Canadian Privacy Law Review

VOLUME 18, NUMBER 12 Cited as (2021), 18 C.P.L.R. NOVEMBER 2021

• UPDATE ON THE TREATMENT OF SEALING ORDERS: THE SUPREME COURT OF CANADA'S DECISION IN *SHERMAN ESTATE V. DONOVAN* •

Sanja Sopic, Associate, Stikeman Elliott LLP

• In This Issue •

Sanja Sopic

In *Sherman Estate v. Donovan*, released on June 11, 2021, the Supreme Court of Canada refined the common law test for the granting of sealing orders in civil matters and, in particular, recognized privacy as an important public interest that may warrant sealing relief. This article considers the reasoning behind the Supreme Court's decision and also reviews several subsequent Ontario and British Columbia sealing order rulings that have applied *Sherman Estate*'s refined common law test in commercial contexts.

BACKGROUND

The Open Court Principle

It is a fundamental element of Canadian law that court proceedings are open to the public. Courts have long recognized the importance of the open court principle in preserving the constitutionally protected rights to

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

freedom of expression and freedom of the press under section 2(b) of the *Charter of Rights and Freedoms*.

Nevertheless, courts have the jurisdiction to order that documents, or information filed in court proceedings, be sealed from the public record in certain circumstances. In determining whether to grant such relief, referred to as a "sealing order", courts must weigh the positive effects of protecting confidential or sensitive information against the negative effects arising from restricting access to court files.

History of the Proceeding

In 2017, a prominent couple was found dead in their home. Following the couple's death, their estate trustees sought sealing orders over the court files related to the probate of the couple's estates (the "Probate Files").

The Ontario Superior Court of Justice granted the sealing orders for a period of two years, finding, among other things, that the harmful effects of the sealing orders were outweighed by their beneficial effects on the privacy of the affected individuals, including the beneficiaries of the estates.

A journalist and the newspaper for which he wrote appealed the Ontario Superior Court decision, arguing that the sealing orders violated the open court principle and the constitutional rights of freedom of expression and freedom of the press.

The sealing orders were unanimously lifted by the Ontario Court of Appeal (2019 ONCA 376), which concluded, among other things, that the privacy concerns of the estate trustees were insufficient to justify the sealing orders that had been granted.

The Court of Appeal's order setting aside the sealing orders was stayed pending the disposition of the appeal to the Supreme Court of Canada, which was brought by the estate trustees.

THE SUPREME COURT OF CANADA'S DECISION

Central to the appeal was the issue of whether protecting the privacy of the individuals affected

by the Probate Files amounts to an important public interest that could justify the sealing of the Probate Files under the applicable legal test for discretionary limits on court openness. Established by the Supreme Court of Canada in *Sierra Club of Canada v. Canada (Minister of Finance)*, that test requires a party seeking a sealing order to show that:

- a sealing order is necessary to prevent a serious risk to an important interest, including a commercial interest, because alternative measures would not prevent the risk; and
- the positive effects of the sealing order outweigh the negative effects, including the public interest in open court proceedings.

The Supreme Court's Analysis

In *Sherman Estate,* the Supreme Court found that the *Sierra Club* test requires that three "core prerequisites" be established in order to obtain a sealing order:

- court openness poses a serious risk to an important public interest;
- the sealing order sought is necessary to prevent the serious risk to the identified interest because reasonably alternative measures will not prevent this risk; and
- as a matter of proportionality, the benefits of the sealing order outweigh its negative effects.

Since *Sierra Club*, the jurisprudence has established that a sealing order will only be granted if the interest sought to be protected has a public component (such as, for instance, the public interest in upholding confidentiality agreements or in protecting the integrity of judicial proceedings).

Notably, the Supreme Court in *Sherman Estate* recognized an aspect of privacy, namely the preservation of individual dignity, as an important public interest, and held that this interest is sufficiently important that it may justify an exception to the open court principle. The Supreme Court characterized dignity as "the right to present core aspects of oneself to others in a considered and controlled manner".

Writing for a unanimous Court, Justice Kasirer cautioned that the presumption in favour of open courts cannot be overcome lightly, and reasoned that the public interest in preserving dignity will only be at risk where the information sought to be protected:

> …strikes at what is sometimes said to be the core identity of the individual concerned: information so sensitive that its dissemination could be an affront to dignity that the public would not tolerate, even in service of open proceedings.

The Court went on to note that examples of such sensitive information include stigmatized medical diagnoses, stigmatized work, sexual orientation, and subjection to sexual assault or harassment.

The Supreme Court's Decision

Applying this framework, the Supreme Court dismissed the appeal on the basis that, among other things, the information at issue in the Probate Files was not of such a highly sensitive character that it engaged the dignity of the affected individuals.

Notably, Justice Kasirer remarked that even if a serious risk to a privacy interest had been established, it would likely not have justified a sealing order because alternative measures, such as a publication ban, would likely have prevented this risk.

APPLICATION OF *SHERMAN ESTATE* TO RECENT SEALING ORDER REQUESTS

Ontario

While *Sherman Estate* did not address sealing order requests made in the commercial context, a number of recent decisions of the Ontario Superior Court of Justice (Commercial List) (the "Ontario Court") have cited *Sherman Estate* in considering whether to grant sealing order relief, including:

- In the receivership proceedings of Canadian investment management firm Bridging Finance Inc. (*Ontario Securities Commission v. Bridging Finance Inc.*, 2021 ONSC 4347), Chief Justice Morawetz applied the Supreme Court's analysis in *Sherman*

Estate in approving the sealing of: (i) a key employee retention plan containing confidential and personal information with respect to the compensation of each eligible employee; and (ii) information regarding the receiver's recommended course of action in connection with a proposed repayment transaction whose terms were confidential.

