IADC COMMITTEE NEWSLETTER

# CYBER SECURITY, DATA PRIVACY AND TECHNOLOGY

*June 2022*

### IN THIS ISSUE

*"As society complexifies, and as technologies evolve, our collective relationship with data and privacy has complexified and evolved as well. Each new year seems to bring with it ever more perplexing dilemmas around privacy, and to awkwardly juxtapose an ever more contrasting cast of public interests and societal norms against novel privacy risks and our expectations regarding their mitigation"*

*– The Honourable Nicole Duval Hesler, former Chief Justice of Quebec*

## Public-Sector Personal Information Class Actions in Canada

### ABOUT THE AUTHORS

**Shaun E. Finn** is the co-leader of BCF LLP's Class Action Defence Group and a partner in the firm's Montreal-based litigation department. Shaun's class action work involves the representation of corporate and institutional defendants in the areas of product liability, consumer protection, privacy, securities, and mass torts, among others. Shaun has been cited by courts including the Supreme Court of Canada. In addition to writing widely on class actions (in English and French), he also teaches a course on the subject at the McGill Faculty of Law. He can be reached at Shaun.Finn@bcf.ca.

**Danielle Miller Olofsson** is a senior associate in the Corporate Group at Stikeman Elliott. Her practice focuses on all matters relating to privacy and data protection and she is particularly well versed in issues relating to new technologies, such as artificial intelligence and blockchain. Danielle is an International Association of Privacy Professionals Certified Expert in Canadian and European data protection and is also certified in privacy program management. She can be reached at DMillerOlofsson@stikeman.com.

### ABOUT THE COMMITTEE

Corporations and law firms around the world are constantly dealing with cybersecurity, data privacy and other important technology issues, both in business and, where available, in litigation discovery. Burgeoning technologies are placing new and increasing demands on in house and outside lawyers and their clients. All are being challenged to meet new and strict data privacy and security guidelines and the consequences for failing to meet these requirements can be devastating. The Cyber Security, Data Privacy and Technology Committee will address the differing substantive laws globally in these areas, and be of interest to many other committees whose members and activities are impacted by technology. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

**Avanti D. Bakane**
Vice Chair of Publications
Gordon & Rees, LLP
abakane@grsm.com

*[1]

## I. Introduction

As with any right, the right to privacy is not absolute. Its definition is frequently fluid, and a successful defence of this right depends on the context, the parties involved, and any other rights with which it may interact. Nowhere is this more evident than in the public sector where the state's right to collect, use, and disclose information (collectively to "Process") – be it for reasons of law enforcement, public health and safety, or the administration of government programs – may potentially conflict with the right of individuals to protect the aspects of their lives that are intimately linked to their biographical core. When the state fails to respect the limit between where its rights end and those of the individual begin, its institutions may be called to defend their actions either against a single plaintiff or, in the case of class actions, against a large number of putative members.

A class action is a civil procedure that allows a person to seek leave to sue a defendant on behalf of other, similarly situated individuals who have allegedly suffered harm as a result of a common act or omission. Because such a procedure does not require the consent of the putative class members, the would-be representative must satisfy the court that the proposed class action should be allowed to proceed on the merits. This preliminary form of procedural filtering is known as "certification" in common law jurisdictions and "authorization" in Québec. Because privacy incidents – notably breaches and malicious cyberattacks – can compromise the personal information ("Personal Information") of thousands and even millions of people, they naturally lend themselves to common, class-wide treatment. As the case law demonstrates, however, evidence of a breach is generally not enough to ground liability. The plaintiff must demonstrate at certification/authorization, and prove on the merits, that the allegedly wrongful act or omission of the defendant caused the class members to sustain a compensable injury. Because Canadian class action regimes, like Canadian privacy and Personal Information protection regimes, constitute a legislative patchwork, context and jurisdiction are important factors in assessing the litigation risks to which public sector defendants may be exposed, as well as the nature and scope of the damages they could be ordered to pay.

