Canadian Privacy Law Review

VOLUME 19, NUMBER 6 Cited as (2022), 19 C.P.L.R. MAY 2022

• ADDRESSING INTRA- AND INTER-COUNTRY DIFFERENCES IN PRIVACY LAW REFORM – THE CANADIAN CHALLENGE AND STRATEGIES •

Chantal Bernier, Of Counsel, Dentons

• In This Issue •

ADDRESSING INTRA- AND INTER-COUNTRY DIFFERENCES IN PRIVACY LAW REFORM – THE CANADIAN CHALLENGE AND STRATEGIES
Chantal Bernier 85

PRIVACY, PLEASE: FIRM THAT BREACHED INSTAGRAM'S PRIVACY POLICIES LOSES CLASS ACTION RULING
Joan M. Young, Mala Milanese 89

SUPREME COURT OF BRITISH COLUMBIA DENIES CERTIFICATION IN FACEBOOK PRIVACY CLASS ACTION
Mark Gelowitz, Tristram Mallett, Robert Carson and Lauren Harper 92

ONTARIO INTRODUCES ELECTRONIC MONITORING LEGISLATION
Daniel J. Michaluk and Shane Morganstein.....94

Chantal Bernier

As privacy law reform legislation multiplies in Canada, each pursuing its own direction, around the world, privacy law reform is also splintering through varied legislative developments. Even with Europe's assertive stance on uniformity with the adoption of the *General Data Protection Regulation* (GDPR) to replace national privacy laws with one European law, and the creation of the European Data Protection Board (EDPB) "*to ensure the consistent application of this Regulation*" (Article 70 GDPR), the domestic pull of local politics and culture is fraying consistency in application of the GDPR, and uniformity proves illusory. Canada's constitutional federation has all the makings to lead us in the same direction. The challenge and the strategy is for governments to ensure interoperability of laws and for organizations to develop cohesive internal compliance mechanisms.

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 0-433-44419-3 (print) ISSN 1708-5446
ISBN 0-433-44652-8 (PDF) ISSN 1708-5454
ISBN 0-433-44420-7 (print & PDF)

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

Please address all editorial inquiries to:

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

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

1. CANADA'S CONSTITUTIONAL PRIVACY LAW FRAMEWORK

Simply to set the stage, it is helpful to step back and situate the Canadian privacy regulatory framework in its constitutional context.

Constitutionalists will argue that Canada is the only truly federated state because of the degree of autonomy of each level of government, ensured by the clear division of revenue sources and legislative power. That is the context of the Canadian privacy regulatory framework. The federal *Personal Information Protection and Electronic Documents Act* (PIPEDA) was adopted under the federal government's legislative competence over "Trade and Commerce" (Article 91(2) of the *Constitution Act of 1867*). Québec challenges the constitutionality of PIPEDA arguing that the protection of personal information in the private sector rests exclusively within provincial legislative competence over "Property and Civil right" (Article 92.13). Provincial privacy laws deemed "substantially similar" to PIPEDA apply within the sphere of provincial jurisdiction. Concretely, this means organizations need to comply with the following division of privacy law within Canada:

- Organizations that fall within the legislative authority of the federal government, such as airlines, banks or telcos, are entirely governed by PIPEDA in relation to both their customer data and their employee data (section 4(1), PIPEDA).
- Organizations that do not fall within the authority of the federal government but are pan-Canadian, such as national retailers, will be governed by both PIPEDA and provincial legislation:
  - Where the province has enacted its own private sector privacy legislation, being Alberta, with the *Personal Information Protection Act* (Alberta PIPA), British Columbia with its own *Personal Information Protection Act* (BC PIPA), and Québec with an *Act respecting the protection of personal information in the private sector* (Québec Act), the organization must comply with those laws in that province

in relation to its customers' as well as its employees' information.
  - In the other provinces and territories, the organization must comply with PIPEDA in relation to its customer information, but there is a legal void in relation to employee information; that being said, because privacy is a fundamental human right, PIPEDA has been recognized to have quasi-constitutional status, and employee information is expected to be protected in accordance with the principles enshrined in privacy law.
- Organizations that do not fall within the authority of the federal government and operate in one province or one territory only, where:
  - The province has not adopted private sector privacy law, are governed by PIPEDA for their customer data and, as above, through a legal void, by principles of privacy in relation to their employees;
  - The province has adopted private sector privacy law, are governed entirely by that law in relation to both its customer and employee information.
- Organizations in the health sector, such as pharmacies, are governed by provincial and territorial health information protection laws, except in British Columbia and Québec, where they are governed by the private sector privacy law and in Nunavut where they are governed by PIPEDA.