- In the *Companies' Creditors Arrangement Act* (the "CCAA") proceedings of Guardian Financial Corporation and certain related entities – affiliates of a U.S. company that operates a network of co-working spaces in the United States and Canada – Justice Dietrich relied on *Sherman Estate* in approving the sealing of a lease amending agreement, finding that it contained commercially sensitive information about lease negotiations.
- In the CCAA proceedings of Laurentian University of Sudbury ("Laurentian") (*Re Laurentian University of Sudbury*, 2021 ONSC 4769), Chief Justice Morawetz considered whether to seal an unredacted version of a proposal prepared by a real estate advisor sought to be engaged by Laurentian. According to Laurentian, the proposal contained commercially sensitive and proprietary information that could jeopardize the business of the real estate advisor if disclosed publicly and made available to competitors. Drawing on the *Sherman Estate* decision, Chief Justice Morawetz expressed concerns about the scope of the sealing relief sought, noting that certain aspects of the proposal did not appear to contain commercially sensitive and proprietary information. Counsel to Laurentian subsequently disclosed certain portions of the proposal related to the real estate advisor's pricing and budget, thereby narrowing the scope of the requested sealing order, which order was granted.

British Columbia

The British Columbia Supreme Court (the "B.C. Court") has also drawn on the *Sherman Estate* decision in deciding whether to grant a sealing order. In the recent decision of *United States v. Meng*, 2021 BCSC 1253, the B.C. Court declined to seal certain bank documents in the extradition proceedings of Wanzhou Meng, the Chief Financial Officer of Huawei, a telecommunications company. The extradition proceedings involved allegations that Ms. Meng misled a bank into facilitating certain transactions in violation of U.S. sanctions against Iran. The documents sought to be sealed included bank reports and high-level bank communications relating to strategy and decisions about its business with Huawei.

In considering the sealing request, the B.C. Court acknowledged that commercial information may engage privacy interests that may give rise to an important public interest. Applying the *Sherman Estate* analysis, the B.C. Court reasoned that the commercial confidentiality interest at issue did not engage an important public interest as it was specific to the bank. The B.C. Court further held that, even if the bank's interest in preserving the confidentiality of its internal documents could be characterized as an important public interest, that interest was not shown to be at serious risk from the publication of the documents since some of the documents had already been summarized in the proceedings and were heavily redacted. Notably, the B.C. Court held that it expected the identities and contact information of the bank representatives in the documents to be redacted in accordance with an earlier "media protocol" established in the proceedings.

KEY TAKE-AWAYS

- The Supreme Court's decision in *Sherman Estate* emphasizes the importance of the open court principle as a reflection of the constitutionallyprotected right of freedom of expression.
- As such, and in keeping with the recent decisions noted above, there may be greater judicial scrutiny of sealing order requests going forward, including in the commercial context.
- Parties seeking sealing relief in the future should bear this in mind, and may want to consider

whether alternative measures, such as redaction, could be used to prevent the disclosure of commercially sensitive information.

This article was first published on Stikeman Elliott LLP's Knowledge Hub and originally appeared at www.stikeman.com.

[***Sanja Sopic*** *is an associate in the Litigation & Dispute Resolution Group at Stikeman Elliott. Her practice focuses on restructuring and insolvency matters representing debtors, court officers, creditors, purchasers and other stakeholders in proceedings under the Bankruptcy and Insolvency Act and the Companies' Creditors Arrangement Act. Sanja was recognized by Best Lawyers in Canada 2022 as "One to Watch" in Corporate and Commercial Litigation, and Insolvency and Financial Restructuring.*]

• MIXED RESULTS IN PRIVACY CLASS ACTION AGAINST DOCTOR WHO ALLEGEDLY FILMED PATIENTS •

Henry Ngan, Senior Associate, Borden Ladner Gervais LLP

Henry Ngan

A plastic surgeon alleged to have filmed his patients with surveillance cameras faced a privacy class action case.

In *G.C. v. Jugenburg* (2021 ONSC 3119), the Ontario Superior Court certified a privacy breach class action against Dr. Martin Jugenburg, but declined to certify a class action for patients whose images were posted on the internet, published, or otherwise displayed in a public setting, allegedly without their consent.

BACKGROUND

The defendant operated a plastic surgery clinic in Toronto.

In January 2017, the clinic completed installation of 24 continuously-operating cameras. The cameras were located across the clinic except for the washrooms. They were not hidden, but were also not overly noticeable. Between January 2017 and December 2018 there was only one sign, located in an operating room that disclosed the presence of a surveillance camera. Clinic staff did not let patients know there were cameras throughout the premises.

Dr. Jugenburg maintained that the cameras were installed for security purposes, not for patient care or any nefarious or voyeuristic purposes.

In 2016, the defendant began marketing himself on various social media platforms. He shared photos and videos of clinic patients, including ones taken during surgery. The patients were not named and their faces were blurred or cropped out. The clinic had a consent procedure with respect to posting of images on the internet or social media.

Following exposure by CBC's *Marketplace* in December 2018, the media coverage and regulatory

actions resulted in the cameras being shut down and seized. Professional disciplinary proceedings also began against Dr. Jugenburg.

Patients of the defendant brought a class action on behalf of two classes:

- Approximately 2,500 patients who attended the clinic when the surveillance cameras were operational (the Surveillance Class); and
- An undetermined number of patients whose images were posted on the internet, published or otherwise displayed publicly, and who claimed they were published without their consent (the Internet Class).

CLASS ACTION CERTIFIED FOR THE SURVEILLANCE CLASS, BUT NOT THE INTERNET CLASS

Justice Perell certified a class action for the Surveillance Class on common issues related to negligence, vicarious liability, breach of trust and fiduciary duty, intrusion upon seclusion, and damages.

However, Justice Perell did not agree there had been public disclosure of private facts because this tort must be determined on a case-by-case basis. He also did not find evidence that Dr. Jugenburg had been unjustly enriched at the expense of the patients, and did not certify the unjust enrichment claims.

