Canadian Privacy Law Review

VOLUME 18, NUMBER 10 Cited as (2021), 18 C.P.L.R. SEPTEMBER 2021

• THE BALANCING OF PRIVACY RIGHTS AND THE OPEN COURT PRINCIPLE: DISCLOSURE OF PRIVATE INFORMATION IN LITIGATION •

Talia Gordner, Partner, Jamieson D. Virgin, Partner, Ralph Cuervo-Lorens, Partner, and Paola Ramirez, Associate, McMillan LLP

• In This Issue •


Talia Gordner


Jamieson D. Virgin


Ralph Cuervo-Lorens


Paola Ramirez

*"**This** Court has been resolute in recognizing that the open court principle is protected by the constitutionally-entrenched right of freedom of expression and, as such, it represents a central feature of a liberal democracy. As a general rule, the public can attend hearings and consult court files and the*

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.

ISBN 0-433-44417-7 (print) ISSN 1708-5446
ISBN 0-433-44650-1 (PDF) ISSN 1708-5454
ISBN 0-433-44418-5 (print & PDF)

Subscription rates: $355.00 per year (print or PDF)
$545.00 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

press — the eyes and ears of the public — is left free to inquire and comment on the workings of the courts, all of which helps make the justice system fair and accountable."

The Supreme Court of Canada's recent decision in *Sherman Estate v Donovan*[1] ("***Sherman Estate***"), offers clarity on when the open court principle will give ground to the right to privacy. The Supreme Court's decision is a reminder that although privacy is fundamental to the preservation of a free and democratic society, it is not absolute.[2] The presumption of openness will only yield in circumstances where there is a serious risk to an important *public* privacy interest. Individual privacy interests, such as the discomfort often associated with sharing private information in open court, are not, without more, sufficient to overturn the strong presumption of court openness.

THE CASE

Sherman Estate arose out of a probate proceeding connected with the highly publicized murders of Bernard and Honey Sherman – the prominent Toronto philanthropists whose murders have been the subject of extensive media coverage since 2017.[3]

The trustees of the couple's estate wanted to keep the probate files private because of the large value of the estate and because the perpetrators of the murders remained at large.[4] The trustees sought sealing orders of the probate files before the Ontario courts to protect the estate trustees and beneficiaries from both privacy intrusions and risks to personal safety.[5] The trustees argued that if the court files were disclosed to the public there would be a real and substantial risk that the affected individuals would suffer serious harm.[6]

Relying on the principle that the *Canadian Charter of Rights and Freedoms* protects court openness, the Toronto Star and its Chief Investigative Reporter, Kevin Donovan, sought to access the probate files. They argued that the sealing orders violated their rights of freedom of expression and freedom of the press as well as violated the principle that the courts should be open to the public as a means of guaranteeing the fair and transparent administration of justice.[7]

The principle of "open court" is protected by the constitutional guarantee of freedom of expression in Canada and is essential to the proper functioning of democracy. However, this principle can sometimes conflict with individual privacy interests as court proceedings can lead to the dissemination of highly sensitive personal information that may be a source of embarrassment.[8]

THE DECISION

The Supreme Court of Canada ultimately agreed with the Toronto Star and Mr. Donovan. In order to overshadow the open court principle there must be a public character of the privacy interest at stake, such as involving the protection of individuals from the threat to their dignity, which can ultimately be threatened by information disclosed in open court.[9]

The Supreme Court clarified that dignity will be at serious risk only in limited cases[10] and that the burden is on the applicant to show that privacy, understood in reference to dignity, is at serious risk.[11] Dignity will be at serious risk where the information disseminated would be sufficiently sensitive such that openness would meaningfully strike at the individual's "biographical core" in a manner that threatens their integrity[12] and undermines their control over the expression of their identities.[13] Information affecting this "biological core" includes information that reveals something intimate and personal about the individual, their lifestyle or their experiences.[14]

The Supreme Court found that the information contained in the probate files did not reveal anything particularly private or highly sensitive about the affected individuals.[15] Public disclosure of information in the files, consisting of names, addresses, and relationships between the Shermans and their trustees and beneficiaries, did not rise to level of being a public interest in privacy.