[1] Shaun E. Finn is a partner in BCF LLP's Litigation Group and Co-Leader of the Class Action Defence Group. Danielle Miller Olofsson, PhD, is a senior associate in the Corporate Group of Stikeman Elliott LLP's Montreal office and was Chief Access to Information and Privacy at a major Quebec-based utility company. Finn and Olofsson co-authored Privacy and Data-Protection Class Actions in Canada: A Practical Handbook (Toronto: Thomson Reuters, 2020). This article is based in part on a new manuscript written by the same authors and tentatively entitled In the Public Eye: Privacy, Personal Information, and High Stakes Litigation in the Canadian Public Sector, scheduled to be published by LexisNexis Canada Inc. in 2022.

The juncture of two phenomena renders public sector Personal Information class actions ("PICA"s) of particular interest. The potential for significant damages and the fact that, unlike private sector actors, bankruptcy protection is not usually available for public sector entities ("Entities") sets them apart. In theory, therefore, the sky is the limit when it comes to possible exposure.

## II. Privacy and Personal Information

It is important to clarify what is meant by two often intertwined but different concepts that should be distinguished: privacy and Personal Information. Personal Information is defined in the law as "information about an identifiable individual"[2] whereas privacy can have many definitions. One of the most common is that provided by the Supreme Court of Canada in *R.* v. *Plant*: "a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state."[3] These two definitions demonstrate that Personal Information can be private but is not always so, just as privacy may include Personal Information but will also include other elements.

## III. Privacy

Privacy protection in the public sector grew from a desire, following the Second World War, to recognize and protect fundamental human rights. Article 12 of the *United Nations' Universal Declaration of Human Rights* and Article 17 of the *International Covenant on Civil and Political Rights* similarly protect the individual against arbitrary interference with his privacy, family, home or correspondence, as well as unlawful attacks upon his honour and reputation. Initially, defending privacy was a question of defending an individual against unwarranted interference by the state.

In 1982, when Canada adopted the *Canadian Charter of Rights and Freedoms* ("*Canadian Charter*"),[4] it did not contain a provision specifically protecting privacy. Instead, this was read into Section 8 that protects against unreasonable search and seizure.[5] It is interesting to note that Québec's *Charter of Human Rights and Freedoms*, which took effect in 1976, does recognize the right of individuals to have their private life respected.[6] The Supreme Court of Canada in its interpretation of Section 8 of the *Canadian Charter* has identified three "privacy interests"[7] or realms in which individuals have a heightened expectation of privacy. The state must tread carefully when

[2] *Privacy Act,* R.S.C., 1985, c. P-21 [*Privacy Act*].
[3] *R. v. Plant*, [1993] 3 S.C.R. 281, 84 C.C.C. (3d) 203, at 293 (S.C.C.).
[4] *Constitution Act*, 1867 (UK), 30 & 31 Vict., c. 3, s. 91, reprinted in RSC 1985, Appendix II, No. 5; *Constitution Act*, 1982, s. 35, being Schedule B to the Canada Act 1982 (UK), 1982, c. 11.
[5] *Constitution Act*, 1982, s. 35, being Schedule B to the Canada Act 1982 (UK), 1982, c. 11, s. 8.
[6] *Charter of human rights and freedoms*, C.Q.L.R., c. C-12, s. 5.
[7] *R. v. Dyment*, [1988] 2 S.C.R. 417, [1988] 2 R.C.S. 417 at 428 (S.C.C.).

entering one of these realms so as not to violate the individual's interest. These privacy interests are:

> **A personal privacy interest**: attached to the individual's physical being. Traditionally, this interest has been perceived as giving rise to the most serious violations of an individual's reasonable expectation of privacy.
>
> **A territorial privacy interest**: certain spaces or territories in which an individual has a heightened expectation of privacy and that are worthy of vigilant protection. These spaces could include in order of decreasing expectation: the perimeter space around the home; commercial space; a private car; a school; and even a prison[8].
>
> **An informational privacy interest**: attached to digital communication devices such as computers, tablets, and mobile phones that store large amounts of Personal Information.

While these interests may involve Personal Information, they are not what the *Canadian Charter* or its corresponding case law protects. Instead, it is the *Privacy Act*, adopted in 1983, and the *Access to Information Act*, adopted in 1985, that govern the way the state Processes the Personal Information belonging to an individual and the individual's rights with respect to this information.