Furthermore, Justice Perell declined to certify the Internet Class altogether, holding that the "holy grail" issue relating to the Internet Class is whether their informed consent was valid.

While the clinic had a policy for getting informed consent before putting patient images and videos online, Justice Perell concluded that whether valid informed consent was obtained is inherently an individualistic issue. It depends on characteristics such as a patient's understanding of what they were consenting to, which in turn is based on their exposure to social media and the clinic's presence on social media. Due to the varied nature of the procedures, the degree of privacy breach was also individualistic. In sum, Justice Perell found there was no basis in fact for any common issue for the Internet Class.

PLAINTIFFS RECEIVE FULL AGREED-ON COSTS

Before the certification motion, the parties agreed to costs in the amount of $150,000.

Following Justice Perell's decision, the defendant argued that costs should not be paid because the plaintiffs were only partially successful.

In a costs decision (2021 ONSC 5213), Justice Perell disagreed with the defendant and awarded the full amount of the agreed-upon costs to the plaintiff. According to Justice Perell, this was justified because the parties came to an agreement when the claims of the Surveillance Class and Internet Class were joined as a singular action.

TAKEAWAYS

Privacy breach class actions remain viable in Ontario when they are based on torts such as negligence, breach of fiduciary duty, and inclusion upon seclusion against defendants alleged to have deliberately invaded plaintiffs' privacy. However, Justice Perell confirmed that courts will carefully scrutinize the existence of common issues where an element of informed consent is involved in the exchange. Furthermore, Justice Perell confirmed that the tort of "public disclosure of private facts" is individualistic and may be unsuitable for a class action.

The costs result is also noteworthy, and serves as a cautionary tale that parties entering into cost agreements should take into account situations where the plaintiffs may only have partial success, especially when the certification of multiple classes are sought.

[***Henry Ngan*** *is a Senior Associate at Borden Ladner Gervais LLP. He represents healthcare institutions and providers in civil liability claims and administrative law proceedings. Henry also advises his clients on a variety of risk, quality, compliance and incident-related matters.*]

• MANDATORY VACCINE POLICY IN THE WORKPLACE: AN OVERVIEW FOR CANADIAN EMPLOYERS •

Justine B. Laurier, Partner, Vanessa Lapointe, Associate, Danny J. Kaufer, Senior Counsel & Co-Chair, Sports & Gaming Law Group, and Stuart S. Aronovitch, Partner Borden Ladner Gervais LLP

Justine B. Laurier

Vanessa Lapointe

Danny J. Kaufer

Stuart S. Aronovitch

CONSIDERATIONS FROM THE LEGAL PERSPECTIVE

As the COVID-19 vaccine becomes more widely available, many employers worldwide have been exploring the idea of mandatory vaccination for employees as a condition of access to the workplace (and a variety of questions related to it). Although employers are eager to move forward with this solution, mandatory vaccine policy may carry important legal implications, depending on where employees live.

Employers may first want to ask themselves a few more questions before taking action, including:

Why Do Employers Want Their Employees to be Vaccinated?

The answer may seem obvious, since governments and the media alike have promoted the vaccine as the ticket back to "normal" life (including the workplace).

Employers may indeed wish to protect the health and safety of their employees by restricting access to the workplace to only fully vaccinated individuals, as it is their statutory duty in all Canadian provinces. However, Canadian employers face a complex issue; they must determine whether the obligation to protect an employee's health and safety justifies the encroachment upon employees' privacy and human rights protections under Canadian law. Unfortunately, the answer to this question is not obvious. Our neighbours to the South have clearly taken the approach of requiring vaccination as a condition for accessing the workplace in many instances. It may be time to question whether the rise of virus variants and the growing number of cases worldwide will drive our governments in Canada to take a similar approach. We have already seen one province implement a vaccination passport system in anticipation of a fourth wave. As such, people will be required to present their proof of vaccination via the passport system to access certain public spaces and non-essential businesses (not for work purposes). These actions are far-reaching and probably would not even have been even contemplated some three months ago. While this specific government measure does not currently require employers to impose such conditions on their employees, ultimately, there may be more significant support for this kind of proposition in the future. Employers may have to adopt similar measures to uphold and justify their obligation to provide a safe and healthy workplace.

However, this is the question that employers may want to be asking themselves today:

Is Mandating Vaccination the Most Efficient Way for Employers to Meet Their Duties, While Mitigating Legal Risks?

Although mandatory vaccination poses potential legal risks, such as human rights and privacy claims,

some employers are willing to move forward with implementing these measures. They would require employees to be fully vaccinated should they want to return to the workplace and engage in specific tasks involving physical contact with the public, clients or business travel. While mandatory vaccination involves risks, other preventive measures can help curb quite effectively the transmission of the COVID-19 virus in workplaces (*e.g.* offices, retail, etc.) and thus expose employers to fewer risks of a legal challenge. Still, to demonstrate the commitment of certain employers, let us look at some recent developments in the U.S.A. Several major law firms have recently stated that only fully vaccinated employees will have access to their offices. At least one firm declared that employees who are not fully vaccinated would have their access cards to enter the building, and their specific offices, deactivated.

Further, many Fortune 100 and 500 companies have taken the public position that their employees must be vaccinated to work and travel for the company. These actions may again show that employers are taking a bolder approach to their obligation to protect their employees' health and safety. In the context of the Delta variant and the approach of a 4th wave, the health and national security argument seems to have taken precedence over privacy and human rights protections.

Can this type of approach be adopted in Canada, and if so, when? As this is a quick-moving issue, it is very possible that companies in Canada may take a more aggressive approach if the situation in the fall deteriorates. Businesses will most likely be forced into rolling back their return to office plans due to the Delta variant and its effect on the number of cases. However, companies cannot ignore the realities of the Canadian legal landscape at this time.