THE TAKEAWAYS

While *Sherman Estate* is undoubtedly of interest to counsel seeking to understand the legal test for obtaining a sealing order (or similar relief), the case also provides helpful clarity for litigants more generally. Civil lawsuits often require the disclosure of sensitive business records or information. This is particularly so in cases involving fraud where production of records and information beyond those created in the ordinary course of business are often sought and produced. The conduct underlying allegations of fraud often involves secret communications between co-conspirators, documents created to facilitate the fraud, and financial transactions to transfer unlawfully taken funds, make payments for unlawful activities or hide assets.

Such documents may include more personal records such as phone records, text messages, personal emails, bank account statements and transaction records. These types of records do not usually need to be produced in the context of typical commercial disputes. However, in the context of allegations of fraud, these records are often where the proof of the fraud lies.

Sherman Estate offers helpful guidance as to how courts might view the often claimed right to privacy by defendants when a plaintiff seeks to obtain a defendant's personal records in order to seek to prove the fraud allegations. A sealing order to prevent information filed in or relating to a court proceeding from being accessible to the public and an order to prevent production of personal records so they are not disclosed to the other parties in the lawsuit or become part of the public record both raise similar privacy issues.

Both require something beyond the usual embarrassment or discomfort experienced by an individual arising from the disclosure of their text messages or bank records. While such threshold is not impossible to overcome, *Sherman Estate* creates additional challenges for defendants facing fraud allegations who seek to prevent the disclosure of their personal information and records.

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.

Content provided with permission from McMillan LLP. Further information is available at [https://mcmillan.ca/insights/the-balancing-of-privacy-rights-and-the-open-court-principle-disclosure-of-private-information-in-litigation/]

[***Talia Gordner*** *is an experienced lawyer with a corporate and commercial litigation practice focused on the resolution of complex environmental, regulatory and real estate disputes. Talia represents clients from a range of industries, including construction, oil and gas, and manufacturing, in matters that range from common commercial disputes such as claims of breach of contract, fraud and negligence, to complex environmental disputes involving recent, ongoing and historical contamination.*

Jamieson D. Virgin's *litigation and dispute resolution practice focuses largely on construction and commercial real estate matters. Assisting clients with product liability, competition law, class actions, insurance law, and commercial litigation, he has also gained significant experience in white collar defence, and fraud and investigations.*

Ralph Cuervo-Lorens *is a leading lawyer practising environmental law and regulatory compliance and dispute resolution for clients in primarily the manufacturing, municipal, construction, transportation, energy and mining industries. In his environmental law practice, Ralph focuses on regulatory matters, corporate social responsibility and environmental risk-management, mitigation, permitting, impact assessment and compliance.*

Paola Ramirez *maintains a diverse civil and commercial litigation practice with a focus on intellectual property. Representing businesses in a range of industries, Paola has gained significant expertise assisting clients in the oil and gas, retail and cannabis sectors.*]

---

1 *Sherman Estate v Donovan*, 2021 SCC 25.
2 *Ibid* at para 31.
3 *Ibid* at para 9.
4 *Ibid* at para 10.
5 *Ibid* at para 11.
6 *Ibid*.
7 *Ibid* at para 12.
8 *Ibid* at para 2.
9 *Ibid* at para 49, 62-63.
10 *Ibid* at para 64.
11 *Ibid* at para 77.
12 *Ibid* at para 86.
13 *Ibid* at para 92.
14 *Ibid* at para 78.
15 *Ibid* at para 92.

• THE RIGHT TO ERASURE OF PERSONAL INFORMATION IN CANADA: BETWEEN FACT AND FICTION •

Éloïse Gratton, Partner, Andy Nagy, Associate, and Simon Du Perron, Articling Student,
Borden Ladner Gervais LLP


Éloïse Gratton


Andy Nagy


Simon Du Perron

It is increasingly common for businesses to receive requests from customers asking for the deletion of all of the information that the business holds about them. Such requests raise the issue of whether there is a right to the deletion or erasure of personal information under Canadian data protection laws.

The concept of the right to erasure comes from the *General Data Protection Regulation* (GDPR), which is frequently referred to as the benchmark legislation for data protection around the world. Effective as of 2018, the GDPR grants several rights to data subjects, including in Article 17, a right to obtain the erasure, as soon as possible, of personal data that a business holds about them, where one of the following grounds applies:

- personal data is no longer necessary in relation to the purposes for which it was collected;
- the data subject withdraws consent upon which the processing is based and there is no other legal ground for the processing;
- the data subject objects to the processing of personal data concerning him or her and where there are no overriding legitimate grounds for processing;
- personal data has been unlawfully processed;
- personal data has to be erased for compliance with a legal obligation; or
- personal data was collected when the data subject was a child and was not fully aware of the risks involved with the processing.