## IV. Personal Information

Personal Information protection regimes evolved in response to the same phenomena as privacy legislation but also because of a crucial recognition: the development of increasingly powerful computer technology that could Process vast amounts of Personal Information. It was believed that measures should be taken to give people control over how their information could be used. In 1980, the Organisation for Economic Cooperation and Development issued its *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* which enunciated principles of: a) limitation collection; b) data quality; c) purpose specification; d) use limitation; e) security safeguards; f) openness; g) individual participation; and h) accountability (collectively, "Principles").[9] In Canada, the adoption of these Principles in the public sector has often been uneven because of the second challenge affecting public sector PICAs: the effects of federalism on the relevant substantive and procedural legislation.

[8] *R. v. Tessling*, [2004] 3 S.C.R. 432, 2004 SCC 67 at 444 (S.C.C.).

[9] OECD Council, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, OECD Guidelines (September 23, 1980).

## V. Personal Information and Federalism

Sections 91 and 92 of the *Constitution Act, 1867* distribute legislative power between the Parliament of Canada and the provincial legislatures respectively.[10] As a result, Entities entrusted with implementing and administering public programs in these jurisdictions may be regulated either by provincial laws or federal laws or both. A first step in defending a PICA in Canada is to establish the applicable legislation governing both the substantive and procedural legal issues – a task that is not always simple given certain cross-jurisdictional differences.

## VI. Entities – Government Institutions, Public Bodies, Trustees, and Custodians

An initial difference among the various Personal Information protection legislation is the terminology used to describe the Entities they regulate. Federally, Canada's *Access to Information Act* and *Privacy Act* apply to "government institutions," that is to any Government of Canada department, ministry of state, body, or office listed in Schedule 1 of the *Access to Information Act*, or crown corporations and their wholly owned subsidiaries.

Provincially, the Entities governed by access to information and Personal Information protection legislation may be referred to as "institutions," "government institutions," or "public bodies" depending on the province. The list of what qualifies as an institution, a government body, or a public body varies slightly between the provinces but generally includes: (i) provincial ministries; (ii) agencies, boards, commissions, corporations, offices, or other bodies designated in a schedule to the *Act*; and (iii) local public bodies – namely, a local government body (i.e. a municipality, library board, water board, etc.) a health care body, a social services body, or a governing body of a profession or occupation.

## VII. The Purposes of Access to Information and Personal Information Protection

The purpose of the *Privacy Act*, the *Access to Information Act*, and their provincial counterparts is to promote the fair and transparent Processing of Personal Information by Entities and to allow individuals access to the Personal Information when it belongs to them. Federally, this protection is offered by two separate statutes. Provincially, access to information and Personal Information protection are contained in a single statute.

In contrast to the common objective shared by federal and provincial access to information and protection of Personal Information legislation, the provincial personal health information statutes frequently have diverging purposes, thus complicating the defence of PICAs across

[10] *Constitution Act*, *1867* (UK), 30 & 31 Vict., c. 3, s. 91-92, reprinted in R.S.C. 1985, Appendix II, No. 5.

jurisdictions. Many provinces have enacted health information protection acts the principal object of which is to regulate the Processing of such information in the health sector.

## VIII. Oversight and Enforcement

One of the greatest divergences among the provincial and federal access to information and Personal Information protection legislation is their models. Federally, and in most provinces and territories except Manitoba, Yukon, New Brunswick, and Québec, the person responsible for overseeing the enforcement of the legislation is a commissioner. Appointed by the Lieutenant Governor in Council, on the recommendation of the legislative assembly, the commissioner can investigate complaints, hear inquiries, and make orders to ensure compliance with the applicable access to information and Personal Information protection legislation. They also comment on the effects of government programs on the protection of Personal Information, authorize the collection of Personal Information from sources other than the individual concerned, and educate the public.

Federally, the Governor in Council appoints the Information Commissioner[11] as well as the Privacy Commissioner.[12] The Information Commissioner and the Privacy Commissioner may also be one and the same person.[13] Although the Privacy Commissioner has broad powers of investigation, he or she does not have much power to enforce recommendations. Any request for enforcement must be brought before the Federal Court.