OVERVIEW OF APPLICABLE CONSIDERATIONS

First, employers with operations outside of Canada may be surprised to discover that imposing vaccinations on employees in Canada is not a widespread practice in our jurisdiction as it may be, for instance, south of the border. This can be explained by the specific legal considerations to contend with when contemplating mandatory vaccination in Canada, such as human rights and privacy laws. The thresholds to meet in Canada are particularly high, and so are the possible legal risks related thereto.

What are the Main Legal Considerations Canadian Employers Must Keep in Mind When Contemplating Requiring Vaccination as a Condition to Access to the Workplace?

Privacy

In most Canadian provinces, an employer may collect, use or disclose personal employee information only with their consent and for reasonable purposes.

In order to impose vaccination as a condition to access the workplace, an employer would necessarily need to ask its employees: "Are you vaccinated?", which would qualify as the collection of personal information. Hence, to do so, not only would employees need to consent to the collection of such information, but employers would need to be able to demonstrate that they are requesting this information for a reasonable purpose. The following are examples of circumstances that, in the event of a legal challenge, our tribunals may potentially consider as a reasonable purpose for the collection of such data in connection with a mandatory vaccination requirement:

- A very high risk of COVID-19 transmission in the specific workplace of the employer (compared to society at large), due to intrinsic characteristics present at the time the mandatory vaccination policy is in place;
- The impossibility (or high impracticality) of implementing other less intrusive measures; and
- The demonstrable inefficacy of other less intrusive measures due to the nature of the work/ the workplace.

Even where such circumstances are not present, one may argue that this question is being asked to protect the health and safety of ALL employees and this is not an interference with anyone's privacy

rights. At the present time, the majority view seems to be that this need to protect the employee's health and safety would not in itself constitute a reasonable purpose. However, this has not been tested and the argument is not only attractive but it is also a very real and plausible one.

Human Rights

Vaccination is an invasive medical treatment, a personal decision for which individuals should have the option to consent to or not.

Further, pursuant to federal and provincial human rights legislation, employees may refuse to receive the vaccine based on prohibited grounds of discrimination (which may include, depending on applicable legislation, disability (interpreted to include "medical conditions"), and religion). A mandatory vaccination policy would need to be reasonably justified and necessary, along with other, less invasive measures being insufficient to protect employee health and safety. In addition, it would also need to account for an employers' obligation to provide reasonable accommodation to employees who refuse to be vaccinated based on such protected grounds, up to the point of undue hardship. Namely, in the province of Québec, this question becomes even more complex as human rights legislation limits employers in even asking job candidates about protected grounds of discrimination, making mandatory vaccination all the more difficult to contemplate and implement. While these are very real concerns, employers may still have arguments to consider.

For example, employers may be able to contest the true continued feasibility of remote work. Are companies really getting the work they require from the employees working from home? Would employers be justified in concluding and arguing that these considerations have now become an instance of undue hardship? While this type of argument may not work in all circumstances, there may be situations where it would prevail. Employers must be consider these types of decisions on a case-by-case basis, a "one size fits all" approach does not apply in these circumstances.

CONCLUSION

While many employers perceive the vaccine as a great tool for medical protection, it is clear that it can also pose a legal threat.

Other options are available which, in the absence of clear science on the vaccine's efficacy, may well protect the workplace just as efficiently, or even more so. Employers should certainly not rely on the fact that their employees are vaccinated to let sanitary and distancing measures fall to the wayside, especially for employees in areas where these procedures are is still mandatory or recommended.

Ultimately, employers imposing any measure that potentially affects their employees' rights should be prepared to defend their decisions in case of a legal challenge. To assist them in doing so, they should notably ask themselves the following questions throughout the process:

- Are the measures imposed necessary and justifiable, given the specific circumstances of our workplace, in light of our business context and reality?
- Are we using the least intrusive measure possible to reach our goal (in other words, is imposing the vaccine on our employees the most efficient way to avoid the risk of contagion)?
- Are we complying with all other applicable legislation and up-to-date government/labour board/health authorities' guidelines?
- Are we protecting employee privacy at all times?
- Are we complying with human rights legislation and accommodating employees where necessary (*e.g.* religious and medical reasons)?

As employees start to return to work in great numbers and employers prepare for the fall, employees will inevitably have questions regarding the future of their workplace. We believe that all employers should seriously consider having a telecommuting or remote work policy to help manage the return to the office, especially with the reduced health measures planned by the various governments. In addition, this approach considers the most effective method to curb the transmission of the virus in your work environment.

Despite the legal risks of imposing the vaccine onto employees, some will decide to proceed in this way. We believe that some employers may be justified in doing so, keeping in mind that they are not immune to legal challenges. A well-thought-out plan in preparation for return to work could help employers demonstrate to the court or tribunal that the decision was considered and weighed appropriately before taking action.

[***Justine B. Laurier's*** *practice focuses on all areas of labour and employment law for both federally- and provincially-regulated undertakings. She specializes in complex litigation and is trusted by clients to handle their most sensitive matters. Justine provides strategic advice on collective labour relations to numerous companies.*

Vanessa Lapointe *represents the interests of unionized and non-unionized companies of all sizes in matters ranging from prevention to representation. Vanessa advises both federally and provincially-regulated companies and represents them before civil courts and administrative tribunals.*

Danny J. Kaufer *is widely recognized for his expertise in negotiation and arbitration and has been involved in many high-profile certification matters. He represents employers before federal and provincial authorities as well as before various arbitration boards across Canada.*

Stuart Aronovitch's *practice covers a broad range of labour, employment and human rights law, with an emphasis on employment contracts and related disputes. Stuart is an experienced litigator, having represented clients before a wide range of courts and administrative tribunals, including the Tribunal administratif du travail, grievance arbitrators, the Superior Court of Québec and the Court of Appeal of Québec.*]

• PRIVACY IN CIVIL SEXUAL ASSAULT CASES •

Loretta P. Merritt, Partner, Torkin Manes LLP

Loretta P. Merritt

Privacy is often, but not always, a concern to plaintiffs in civil sexual assault cases. This article will discuss keeping the plaintiff's identity confidential as well as production of confidential records. The law treats sexual assault survivors' privacy very differently in criminal and civil cases.