It is worth pointing out that **the GDPR does not provide a general right to erasure but rather a limited right to specific circumstances**. Canadian businesses subject to the extraterritorial scope of the GDPR, must ensure that they have procedures to assess and handle requests for erasure made under the legislation. Namely, should these businesses offer goods or services to individuals located in the European Union or monitor the behaviour of those individuals, to the extent that the behaviour in question takes place within the Union.

Do Canadian data protection laws provide individuals with a similar right? This article seeks to answer this question in order to provide guidance to businesses dealing with requests for says deletion of personal information.

WHAT THE LAW IS SAYING

In Canada, the *Personal Information Protection and Electronic Documents Act* (PIPEDA) applies to personal information held by businesses in all provinces that have not adopted legislation that has been deemed as substantially similar to PIPEDA.

Québec, Alberta and British Columbia are the three provinces with private sector data protection laws. Thus, businesses operating entirely in Québec, Alberta or British Columbia are subject to the provincial legislation. However, even in those provinces, PIPEDA applies to businesses whose activities involve the transfer of personal information across provincial or Canadian borders, as well as to federally regulated organizations such as banks and telecommunications companies.

A. Federal

PIPEDA requires that an organization destroy, erase or make anonymous personal information that is no longer required to fulfil the pre-identified purposes (Principle 4.5.3). PIPEDA also provides that an individual must be given access to his or her personal information (Principle 4.9.1) the opportunity to request correction of that information if it is inaccurate or incomplete (Principle 4.9.5). Yet, **PIPEDA does not provide individuals with a right to request the deletion of their personal information when it is still required for the purposes for which it was collected**. Therefore, it is only when the information is no longer necessary for the organization that an individual would be able to request that the organization delete the information as part of a challenge concerning compliance (Principle 4.10).

B. Québec

In Québec, the purpose of the *Act respecting the protection of personal information in the private sector* (QC Private Sector Act) is to establish specific rules for the exercise of the rights provided in articles 35 to 40 of the Civil Code of Québec (C.c.Q.) concerning personal information collected in the course of business operations carried within the scope of article 1525 C.c.Q. Thus, article 40 (1) C.c.Q. provides that an individual may request that "obsolete information or information not justified by the purpose of the file" be deleted. Section 28 QC Private Sector Act further adds to this section by stipulating that an individual may request the deletion of personal information about him or her if the collection is unauthorized under law. Consequently, **Québec legislation recognizes three situations in which an individual may ask a business to delete personal information that it holds about him or her**:

1. when the information is obsolete[1];
2. when the retention of the information is no longer justified for the purpose for which it was collected; or
3. where the information was not collected in a lawful manner[2].

Once again, it must be noted that, like PIPEDA and the RGPD, QC Private Sector Act and the Civil Code do not grant individuals a general right to obtain the deletion of their personal information held by a business. Deletion can therefore only be requested on specific grounds. This statement appears to be consistent with the overarching purpose of the QC Private Sector Act, which seeks to balance the privacy rights of individuals with the needs of businesses to process personal information[3]. Indeed, companies may have several legitimate purposes for keeping their customers' personal data: to provide a product or service, to send warranty or safety information to the customer, to comply with legal retention requirements, to conduct internal performance analyses, to conduct research and development projects, etc. A general right to the erasure of personal information would undermine many of these goals. It would place a significant logistical and operational burden on businesses without necessarily ensuring greater protection of privacy rights.

C. British Columbia and Alberta

In both British Columbia and in Alberta, the *Personal Information Protection Act* (PIPA) **does not grant individuals with a right to request the erasure of their personal information held by businesses**. The rights under both the British Columbia's and Alberta's PIPAs are limited to the right to correct an error or omission in personal information. The PIPAs also includes a requirement for businesses to destroy or

anonymize personal information when it is no longer needed for legal or business purposes or to comply with the law.

WHAT THE RECENT BILLS ARE SAYING

Two major reforms of privacy legislation were introduced in 2020.

Two major reforms of privacy laws were introduced in 2020 in Canada. On the one hand, Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information*, introduces several modifications to *QC Private Sector Act*. On the other, the federal level, Bill C-11, *the Digital Charter Implementation Act, 2020*, proposes to replace Part 1 of PIPEDA with the new *Consumer Privacy Protection Act* (CPPA).