## IX. PICAs and Recent Developments

Just as defendants must be mindful of the complex patchwork of privacy and Personal Information Legislation, they must also be mindful of the complex patchwork of class action legislation that exists in Canada. Unlike some other jurisdictions, class action procedures and rules are primarily provincial (as opposed to federal) in nature and vary from jurisdiction to jurisdiction. Although the common law provinces have adopted similar statutory regimes, they are not identical, especially given recent amendments to Ontario's *Class Proceedings Act, 1992*.[14] Québec's codified regime is arguably the most unique of all and is generally viewed as more favourable to plaintiffs than those of the other provinces. Importantly, class actions must first be formally certified (or authorized in Québec) before they can proceed on the merits. This preliminary test imposes a lower standard of proof than the balance of probabilities. More specifically, the plaintiff must satisfy the court that the criteria for certification/authorization have all been met. Once again, these criteria – and the case law to which they have given rise – will vary from jurisdiction to jurisdiction.

[11] *Access to Information Act*, s. 54(1).
[12] *Privacy Act*, s. 53(1).
[13] *Privacy Act,* R.S.C., s. 55(1).
[14] *Class Proceedings Act, 1992*, S.O. 1992, c. 6.

The reasonableness (or unreasonableness) of a defendant's conduct with respect to the protection of Personal Information will often determine: whether a PICA should be certified/authorized; if so, whether it should be granted on the merits; and, if so once again, the nature and extent of the remedies that should be awarded to the plaintiff and the class members. Indeed, should a class action be certified/authorized and proceed on the merits, the representative plaintiff will be held to the same standard of civil or statutory proof as any other plaintiff.

Recently, in *Lamoureux v. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*,[15] the Court of Appeal of Québec confirmed the dismissal of a public sector PICA on the merits[16] – the first Canadian decision to do so – in which a class action was brought following the loss of a computer by an employee of the Investment Industry Regulatory Organization of Canada ("IIROC"). The computer in question contained the Personal Information of thousands of Canadian investors. Not only did the courts of first instance and appeal conclude that IIROC acted reasonably by investigating the incident, advising customers of the breach, informing authorities and the privacy commissioners, and providing free credit monitoring services (among other things), but that the harm complained of by the representative plaintiff - which amounted to allegations of stress and inconvenience – was not compensable under applicable principles of civil law. Indeed, according to the Supreme Court of Canada in *Mustapha v. Culligan of Canada Ltd*.: "The law does not recognize upset, disgust, anxiety, agitation, or other mental states that fall short of injury. I would not purport to define compensable injury exhaustively, except to say that it must be serious and prolonged and rise above the ordinary annoyances, anxieties, and fears that people living in society routinely, if sometimes reluctantly, accept."[17]

Other *private sector* PICAs have also been dismissed at the certification stage due to the absence of a compensable injury. For instance, in *Setoguchi v. Uber B.V.*, the Court of Queen's Bench of Alberta stated "there must be some evidence or basis in fact in support of real (not *de minimus*) compensable harm or loss, leading to a claim that is at least arguable, and that certification should indeed must not be allowed without it. Otherwise, a class proceeding could be a mere 'fishing trip' based on speculation, without any evidence of fish being present."[18] Similar reasoning

[15] *Lamoureux c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2022 QCCA 685.
[16] *Lamoureux c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2021 QCCS 1093.
[17] *Mustapha v. Culligan of Canada Ltd*., [2008] 2 S.C.R. 114, 2008 SCC 27 (S.C.C.), at para. 9.
[18] *Setoguchi v. Uber BV*, [2021] A.J. No. 22, 2021 A.B.Q.B. at para. 37 (A.B.Q.B.).

was developed in *Simpson v. Facebook*[19] and *Kish v. Facebook Canada Ltd*.[20]

Although the "evolving" common law tort of intrusion upon seclusion[21] does not require proof of economic injury, in *Owsianik v. Equifax Canada Co*. a majority of the Divisional Court of the Ontario Superior Court of Justice stated that "[t]he tort ... has nothing to do with a database defendant. It need not even involve databases. It has to do with humiliation and emotional harm suffered by a personal intrusion into private affairs, for which there is no other remedy because the loss cannot be readily quantified in monetary terms."[22] As a result, it would be inappropriate "to extend liability to a person who does not intrude, but who fails to prevent the intrusion of another ..."[23]