To ensure interoperability through this legislative quilt, two strategies are imperative: i) legislative consistency among privacy laws such that they are substantively similar, and ii) clear delineation of scope, such as section 3 of the BC PIPA excluding from its application the collection, use or disclosure of personal information, if "*the federal Act applies to* [it]".

Both strategies appear at risk as Canadian privacy law reform plans evolve independently. Still, organizations can achieve harmonization in their privacy programs with their own strategies. We will come to that after having surveyed how main emerging trends in privacy law reform in Canada converge and diverge.

2. EMERGING DATA PROTECTION TRENDS AND REGULATIONS

Trends in Canadian privacy law reform appear from four legislative proposals, at various stages of adoption: i) Québec Bill 64, amending *An Act respecting the protection of personal information in the private sector*, passed on September 22, 2021, is set to come in force gradually in September 22, 2022, 2023 and 2024; ii) former Bill C-11, *An Act to Implement the Digital Charter 2020*, introduced on November 17, 2020, died on the Order Paper due to the election and will be re-introduced, similar or equal to the earlier version; iii) the Ontario White Paper on Modernizing Privacy in Ontario leads public consultation in view of adopting an Ontario private sector privacy law; iv) the Report of the British Columbia Legislative Assembly Special Committee to Review the *Personal Information Protection Act* was released on December 6, 2021.

These legislative proposals have much in common:

- Consent requirements are increased to ensure "meaningful consent";
- Transparency requirements are also higher to ensure simple, clear and accessible privacy policies, inherent to ensuring meaningful consent;
- Explicit consent is required for the processing of sensitive data;
- Automatic decision-making systems (ADS), referring to the use of artificial intelligence, are subject to specific transparency requirements to counter both discrimination through algorithmic bias and violation of privacy through excessive collection;
- Privacy regulation now includes within its scope de-identified and anonymized information;
- Breach notification will be mandatory where there is a risk of significant harm;
- Additional individual rights are considered, such as the right to disposal or right to be forgotten and the right to portability; and

- Regulators will have enforcement powers with fines proportionate to the organization's revenues.

The report of the British Columbia Special Committee stresses the need to maintain BC privacy legislation "substantially similar" to PIPEDA and to aim at adequacy with the GDPR.

But these legislative proposals differ on critical points:

- Québec's Bill 64 subjects transfer of personal information outside Québec to a privacy impact assessment to ensure the jurisdiction of destination provides adequate protection; other proposed legislation only requires notification of the individual;
- Bill 64 makes privacy impact assessments (PIAs) mandatory in relation to certain operations increasing privacy risk; the only other reference to PIAs is raised as a question for consultation in the Ontario White Paper;
- Bill 64 creates access and challenge rights around ADS, beyond other legislation or proposals; and
- "De-identified" and "anonymized" information are defined and treated differently among the legislative proposals.

3. STRATEGIES FOR HARMONIZATION IN ORGANIZATIONS' INTERNAL COMPLIANCE PROGRAMS

To implement cohesive and operational internal privacy compliance programs, organizations may pursue the following strategies:

- Elevating the privacy program to one, highest common denominator: that was Microsoft's strategy upon the adoption of the *California Consumer Privacy Act* (CCPA). It announced that, throughout the United States, it would comply with the requirements of the CCPA.
- Following action from and between different Data Protection Authorities (DPAs). As DPAs proceed to joint enforcement action or release joint policy statements, as they often do, common positions emerge in the application of diverse privacy laws. They serve as guidance for organizational compliance in a diversified privacy regime.
- Approaching cross-border data transfers for the real privacy risks they raise. Hosting data in certain states, for political, economic and/or legal reasons, undermines the security of the data. Both privacy law, as a matter of accountability for safeguarding personal data, and consumers' expectations impose due diligence in cross-border of data transfers. Adopting a PIA process to identify low to high risk cross-border transfers could both ensure compliance where required and serve to guide decisions on data storage on a long term basis, informing supplier risk management.
- Ensuring integrity of artificial intelligence processes or use of ADS is a matter of organizational risk management in general. No organization wants recruitment efforts skewed by algorithmic bias or to lose control over ADS for lack of algorithmic transparency. Discipline around ADS will assist organizations in providing a general account of its use to meet their transparency obligations and will ensure integrity of ADS, both in relation to the organization's corporate objectives and to its obligations under privacy law on the use of ADS.
- Achieving convergence in a global privacy data program is an organization's best strategy to bring certainty, clarity and effectiveness to its internal compliance mechanisms. Global corporate privacy and security policies, supported by intra-group agreements, offer a robust governance structure to ensure compliance with diverse privacy regimes. Without the formality of Binding Corporate Rules, global policies implemented through an intra-group agreement provide convergence of privacy rules for the organization and an internal accountability mechanism to ensure their implementation.