In Québec, Bill 64, which is currently under clause-by-clause consideration, proposes a slight rewording of section 28 of QC Private Sector Act, which would read as follows[4]:

> *"In addition to the rights provided under the first paragraph of article 40 of the Civil Code, any person may, if personal information concerning him is inaccurate, incomplete or equivocal, or if collecting, communicating or keeping it are not authorized by law, require that the information be rectified."*

As a result, the fact that Bill 64 does not mention the "deletion" of personal information in section 28 means that **deletion requests will be limited to the two circumstances set out in article 40 C.c.Q.**, i.e., when the information is obsolete or when it is no longer necessary to fulfill a specific purpose. Two grounds that are practically the same if we consider that information that is no longer necessary is "obsolete".

Bill C-11 directly deals with the issue of deletion of personal information by introducing a "**right to disposal**" of personal information, at the request of the individual, in section 55 of the CPPA. The term "disposal" is defined as the "permanent and irreversible deletion of personal information". However, this new right would only cover information that the organization has collected "from the individual". i.e. excluding information derived or inferred by the organization about the individual (e.g., credit score, online consumer behaviour, etc.) or information obtained from third parties. The Bill further states that a company may refuse a request to opt out only if:

- the request would result in the disposal of personal information about another individual and that the information is not severable; or
- a legal requirement or the reasonable terms of a contract prevent it from carrying out the disposal request.

The scope of the expression "reasonable terms of a contract" remains unclear. Notably, this exception does not appear to be limited to contracts with the individual. In other words, an organization could rely on some restrictions in a contract with a third party to restrict the exercise of the individual's right to disposal to the extent that such a limitation is "reasonable"[5]. On the other hand, this exception may be difficult to apply in situations where the organization holding the personal information does not interact directly with the individual, for instance, in cases where information is collected under an exception consent or under implied consent.

CONCLUSION: IS A RIGHT TO DELETION REALLY NECESSARY?

The main conclusion of our analysis is that Canadian private sector data protection laws do not provide individuals with a general right to request the deletion of their personal information held by a business.

Thus, under Canadian law, a business should destroy personal information it keeps not because the individual to whom the information relates requests it, but rather because retaining such information is no longer necessary to achieve a specific purpose. Indeed, in its investigation of the Desjardins data breach, the Office of the Privacy Commissioner of Canada emphasized that retaining personal information that is no longer needed increasingly exposed businesses to security breach risks.

That being said, given that Bill C-11 proposes to introduce a general right to request the "disposal" of their personal information, it seems appropriate to question the relevance of such a right. Insofar, privacy legislation already obliges organizations to collect and retain only the personal information necessary to fulfil a predetermined purpose. The added benefit of a right to deletion, in terms of increased protection of privacy rights, seems to be questionable. Instead, a right to deletion may create unrealistic expectations for consumers and increase the logistical burden of organizations.

[***Éloïse Gratton*** *is recognized internationally as a pioneer in the field of privacy and she co-leads the firm's national Privacy and Data Protection practice. She offers strategic advice relating to best business practices relevant to the monetization of big data and the use of artificial intelligence, in addition to providing support in crisis management situations (e.g. security breaches, privacy commissioners' investigations, class actions) both nationally and internationally. She also advises companies and their board of directors on the management of personal information and the protection of privacy, including on issues relating to compliance, risk management, ethics and data governance.*

Andy Nagy's *practice focuses on privacy and cybersecurity. He advises businesses from various sectors on issues ranging from compliance with privacy, to data protection, to anti-spam laws. He also assists businesses on matters pertaining to IT, AI, big data analytics, consumer protection and data breach management. Andy was media editor for the McGill Journal of Dispute Resolution, and has also authored and contributed to various publications pertaining to privacy, cybersecurity and technology law.*

Simon Du Perron *is articling with the Privacy and Data Protection practice group. He provides advice to clients on issues such as: Compliance with Canadian privacy legislation; the use of artificial intelligence, big data and biometrics systems; and interpretation of Québec's Act to establish a legal framework for information technology. Simon holds an LL.M. in IT Law and authored several publications on topics related to law and emerging technologies.*]

---

1 However, it should be noted that there is some ambiguity in QC Private Sector Act as to whether individuals can ask a business to delete personal information that they consider obsolete, given that the CAI ruled that it did not have jurisdiction to determine whether personal information is obsolete and therefore is prevented from ordering the deletion of obsolete information held by a business, see *S.B. c. Trans Union du Canada inc.,* 2015 QCCAI 78, par. 30.

