with a particular interest in regulatory and litigation matters. Kristen is enjoying a varied articling experience including a secondment to a BC-based mining company. After having written an extensive paper on smart home technology in law school, Kristen has a passion for*

assisting in privacy matters. She can be reached at [kristen.shaw@mcmillan.ca](mailto:kristen.shaw@mcmillan.ca).]

<sup>1</sup> Robert C. Piasentin and Grace Shaw, “Big Brother’s Access Limited – Canadian Privacy Commissioners Rule Clearview AI’s Facial Recognition Tool in Breach of Canadian Privacy Laws” (17 February 2021), online: McMillan LLP <<https://mcmillan.ca/insights/access-denied-canadian-privacy-commissioners-rule-clearview-ais-facial-recognition-tool-in-breach-of-canadian-privacy-laws/>>.

<sup>2</sup> Robert C. Piasentin and Grace Shaw, “Big Brother’s Access Limited – Canadian Privacy Commissioners Rule Clearview AI’s Facial Recognition Tool in Breach of Canadian Privacy Laws” (17 February 2021), online: McMillan LLP <<https://mcmillan.ca/insights/access-denied-canadian-privacy-commissioners-rule-clearview-ais-facial-recognition-tool-in-breach-of-canadian-privacy-laws/>>.

<sup>3</sup> Office of the Privacy Commissioner of Canada. News Release. *Clearview AI ordered to comply with recommendations to stop collecting, sharing images*. (14 December 2021), online: Office of the Privacy Commissioner of Canada.

<sup>4</sup> Office of the Information and Privacy Commissioner of Alberta. News Release. *Announcement: Clearview AI Ordered to Comply with Alberta’s Privacy Law*. (14 December 2021), online: Office of the Information and Privacy Commissioner of Alberta.

<sup>5</sup> Commission d’accès à l’information du Québec. News Release. *La Commission ordonne à Clearview AI de cesser ses pratiques de reconnaissance faciale non conformes*. (14 December 2021), online: Newswire.

<sup>6</sup> Robert C. Piasentin, Gurb Dhalwal, and Yue Fei, “Special Committee Releases Report Suggesting Changes to Modernize BC’s Privacy Sector Privacy Law” (14 December 2021), online: McMillan LLP <<https://mcmillan.ca/insights/special-committee-releases-report-suggesting-changes-to-modernize-bcs-private-sector-privacy-law/>>; Lyndsay A. Wasser and Kristen Pennington, “Is Privacy Sector Privacy Legislation Looming in Ontario?” (5 July 2021), online: McMillan LLP <<https://mcmillan.ca/insights/is-private-sector-privacy-legislation-looming-in-ontario/>>; Rish Handa, “Bill 64 Enacted: Quebec’s Modern Privacy Regime” (15 October 2021), online: McMillan LLP <<https://mcmillan.ca/insights/bill-64-enacted-quebecs-modern-privacy-regime/>>.

## • THE OPC PUBLISHES ITS 2020-2021 ANNUAL REPORT – “PROJECTING OUR VALUES INTO LAWS: LAYING THE FOUNDATION FOR RESPONSIBLE INNOVATION” •

Amy Quackenbush, Information Governance Specialist, and Theo Ling, Partner,  
Baker & McKenzie LLP  
© Baker & McKenzie LLP, Toronto



**Amy Quackenbush**



**Theo Ling**

In December 2021, the Office of the Privacy Commissioner of Canada (OPC), published its annual report, titled *Projecting Our Values into Laws: Laying the Foundation for Responsible Innovation*.<sup>1</sup> The report marks the last under the current Privacy

Commissioner of Canada, Daniel Therrien whose mandate will come to a close in June 2022.

In the report the OPC highlights the need for a strengthened privacy framework that allows Canadians to participate safely in the digital economy where there is an increasing dependence on the value of data and new technologies. While economic growth and privacy protection are not conflicting values, the OPC cautions that responsible use of Canadian’s personal information is paramount as we move into a sustainable post-pandemic economy. This requires a regulatory framework that reflects Canadian values and ensures the benefits of participating in the digital

space do not come at the expense of individual's rights. To help achieve this, the OPC calls for a move away from the model of self-regulation, to a model of true regulation with "objective and knowable standards adopted democratically, [and] enforced by democratically appointed institutions".

Building on identified inadequacies of the previously tabled *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* (Bill C-11), the report highlights key issues the OPC wants to see addressed in the modernization of Canada's federal privacy laws, including:

1. *Enable responsible innovation* – define permissible uses of data so as to both enable responsible innovation and protect the rights and values of citizens;
2. *Adopt a rights-based framework* – provide organizations with greater flexibility to use personal information, including without consent for legitimate business interests, within a legal framework where privacy is entrenched as a human right;
3. *Increase corporate accountability* – clearly define the accountability principle, and provide protective measures such that corporate accountability is real and demonstrable;
4. *Adopt similar principles in public and private sectors laws* – given the increased reliance on public-private partnerships, common privacy principles enshrined in both public and private sector privacy laws would help address gaps in accountability where the sectors interact;
5. *Ensure Canadian laws are interoperable, internationally and domestically* – help to facilitate and regulate trans-boarder data flows and reassure citizens that their personal information is subject to similar protections across and outside of Canada. It also benefits organizations by reducing compliance costs and increasing competitiveness; and
6. *Adopt quick and effective remedies and increased authority of the OPC* – includes giving the OPC

the authority to make legally binding orders against offenders and to impose meaningful monetary penalties where warranted.

The report also highlights the importance of considering artificial intelligence (AI) in the modernization of Canada's federal privacy laws, and points to the public consultation undertaken by the OPC in November 2020. Key recommendations from this included creating the right to meaningful explanation for automated decisions and the right to contest those decisions, as well as requiring organizations to design AI systems from their conception in a way that protects privacy and human rights.

While many of the themes and desired outcomes highlighted in the 2020-2021 annual report are not new, there appears to be a renewed tone of optimism that the Canadian Parliament will be working to enact long overdue updates to Canada's privacy laws in the near future.

*[Amy Quackenbush is an Information Governance Specialist with the global Information Governance group within Baker McKenzie's Information Technology & Communications Practice in Canada. She holds a Masters of Information and a CIPP/C certification, and has a background in records and information management, knowledge management, and user experience design. She helps advise clients on information governance matters relating to records and data retention, data privacy and localization, cross-border transfer, media/format, and digital transformation.*

*Theo Ling heads Baker McKenzie's Canadian Information Technology/Communications practice and is a member of the Firm's Global IP/Technology Practice Group, and Technology, Media & Telecoms and Financial Institutions Industry Groups. Theo is ranked by several legal directories, including Chambers Canada, where he is described as "a knowledgeable technology lawyer, with a practical, 'can-do' attitude who is excellent at getting things done." Named by the Financial Times as one of the Top Ten Most Innovative Lawyers in North America, Theo founded the legal industry's first global legal innovation lab focused on multidisciplinary*

*collaboration and serves on the Firm's Global Innovation Committee.]*

---

<sup>1</sup> Office of the Privacy Commissioner of Canada, "Laying the Foundation for Responsible Innovation:

2020-2021 Annual Report to Parliament on the *Privacy Act* and the *Personal Information Protection and Electronic Documents Act*", online: <[https://www.priv.gc.ca/en/opc-actions-and-decisions/ar\\_index/202021/ar\\_202021/](https://www.priv.gc.ca/en/opc-actions-and-decisions/ar_index/202021/ar_202021/)>.