These strategies have already proven successful for many organizations. Still, they do not relieve governments of their duty to ensure a cohesive privacy regulatory framework.

[***Chantal Bernier*** *is a member of Dentons' Canadian Privacy and Cybersecurity, Government Affairs and Public Policy practice groups. Chantal advises leading-edge national and international companies as they expand into Canada and Europe, enter the e-commerce space, adopt data analytics and roll out data-based market initiatives. Her clients include ad tech companies, financial institutions, biotech companies, data analytics firms and government institutions.*]

• PRIVACY, PLEASE: FIRM THAT BREACHED INSTAGRAM'S PRIVACY POLICIES LOSES CLASS ACTION RULING •

Joan M. Young, Partner, Mala Milanese, Associate, McMillan LLP

Joan M. Young

The B.C. Supreme Court recently certified a class action proceeding against Hyp3R Inc. ("**Hyp3R**"),[1] a U.S.-based marketing firm that collected Canadian Instagram users' personal information in breach of the platform's policies. The Court also ordered Hyp3R to pay more than $24 million in damages.

BACKGROUND

Instagram permits users to share posts, including texts, photos, and videos, with other members and the public. It makes available tools that allow third parties to interact with Instagram, but requires third parties to adhere to certain policies, including the prohibition of "scraping" or improper collection and retention of users' personal information.

In April of 2018, Instagram made changes such that it would not be possible to access or collect all public posts from specific locations or collect and retain users' Instagram stories through those tools. After these changes were made, the defendant Hyp3R carried out "scraping" of personal information from users' profiles on Instagram up until about August 2019, at which time Instagram announced that Hyp3R's actions were in violation of its policies and that it was removing the company from its platform.

The plaintiff sought to hold Hyp3R accountable for this conduct to Instagram users in Canada (other than Quebec). It was alleged that Hyp3R's actions constituted a breach of the privacy statutes of four provinces as well as the tort of intrusion upon seclusion (in the remaining provinces and territories).

THE DECISION

The Court noted that the plaintiff had served Hyp3R with the notice of civil claim, but that Hyp3R had failed to respond, resulting in the plaintiff obtaining a default judgment for damages to be assessed. After reviewing applicable case law, the Court concluded

that it was appropriate to proceed with certification and determination of the issues notwithstanding the defendant's default. The Court went on the address the following matters:

Certification

The plaintiff argued that all of the certification requirements for a class action were met. The Court accepted this argument for the reasons set out below.

i. The Pleadings Disclosed a Cause of Action

Statutory torts for breach of privacy are set out in provisions of the privacy statutes in B.C.,[2] Saskatchewan,[3] Manitoba,[4] and Newfoundland and Labrador.[5] The privacy statutes of these provinces contain a significant amount of parallel language.

In each of these provinces, it is a tort to violate a person's privacy wilfully and without claim of right; "proof of damages" is not a required element of the tort.[6] Privacy may be violated by eavesdropping or surveillance.[7]

It is also a tort to use, without authorization, the name or likeness of a person for purposes of advertising or promoting the sale of, or any other trading in, any property or services.[8]

The plaintiff claimed that Hyp3R breached both of these torts in B.C., Saskatchewan, Manitoba, and Newfoundland and Labrador when it collected personal information without consent from the plaintiff and class members in each of these provinces and sold that information to third parties.

The remaining common law jurisdictions in Canada (i.e., Ontario, Alberta, New Brunswick, Nova Scotia, Prince Edward Island, Yukon, the Northwest Territories, and Nunavut) do not have statutes comparable to the privacy statutes described above. However, the common law tort of intrusion upon seclusion is available in these jurisdictions. The plaintiff alleged that, through its unauthorized collection, retention, and use of class members' personal information, Hyp3R committed the tort of instruction upon seclusion against class members in these jurisdictions.