2 See *E.R.* c. *Sirco-Enquête et protection*, 2012 QCCAI 407, par. 29-30 ; *N.L.* c. *Fédération des caisses Desjardins du Québec*, 2014 QCCAI 168, par. 64-66 ; et *X* c. *Anapharm inc.*, no. 06 08 16, 30 novembre 2006, H. Grenier, par. 71.

3 See *Garderie Cœur d'Enfant Inc.*, 2014 QCCAI 080272, par. 24 ; *Banque Nationale du Canada*, 2016 QCCAI 110676, par. 42 ; *X. Et Pharmaprix*, 2014 QCCAI 1003352, par. 10

4 However, Bill 64 proposes to introduce the right of an individual to require that organization to cease disseminating personal information about him or her or to de-index any hyperlink associated with his or her name that provides access to such information, provided some specific criteria are met (see section 113 of the Bill).

5 For instance, an organization could be required by contract with "financial institutions that process credit card transactions to retain transaction data" for "charge backs, audits, and other unspecified purposes", see Office of the Privacy Commissioner of Canada, PIPEDA Report of Findings #2007-389, at paras. 62–63, Investigations into business.

• REGULATION OF PRIVACY IN ONTARIO: ONE STEP CLOSER •

Ruth E. Promislow, Partner, J. Sébastien A. Gittens, Partner, and Carolin Jumaa, Associate, Bennett Jones LLP


Ruth E. Promislow


J. Sébastien A. Gittens


Carolin Jumaa

Organizations operating in Ontario may soon be subject to an entirely new provincial privacy regime that could impose substantial compliance obligations, and establish significant penalties for contravention of those obligations.

On June 17, 2021, the Ontario Ministry of Government and Consumer Services (Ontario) published a white paper titled "Modernizing Privacy in Ontario: Empowering Ontarians and Enabling the Digital Economy." Following a privacy reform consultation process (which we previously reported on in *Ontario Promises to Create Canada's First Provincial Data Authority*), Ontario has identified several key privacy issues and corresponding draft legislative language to address those issues. Ontario has called for submissions in response to its proposed legislative text.

The key themes in the Ontario white paper are generally aligned with those underlying the federal government's Bill C-11 (C-11), namely:

- requirements for obtaining meaningful consent;
- obligation on organizations to implement a privacy management program which includes their policies and protocols setting out how they comply with regulatory obligations;
- exposure to penalties for contravention of obligations;
- increased individual rights; and
- required transparency in connection with the use of artificial intelligence.

The proposals in the Ontario white paper are summarized as follows:

PROPOSAL 1: RIGHTS-BASED APPROACH TO PRIVACY

Ontario proposes to establish a fundamental right to privacy "as the underpinning principle for a provincial privacy law, ensuring that Ontarians are protected, regardless of commercial interests." In connection with this principle, Ontario proposes the following concepts, which are generally aligned with proposed language in C-11:

- **Fair and appropriate purposes**: Information should only be collected, used and disclosed for purposes that an individual would reasonably expect, regardless of the lawful grounds that may apply.
- **Limitations on collection, use and disclosure of personal information**: Organizations should limit their collection, use and disclosure to personal information that is necessary to carry out the intended purpose.

- **Data mobility**: Individuals should have the right to obtain and transfer their own personal information.
- **Right of disposal (or erasure)**: Individuals should be able to request that an organization dispose of their personal information.
- **Right of access and correction**: Individuals should have access to, and be able to correct, personal information in the custody of an organization

PROPOSAL 2: AUTOMATED DECISION-MAKING

Ontario proposes to regulate the use of automated decision-making by:

- providing individuals with the right to know about the use of automated decision-making in connection with their personal information;
- requiring organizations to answer requests for information regarding decisions made about individuals through the use of automated decision-making;
- empowering individuals with the right to comment on, contest, or request a review of the decision impacting them that is rendered through the use of automated decision-making; and
- prohibiting the use of automated decision-making in situations of significant impact.

PROPOSAL 3: MEANINGFUL CONSENT

Ontario proposes to combat the effect of "consent fatigue" (whereby individuals will accept any legal notice presented to them without reading or understanding its terms) and provide for meaningful consent by:

- requiring certain information be provided by organizations when seeking consent for the collection, use or disclosure of personal information;
- providing individuals with the right to withdraw consent;
- requiring organizations to consider the sensitivity of the personal information to be collected when formulating the consent process;
- prohibiting organizations from making consent a condition for service or from using deceptive or duplicitous means to obtain consent; and
- allowing for implied consent circumstances where individuals would reasonably expect their information to be collected and used.