## X. Conclusion

An invasion of privacy – and, more specifically, the compromise of Personal Information – can give rise to a class action when the injuries alleged by a group of victims originate from the same incident. This is so regardless of whether the defendant is a private enterprise or an Entity. In fact, several cases in common law Canada and Québec show that such Entities are a natural target for class actions since, in order to accomplish their public purpose, they are required to collect, store, analyse, and communicate sensitive personal information belonging to patients, students, investors, and other ordinary citizens. These cases further show that insufficient safeguards and negligent, ill-intentioned, and/or unsupervised employees can lead to costly and protracted litigation, even in instances where the Entities themselves have made good faith efforts to discharge their responsibilities in accordance with applicable privacy and Personal Information legislation.

As a result, it is vital for Entities to adopt a two-pronged approach: 1) a *proactive* approach that aims to ensure Personal Information is kept and accessed in a manner fully consistent with the laws of the jurisdiction(s) in which the Entity operates; and 2) a *responsive* approach that represents a diligent, thoughtful, and reasonably transparent response to an invasion of privacy in order to protect the persons whose Personal Information has been compromised and mitigate or avoid altogether any injuries stemming from that compromise. Given the patchwork nature of Canadian privacy, Personal Information, and

[19] *Simpson v. Facebook Inc*, [2021] O.J. No. 726, 2021 O.N.S.C. 968 (O.N.S.C.).

[20] *Kish v. Facebook Canada Ltd*, [2021] S.J. No. 339, 2021 S.K.Q.B. 198.

[21] In *Jones v. Tsige*, 2012 ONCA 32, the Court of Appeal for Ontario specified that "[t]he key features of this cause of action are, first, that the defendant's conduct must be intentional, within which I would include reckless; second, that the defendant must have invaded, without lawful justification, the plaintiff's private affairs or concerns; and third, that a reasonable person would regard the invasion as highly offensive causing distress, humiliation or anguish."

[22] *Owsianik v. Equifax Canada Co*., 2021 ONSC 4112 at para. 54.

[23] *Owsianik v. Equifax Canada Co*., 2021 ONSC 4112 at para. 54.

class action legislation, it is essential to develop proactive and responsive best practices with seasoned counsel, in each of the relevant jurisdictions, to ensure that the rights of the Entity – and indeed those of the citizens they exist to serve – are secured to the full extent possible.

**Past Committee Newsletters**

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

JUNE 2021
Facial Recognition Technology - The Good, Bad, and the Future
Avanti Bakane, Margaret Martin and Kyla Guru

MAY 2021
The Ransomware Scourge: Connectivity and Vulnerability in an Internet of Things, 5G World
David Patrón

FEBRUARY 2021
If you Want to Stay Friends with your IT Supplier, Use the Contract!
Anna Cook and Robert Graham

MARCH 2018
First Class Action Data Breach in the UK – Employer Found Vicariously Liable for Rogue Employee's Actions
Elena Jelmini Cellerini and Vikram Khurana

NOVEMBER 2017
Blockchain Unchained: One Lawyer's Quest to Figure out what the Hell Everyone is Talking About
Kendall Harrison

AUGUST 2017
Def Con Hacker Conference: An Accidental Tourists Observations
Elizabeth S. Fitch

MAY 2017
*Doe v. Backpage.com* and its Aftermath: Continued Uncertainty and New Litigation in the Wake of the Supreme Court's Denial of Certiorari
David Patrón

APRIL 2017
Incorporating Technology into the Management of the Work Processes at the Firm
Donna L. Burden, Elizabeth S. Fitch and Park L. Priest

FEBRUARY 2017
"The First Thing We Do, Let's Kill All The Lawyers"
Elizabeth S. Fitch and Elizabeth Haecker Ryan

DECEMBER 2016
A Primer for Understanding Blockchain
Doug Vaughn and Anna Outzen

AUGUST 2016
The Attorney-Client Relationship in the Electronic Age
Elizabeth S. Fitch and Theodore M. Schaer