In criminal cases involving sexual assault (particularly historical cases), Crown Attorneys usually seek and obtain publication bans preventing everyone from publishing any information which would identify the complainant. In civil cases, plaintiffs sometimes wish to keep their identity confidential and proceed using a pseudonym. It is up to the plaintiff to decide if they want to proceed anonymously. In my experience generally defendants do not object to this procedure, particularly institutional defendants such as churches, school boards, children's aid societies, etc. However, if the issue is contested, ultimately the court will decide whether the plaintiff can proceed using a Jane/John Doe pseudonym. Factors the court will consider include whether there has been a publication ban in a related criminal proceeding, whether the case has already received media attention, whether the case may be a matter of interest to the media, whether the identity of the plaintiff is a matter of public interest, whether the plaintiff or other sexual abuse survivors will be deterred from reporting abuse if they are publicly scrutinized, whether the plaintiff will suffer psychological harm if their identity is not kept confidential and whether the defendant will suffer any prejudice as a result. When a motion is brought, there

is a Practice Direction in Ontario requiring that the media be put on notice of the motion. I have never had a case where the media responded or tried to participate in a pseudonym motion where we were simply trying to keep the plaintiff's identity confidential (as opposed to sealing the entire court file).

In October, 2020 the Nova Scotia Court of Appeal[1] decided a case involving a Confidentiality order (pseudonym motion) in a civil sexual assault case. In that case, a publication ban had been issued in a related criminal proceeding. In the subsequent civil case the judge gave the plaintiff (who sought to protect her privacy) a Confidentially Order allowing her to keep her identity confidential. On appeal, the court said that a confidentiality order was not necessary because the complainant was already protected by the pre-existing criminal publication ban. The court said that when information in a civil matter can identify the complainant from a criminal case, the publication ban prevents its publication. This case seems to suggest that in some circumstances a pseudonym motion in the civil case may not be necessary if there is a publication ban in the criminal case. However, I wonder what this means for a sexual assault survivor who wishes to go public with his or her name. In some cases, plaintiffs do not wish to keep their identity confidential. Could suing civilly be a violation of the criminal publication ban?

Until recently, I never gave it much thought when issuing a civil claim using the plaintiff's own name (when instructed to do so by my client). However, in April, 2021 a sexual assault survivor was charged criminally and fined $2,600 for violating a publication ban on her own identity. As is often the case, the Crown attorney in the criminal case sought and obtained a publication ban preventing anyone from publishing the identity of the sexual assault complainant. At the criminal trial, the sexual assault complainant was not in court when the Crown asked for the publication ban, the ban was not discussed with her and she did not consent to it. After the trial was over the sexual assault complainant sent a copy of the transcript to some of her family and friends. The perpetrator complained after he learned about it. The woman was charged and was fined. Fortunately, in May, 2021, she successfully appealed her conviction. The Crown conceded and the appeal judge set aside the conviction and the money she was fined was returned to the complainant. Clearly, the purpose of publication bans in sexual assault cases is to protect the privacy rights of complainants and they should not become a vehicle to take away autonomy from them. It would be a sad state of affairs if complaints who do not want a publication ban have to ask a Crown Attorney to bring a motion to the court to lift them. As has been suggested by Lisa Taylor, Associate Professor, Ryerson School of Journalism, the best solution is to change the law to provide that publication bans do not apply to the complainant.

There is also a different approach in civil and criminal case when it comes to medical and other confidential records. In criminal cases, the courts recognize the complainant's right to privacy with regard to their medical records. There is a strict legal test and procedure to be followed if the defendant wants access to those records. The same is not true in civil cases. If a plaintiff claims that their life has been affected by a sexual assault and they have suffered damages as a result, they will be required to produce records that are relevant to those issues. Typically they will be required to produce therapy and other medical records and if income loss is claimed, employment and tax records. What records are producible depends on the nature of the claim and if production is a concern it should be considered before the claim is issued. If there is information in the records that is confidential and not relevant, the records may be redacted.

In any case, before starting a civil lawsuit, a plaintiff is well advised to consider what privacy rights and confidentiality protections may be afforded to him or her.

[***Loretta P. Merritt*** *is one of the few lawyers in Ontario who has substantial experience in dealing with abuse and harassment in civil lawsuits and employment cases. She understands and cares about abuse survivors, recognizing that coming forward, being heard and acknowledged as well as gaining a sense of justice and closure, in addition to the amount of a settlement, are what matter to her clients. She has represented hundreds of clients in a variety of*

historical and recent sexual and physical abuse cases, including abuse by members of clergy, doctors, police officers, teachers, relatives and neighbors.]

[1] *United Kingdom of Great Britain and Northern Ireland (Attorney General) v. L.A.,* 2020 NSCA 75, and for more about this case see Loretta P. Merritt, "Publication Bans: Do They Help or Hurt Abuse Survivors? *Torkin ManesLLP* (December 2020), online: <https://www.sexualabuselawyer.ca/resources/publications/details/publication-bans-do-they-help-or-hurt-abuse-survivors>.