PROPOSAL 4: TRANSPARENCY

Ontario recognizes that "stronger transparency requirements could provide citizens with a right to know when and how their data is used by organizations, allowing them to regain control and participate more meaningfully in the decisions that affect their well-being."

In an effort to enhance individuals' rights to know when and how their data is used, Ontario has put forth two proposals for consideration:

- organizations must implement a privacy management framework (internal privacy policies, practices and procedures) detailing their compliance with regulatory obligations; and
- organizations must make information about their compliance-related policies, practices and procedures available to individuals. Such information, which would have to be provided in plain language, would convey the organization's use of data, the lawful basis relied upon for any such uses and how individuals may exercise their data rights.

PROPOSAL 5: PROTECTING CHILDREN AND YOUTH

Ontario proposes to provide special protections for children to guard by "introducing a minimum age of valid consent and prohibiting organizations from monitoring children for the purpose of influencing their decisions or behaviour."

PROPOSAL 6: INCREASED POWERS FOR ONTARIO'S PRIVACY COMMISSIONER AND PENALTIES

Ontario is proposing to extend the mandate of the Information and Privacy Commissioner of Ontario (IPC) to include regulatory oversight, enforcement powers and the provision of support to organizations in connection with the new privacy regime.

Pursuant to the proposed language, the IPC would be empowered to:

- initiate and conduct investigations or audits;
- compel organizations to provide information;
- issue binding orders to non-compliant organizations; and
- impose administrative monetary penalties to a maximum of $10 million or 3 percent of gross global revenue for organizations, and to a maximum of $50,000 for individuals.

PROPOSAL 7: SUPPORTING ONTARIO INNOVATORS

Ontario proposes to permit the use of de-identified information in specified circumstances to support innovation so that organizations can use this information to improve upon or develop technologies, services or products. Ontario proposes to clarify the meaning of de-identified information, defining it as: "information about an individual that no longer allows the individual to be directly or indirectly identified without the use of additional information.

Ontario has requested feedback in respect of its proposals from organizations, impacted stakeholders and the general public by August 3, 2021.

[***Ruth E. Promislow*** *practices in the areas of privacy, data protection and management, cybersecurity and fraud. Ruth has over 20 years of experience in litigating complex commercial disputes in a wide variety of areas (including privacy, cybersecurity, fraud, reinsurance and professional negligence), with an impressive track record of success. Ruth has extensive experience with data protection, privacy and cybersecurity matters including regulatory compliance, cyber preparedness, breach response and related litigation.*

J. Sébastien A. Gittens *understands the need to provide legal advice in a timely, efficient and pragmatic way. This businesslike philosophy is backed by the first joint Ph.D. in Pharmaceutical Sciences and Biomedical Engineering awarded by the University of Alberta and a Master's degree in law from Stanford University. Sébastien is a technology lawyer and registered trademark agent who advises clients both domestically and internationally on all matters relating to the management and commercialization of intellectual property.*

Carolin Jumaa *has a general corporate commercial and real estate practice. Carolin's corporate commercial experience includes broad exposure to mergers and acquisitions, public offerings and private placements of both equity and debt securities, and corporate reorganizations among a wide variety of other transactional work. Carolin's real estate practice involves the acquisition, disposition, financing and leasing of commercial properties throughout Canada, including office buildings, retail properties, industrial properties, multi-family residential developments and seniors housing.*]

• ONTARIO DIVISIONAL COURT OVERTURNS CERTIFICATION OF INTRUSION UPON SECLUSION CLAIM •

Nicole Henderson, Partner, and Mackenzie Claggett, Summer Law Student, Blake, Cassels & Graydon LLP

Nicole Henderson

Mackenzie Claggett

On June 9, 2021, in *Owsianik v Equifax Canada Co* (*Equifax*), 2021 ONSC 4112, a majority of the Divisional Court overturned the certification of intrusion upon seclusion as a common issue in a class proceeding involving a cyberattack. The decision represents the first time an appellate court has considered the scope of the tort since the Ontario Court of Appeal first recognized it as a cause of action in *Jones v Tsige (Jones)*.

BACKGROUND

In 2017, hackers accessed Equifax's computer network without authorization, allegedly exposing personal and financial information of consumers across North America to the hackers.

The plaintiffs commenced a class action alleging various causes of action, including the tort of intrusion upon seclusion. In the pleadings, the plaintiffs claimed that Equifax knew that its computer network was vulnerable to cyberattacks and chose to do nothing, and that those omissions constituted an intentional or reckless intrusion upon seclusion. This claim represented a novel application of the tort against a defendant who was the victim of a cyberattack perpetrated by a third party.

The tort of intrusion upon seclusion was first recognized in *Jones* in 2012. To make out a claim for intrusion upon seclusion, the plaintiff must show that:

1. The defendant committed an intentional (or reckless) and unlawful intrusion into the plaintiff's affairs;
2. The matter intruded upon was private;
3. The intrusion would be highly offensive to the reasonable person; and
4. The intrusion caused the plaintiff distress, humiliation, or anguish.

Since *Jones*, intrusion upon seclusion has been certified as a common issue in several privacy class actions, although some courts had expressed doubt that such a claim could succeed against a defendant who was not itself an "intruder." A central issue in *Equifax* was whether it was plain and obvious that the plaintiff's intrusion upon seclusion claim was doomed to fail, because the defendant was the victim rather than the perpetrator of the cyberattack.

The motion judge certified the plaintiff's claim for intrusion upon seclusion on the basis that it represented a novel application of the tort. He found that the question of whether a defendant who recklessly permits a cyberattack to occur is liable for intrusion upon seclusion had not yet been settled. For this reason, he concluded it was not plain and obvious that the claim would fail.

DIVISIONAL COURT DECISION

A majority of the Divisional Court held that the plaintiff's claim for intrusion upon seclusion did not disclose a reasonable cause of action and should not have been certified. Accepting the pleaded facts as true, the majority found that Equifax was not an

intruder because it was the hackers that perpetrated the cyberattack. Considering that *Jones* requires the defendant to commit the intrusion, the plaintiffs' claim amounted to more than an incremental development in the law and was doomed to fail. The majority also emphasized that the tort of negligence adequately addressed the conduct alleged by the plaintiff, provided that class members could prove they suffered compensable damages.

The majority relied on recent guidance from the Supreme Court of Canada in *Atlantic Lottery Corp Inc v Babstock (Babstock)* (see *Blakes Bulletin: SCC Waves Goodbye to Waiver of Tort)* that claims – even novel claims that are doomed to fail should be disposed of at an early stage of the proceedings. *Babstock* underscored that such claims present "no legal justification for a protracted and expensive trial." The majority in *Equifax* found that the plaintiff's intrusion upon seclusion claim needed to be vetted at the pleadings stage.

The dissenting judge did not consider *Babstock* to be applicable to this case because the plaintiff alleged a novel application of a recognized tort rather than an entirely new cause of action. She would have found that such a claim constituted an incremental development of the law that should be allowed to proceed to trial for adjudication on its merits.

DISCUSSION

While there may be further appeals, the *Equifax* case represents a significant development in Canadian privacy law, with the majority confirming the status of intrusion upon seclusion as an intentional tort that should not be conflated with negligence. The defendant must be the party to commit the intrusion - intrusion upon seclusion is not a viable cause of action where the plaintiff alleges only that the defendant failed to act to prevent a cyberattack.

The majority judgment also reaffirms the cause of action certification criterion as a meaningful screening tool. *Equifax* confirms that novel claims, including a novel application of a recognized cause of action, should be fully vetted at the pleadings stage if it is possible to do so.

Blakes periodically provides materials on our services and developments in the law to interested persons. This article is for informational purposes only and does not constitute legal advice or an opinion on any issue. Blakes would be pleased to provide additional details or advice about specific situations if desired.

[***Nicole Henderson*** *litigates class actions and other complex disputes, including in the areas of cybersecurity, product liability, and competition. She also practises public law, including constitutional, administrative, regulatory and freedom of information matters. In her cybersecurity practice, Nicole frequently advises organizations dealing with a data breach or information security incident. She also represents defendants in privacy class actions and regulatory investigations arising out of cybersecurity incidents. Nicole has considerable experience in the life sciences industry and regularly acts for leading manufacturers and distributors of pharmaceutical medicines, medical devices and other health products. Prior to joining Blakes, Nicole clerked at the Federal Court of Appeal.*

Mackenzie Claggett *is a second-year summer student in the Competition Group.*]