• END OF CLAUSE-BY-CLAUSE CONSIDERATION OF BILL 64: WHERE WE STAND •

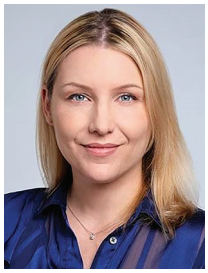
Éloïse Gratton, Partner and National Co-leader, Privacy and Data Protection, Elisa Henry, Partner and National Co-leader, Privacy and Data Protection, François Joli-Coeur, Senior Associate, Max Jarvie, Senior Associate, Julie M. Gauthier, Counsel, Andy Nagy, Associate, and Simon Du Perron, Associate, Borden Ladner Gervais LLP


Éloïse Gratton


Elisa Henry


François Joli-Coeur


Max Jarvie


Julie M. Gauthier


Andy Nagy


Simon Du Perron

On August 24, the Committee on Institutions of the Québec National Assembly completed its clause-by-clause consideration of Bill 64, *An Act to modernize legislative provisions as regards the protection of personal information* (Bill 64), which had begun in February 2021. In our previous bulletin,[1] published at the end of the parliamentary proceedings in June, we discussed key changes made to Bill 64 up to this date.

Building on these previous developments, this bulletin highlights the most recent round of amendments passed in the few Committee sessions held in August. We invite you to consult our amended version of the *Act respecting the protection of personal information in the private sector* (*Private Sector Act*) for the exact wording of these amendments.

When the Committee reconvened, it had moved on to the consideration of section 124 of Bill 64 (of which there are 165 in total), which introduced an amendment to section 46 of the Private Sector Act. However, a few earlier sections of Bill 64 that had been suspended were revisited by the Committee in order to be considered for adoption; our review begins with discussion of these.

PRIVACY BY DESIGN / BY DEFAULT

The Committee revisited and ultimately adopted section 100 of Bill 64 in a slightly amended form. This section enshrines the principle of privacy by default in the Private Sector Act by introducing section 9.1, which reads as follows:

> 9.1. *Any person carrying on an enterprise who collects personal information by offering to the public a technological product or service that has privacy parameters must ensure that, by default, the parameters of the product or service provide the highest level of confidentiality without any intervention by the person concerned.*
>
> *The first paragraph does not include the privacy settings of a cookie.*

The government's amendment clarifies three elements regarding the application of the privacy by default requirement. First, it does not apply to technological products and services used internally by a business' employees (e.g. intranet, back-to-the-office mobile app). Second, section 9.1 applies only when a technological product or service has privacy settings, such as a social networking account, a search engine or a mobile application. Finally, section 9.1(2) specifies that cookies are outside the scope of the provision. In this regard, the government has indicated that cookies are excluded since they are not "customizable".

The practical consequences of section 9.1 of the Private Sector Act for businesses operating in Québec are difficult to assess, particularly given the uncertainty surrounding the meaning of the term "highest level of confidentiality". Moreover, the intent of the legislator with this new section is also difficult to ascertain since the notion of privacy by design and/or by default was used in different ways during the Committee's deliberations, notably in relation to the obligation to conduct privacy impact assessments (PIA) (s. 3.3), the need to obtain express consent for the processing of sensitive personal information (s. 12(1)) and the requirement to disable technological functions that allow a person to be identified, located or profiled (art. 8.1(1)(2)). However, when Bill 64 was introduced, the government viewed this principle as requiring businesses to ensure that the privacy settings of their products and services guarantee that personal information collected will not be shared with an unspecified number of persons (whether organizations or individuals) without the consent of the individual concerned.[2]

DATA PORTABILITY RIGHT

The government also adopted an amendment to resolve the ambiguity surrounding the application of the portability right to personal information inferred or derived by a business from other information provided by the individual. Thus, section 27(3) of the Private Sector Act now provides that an individual may request that personal information collected from them, and not created or derived from their personal information, be communicated to them (or to another organization designated by the individual) in a structured, commonly used technological format.

In this regard, the government has clarified that the purpose of the portability right is to allow an individual to be able to retrieve the information they have provided to the business (and nothing more). Thus, the amendment aims to prevent the portability right from being used in such a way as to force a business to share data it has produced using proprietary methods with one of its competitors.

PERSONAL INFORMATION AGENTS

New provisions regarding personal information agents have been adopted. As a reminder, the Private Sector Act defines this role as including "Any person who, on a commercial basis, personally or through a representative, establishes files on other persons and prepares and communicates to third parties credit reports bearing on the character, reputation or solvency of the persons to whom the information contained in such files relates is a personal information agent" (s. 70(2)). Businesses in the field of credit or debt collection, or those who carry out private investigations or identity checks on individuals, are generally considered to be personal information agents.

Under the new provisions introduced by Bill 64, personal information agents will be required to:

- File a registration request with the Commission d'accès à l'information (CAI) accompanied with the required fees (s. 72);
- Provide various information to the public, including the fact that it holds personal information about other persons and, if applicable, credit reports, how to exercise access and rectification rights and the contact information of the person in charge of the protection of personal information (s. 79);
- Adopt rules of conduct to allow any person to whom personal information held by an agent relates to have access to the information and to have it rectified (s. 78);
- Destroy personal information after a seven-year retention period (s. 79.1).

It should be noted that the CAI maintains a register of personal information agents that is publicly available. The CAI specifies, however, that registration does not guarantee compliance with the Private Sector Act. Furthermore, it is important to remember that a personal information agent who fails to comply with the requirements prescribed by the Private Sector Act may be subject to monetary administrative penalties and/or penal fines.

POLITICAL PARTIES

The Committee also adopted two new sections to the *Election Act*. Section 127.22 provides that the Private Sector Act applies to personal information about electors held by a political party, an independent deputy or independent candidate. As a result, political parties will have to designate a person in charge of the protection of personal information. It should be noted, however, that individuals will not be able to exercise their right of access, rectification or deletion with respect to personal information held by a political party since these provisions have been specifically excluded from the scope of section 127.22.

In addition, section 127.23 states that political parties may collect only electors' personal information that is necessary for election purposes, political financing, or for the purpose of a political activity as defined in section 88 of the Election Act. This provision also requires political parties to obtain the consent of individuals concerned when collecting or using their personal information. Consent may be implied, for example, when an elector responds to a request concerning their intention to vote.

CAI INVESTIGATION PROCEDURE

The procedure for conducting investigations by the CAI's surveillance section has also undergone some changes. From now on, any person, whether qualified as having an interest in the matter or not, will be able to file a complaint with the CAI so that it may investigate any matter relating to a business' information handling practices. This complaint may be made anonymously (s. 81). In order to carry out its investigation, the CAI may require the production of any information or document (s. 81.2 and 83.1). Refusal to cooperate with an investigation or to provide the required documents will be considered a penal offence punishable by a fine.

In addition, a "whistleblower protection" provision prohibiting businesses from taking reprisals (e.g., demotion, suspension, dismissal, transfer or other disciplinary measure) against a person for having filed a bona fide complaint with the CAI or cooperated in an investigation has been introduced (s. 81.1).

It is also worth mentioning the new section 81.3 of the Private Sector Act, which gives the CAI the power to order any person involved in a confidentiality incident to take any measure to protect the rights of the individuals concerned, including an order that the compromised personal information be returned to the business or be destroyed. While it is questionable whether the CAI will be able to actually enforce such orders in many circumstances, such as an order directing a threat actor to surrender or destroy the personal information exfiltrated from a business' network, it is interesting to see the government recognize a more active role for the CAI in managing confidentiality incidents.

MONETARY ADMINISTRATIVE PENALTIES AND PENAL OFFENCES

The Committee adopted the controversial regime allowing the CAI to impose monetary administrative penalties (more commonly known as "administrative monetary penalties" or "AMPs"). The maximum amount of penalties is set at $50,000 for an individual and $10,000,000 or 2 per cent of worldwide turnover for a legal entity (s. 90.12). The grounds on which the CAI may impose an AMP are:

- Failure to provide a proper privacy notice to individuals in accordance with sections 7 and 8 of the Private Sector Act; [3]
- Collecting, using, communicating, holding or destroying personal information in contravention with the provisions of the Private Sector Act;
- Failure to report a confidentiality incident to CAI or affected individuals in contravention of section 3.5 of the Private Sector Act;
- Failure to take appropriate security measures to protect personal information in accordance with section 10 of the Private Sector Act;
- Failure to inform the individual concerned by a decision based solely on an automated process of his or her personal information or giving the individual an opportunity to make representations, in contravention of section 12.1 of the Private Sector Act;
- For a personal information agent to contravene sections 70, 70.1, 71, 72, 78, 79 or 79.1 of the Private Sector Act.

It should be noted that section 90.1 of the Private Sector Act provides that AMPs will be imposed by "a person designated by the Commission, but who is not a member of any of its divisions". The fact that the status of the person in charge of administering and imposing AMPs is left uncertain is concerning, especially considering the significant penalties that can be imposed under this new regime. That said, this issue may be resolved in the general framework for the application of monetary administrative penalties to be developed by the CAI pursuant to section 90.2 of the Private Sector Act, which the government has indicated may be similar to the one developed by the Minister of the Environment and the Fight Against Climate Change (available in French only).

In addition, the Committee adopted an amendment to section 90.1 introducing a mechanism by means of which a business can acknowledge its failure to comply with applicable legal requirements and enter into an undertaking with the CAI to remedy the contravention or mitigate its consequences. Where such an undertaking is accepted by the CAI, the business cannot be subject to an AMP with respect to the acts or omissions covered by the undertaking (s. 90.1(2) and (3)).

In this regard, it is relevant to note that the government has repeatedly emphasized that the purpose of the AMP regime is to ensure compliance with the Private Sector Act's requirements. Thus, unlike fines that may be imposed following a penal offence, AMPs are not intended to be punitive. The government has also clarified that a business that has received an AMP and continues to violate the law could subsequently be fined under the penal regime. In other words, the two regimes are not mutually exclusive.

The Committee also adopted the amendments made by Bill 64 to the penal provisions of the Private Sector Act. Thus, the offences set out in section 91 encompass the grounds for the imposition of an AMP, with the addition of the following:

- Contravening the prohibition formulated in section 8.4 of the Private Sector Act (introduced by section 108 of the *Credit Assessment Agents Act*) against obtaining communication of personal information that is subject to a security freeze;
- Identifying or attempting to identify a natural person using de-identified information without the authorization of the person holding the information or using anonymized information;
- Obstructing an investigation or inspection by the CAI or the processing of an application by the CAI by, among other things, providing false or inaccurate information or failing to provide required information;

- Taking reprisals against whistleblowers in contravention of section 81.1 of the Private Sector Act;
- Refusing or neglecting to comply, within the specified time, with the CAI's request to produce information or a document as per section 81.2 of the Private Sector Act; or
- Failing to comply with an order from the CAI.

The maximum fine that can be imposed for a penal offence is $100,000 for a natural person and $25,000,000 or 4 per cent of worldwide turnover for a legal entity (s. 91). Moreover, the maximum amount for a natural person has been increased from $50,000 to $100,000 to distinguish the penal regime from the administrative regime and to reflect its dissuasive nature.

The statute of limitations for an AMP is 2 years from the date of the contravention (s. 90.10), whereas it is 5 years for penal offences (s. 92.2). An AMP can be contested before the Court of Québec (s. 90.9) whereas a penal sanction, which is imposed by a judge of the Court of Quebec, is subject to a right of appeal to the Superior Court (s. 270 Code of Penal Procedure).

PRIVATE RIGHT OF ACTION

The Committee also adopted an amendment to replace section 93.1, proposed by section 152 of Bill 64, with the following:

> 93.1. *Where an unlawful infringement of a right conferred by this Act or by sections 35 to 40 of the Civil Code causes an injury and the infringement is intentional or results from gross negligence, the court shall award punitive damages of not less than $1,000.*

The Minister's comments indicate that the goal of the amendment is to ensure that the recourse provided for in this section is subject to the general rules of civil liability. However, section 93.1 is now limited to recognizing the court's authority to sanction an unlawful infringement of a right conferred by the Act or by sections 35 to 40 of the Civil Code with punitive damages where the infringement is intentional or results from gross negligence. The notion of a private right of action, *i.e.* the possibility for an individual to bring a civil claim against a business for compensation for an injury caused by a breach of the Private Sector Act, seems to have been set aside. However, given the lack of clear legislative intent in this regard, it is advisable to await clarification either during the final adoption debate or from the CAI before jumping to conclusions.

NEXT STEPS

There are only two steps left in the legislative process of Bill 64 in the National Assembly, namely the consideration of the Committee's report and the final passage debate. These two sessions will allow the Committee's members to present to their fellow members of Parliament the changes that were made to the Bill during its clause-by-clause consideration. However, it is unlikely that any further changes will be made to Bill 64 between now and its final passage. Given that the National Assembly officially resumes on September 14, it is reasonable to expect that Bill 64 will be passed by the end of October 2021.

COMING INTO FORCE

The Committee adopted an amendment to section 165 of Bill 64 to provide for the coming into force of the *Act to modernize legislative provisions as regards the protection of personal information* in several phases. As a result, most of the new provisions introduced to the Private Sector Act will come into force two years after the Act receives its assent, except for certain specific provisions that will come into force one year after the Act receives its assent, including:

- The requirement to designate a person in charge of the protection of personal information (s. 3.1);
- The obligation to report a confidentiality incident (s. 3.5 to 3.8);
- The exception for disclosure of personal information in the course of a commercial transaction (s. 18.4); and

- The exception to disclosure of personal information for study or research purposes (s. 21 to 21.0.2).

In addition, the period for the right to portability of personal information (s. 27) has been maintained at three years from the date of the Act's assent.

CONCLUSION

There is no doubt that the work of the Committee on Institutions, which was spread out over 19 meetings over more than six months, has resulted in significant improvements to the initial version of Bill 64. Indeed, it is clear that by adopting this reform, Québec is taking an important step forward to ensure better protection of its citizens' personal information in the context of the digital economy.

However, it is unfortunate that members of Parliament were not more sensitive to the recommendations made by various stakeholders from the business community. Indeed, many of the new requirements that Bill 64 introduces in the Private Sector Act will be difficult for businesses to implement. These include the requirement to inform individuals of the names of third parties (including service providers) to whom the business may disclose personal information, the requirement to have technologies that identify, locate or profile an individual be deactivated by default and the requirement to ensure that the privacy settings of a product or service provide the highest level of confidentiality without any input from the individual.

Finally, the CAI will have a major role to play between now and the coming into force of the new provisions, as Bill 64 entrusts it with the responsibility of developing guidelines to facilitate the application of the *Private Sector Act* (new section 123(9) of the *Act respecting Access to documents held by public bodies and the Protection of personal information*) as well as a general framework for the application of AMPs (section 90.2).

[***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.*

Elisa Henry *co-leads the firm›s Privacy and Data Protection practice group and is Montreal Regional Leader of the firm›s Technology Law Group. She is a recognized expert in privacy and technology law and advises multinational and Canadian companies on strategic issues related to compliance with Canadian and European (GDPR) law requirements, big data and AI projects, anti-spam and data breaches.*

François Joli-Coeur's *practice focuses on privacy and cybersecurity. He advises and assists international and domestic clients from various sectors on a wide range of issues, including: compliance with privacy and data protection laws; anti-spam legislation compliance; cybersecurity issues; data breach management; information technology; telecommunications; advertising, marketing and sponsorship; consumer protection; and access to information.*

Max Jarvie *is a senior associate in the Privacy and Data Protection practice group at BLG LLP. He provides assistance and strategic advice to organizations relating to privacy and data protection, the use of machine learning, distributed ledgers and other technologies, information governance, data trusts, technology licensing, consumer protection, and corporate commercial matters.*

Julie M. Gauthier *is a recognized expert in privacy and technology law and advises multinational and Canadian companies from various sectors on a wide range of strategic issues related to compliance with Canadian privacy law requirements, cybersecurity, information governance, anti-spam, technology licensing and consumer protection.*

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.*

Simon Du Perron *is an associate 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.*]

1 Éloïse Gratton, Elisa Henry, François Joli-Coeur, Max Jarvie, Julie M. Gauthier, Andy Nagy, and Simon Du Perron, "End of Parliamentary Proceedings in Quebec: An Update on Bill 64" Borden Ladner Gervais LLP (June 21, 2021), online: <https://www.blg.com/en/insights/2021/06/end-of-the-parliamentary-proceedings-quebec-update-bill-64>.

2 Gouvernement du Québec, "Mémoire au Conseil des ministers" (May 25, 2020) at 11, online: <https://cdn-contenu.quebec.ca/cdn-contenu/gouvernement/MCE/dossiers-soumis-conseil-ministres/protection_des_renseignements_personnels.pdf?1597849858>.

3 These sections provide that the business must inform the individual, when collecting personal information, of the purposes for which the information is collected, the means by which the information is collected, the rights of access and rectification provided by law, and the right to withdraw consent to the disclosure or use of the information. Where applicable, the business must also inform the individual of the name of the third party for whom the information is being collected, the names of the third parties to whom it is necessary to communicate the information and the possibility that the information may be communicated outside Quebec. At the individual's request, the business must also indicate the specific personal information collected, the categories of persons who have access to this information within the business, the retention period of this information, the source of the information when it was collected from a third party, and the contact information of the person in charge of the protection of personal information.