The Court found that the plaintiff had pleaded claims that demonstrated causes of action on behalf of class members both in the four provinces with privacy statutes and in the remaining common law jurisdictions.

ii. There was an Identifiable Class of Two or More Persons

The plaintiff sought an order defining the class as all persons in Canada (excluding Quebec) who were Instagram users with profile settings set to public at any time between April 4, 2018 and the date of certification of the action at issue. The Court concluded that the class as so defined had objective criteria and appeared to be clear.

iii. The Claims of the Class Members Raised Common Issues

The Court found that the common issues as proposed met the requirements for certification.

iv. A Class Proceeding was the Preferable Procedure for the Fair and Efficient Resolution of the Common Issues

The plaintiff argued that Hyp3R's misconduct was uniform against people using its services, and that aggregating claims against Hyp3R under the *Class Proceedings Act*[9] was beneficial to class members and to the Court. The Court agreed with these submissions and concluded that a class proceeding was the preferable procedure for resolution of the common issues.

v. There was an Appropriate Representative Plaintiff

The plaintiff, Catherine Severs, was a class member, and an Instagram user with her privacy settings set to public at the relevant times. The Court was satisfied that Ms. Severs was an appropriate

representative of the class and met the requirements for certification.

Judgment on the Common Issues and Assessment of Damages

As these were default proceedings, the plaintiff was entitled to proceed on the basis that the allegations set out in the notice of civil claim were true. Based on the deemed admission of the allegations of fact in the notice of civil claim, along with affidavit evidence filed by the plaintiff, the Court was satisfied that there had been a violation by Hyp3R of the privacy of class members in each of the four provinces with privacy statutes, through the intentional and unauthorized collection of information (which the Court characterized as surveillance) and use of names and photographs of class members for commercial purposes. With respect to the tort of intrusion upon seclusion, the Court similarly concluded based on the evidence and the deemed admissions that the conduct of Hyp3R was intentional, that it involved the invasion of class members' privacy without lawful justification, that a reasonable person would regard that invasion as highly offensive, and that a reasonable person would be caused distress, humiliation or anguish.

The Court determined that each class member should be entitled to $10 in damages. The award applies only to Instagram users who had their accounts on a public rather than a private setting at the relevant times, which includes more than 2.4 million users.

TAKEAWAYS

The decision in *Severs v. Hyp3R* appears at odds with the more recent decision of the court in the *Chow v. Facebook, Inc.*[10] class proceedings. The B.C. Supreme Court in this case has clearly stated that the intentional and unauthorized collection and commercial use of personal data from public social media profiles constitutes a breach of the *Privacy Act* (in British Columbia, Saskatchewan, Manitoba, and Newfoundland and Labrador) as well as the tort of intrusion upon seclusion (in the remaining Canadian common law jurisdictions). In contrast, the court's decision in the recent *Facebook* case suggested that these kinds of claims were too individualized and not suitable for class proceedings.

Ultimately, the result in this case is probably more a function of the claim not being defended on its merits and the result of the default judgment, more than anything. Going forward it will prove interesting to see whether this case or the *Facebook* decision is the leading law in B.C. on these types of claims.

[***Joan M. Young*** *is a leading litigator, widely recognized for exceptional experience in complex litigation and dispute resolution matters, class actions, and product liability and regulation. She represents a wide variety of clients in industries such as the automotive, manufacturing and government sectors. Joan is skilled in providing proactive advice to public and private sector businesses on preventing and resolving disputes.*

Mala Milanese *is a member of the Litigation and Dispute Resolution group in McMillan LLP's Vancouver office. She is building a diverse practice focused on commercial litigation matters. Mala also has significant experience in all areas of intellectual property law, with an emphasis on litigation and patent drafting and prosecution.*]

---

1 *Severs v. Hyp3R Inc*, [2021] B.C.J. No. 2507, 2021 BCSC 2261 (B.C.S.C.).

2 *Privacy Act*, R.S.B.C. 1996, c. 373.

3 *Privacy Act*, R.S.S. 1978, c. P-24.

4 *Privacy Act*, C.C.S.M., c. P125.

5 *Privacy Act*, R.S.N.L. 1990, c. P-22.

6 See *Privacy Act*, R.S.B.C. 1996, c. 373 at s. 1; *Privacy Act*, R.S.S. 1978, c. P-24 at s. 2; *Privacy Act*, C.C.S.M., c. P125 at s. 2; and *Privacy Act*, R.S.N.L. 1990, c. P-22 at s. 3(1).

7 See *Privacy Act*, R.S.B.C. 1996, c. 373 at s. 1(4); *Privacy Act*, R.S.S. 1978, c. P-24 at s. 3(a); *Privacy Act*, C.C.S.M., c. P125 at s. 3(a); and *Privacy Act*, R.S.N.L. 1990, c. P-22 at s. 4(a).

8 See *Privacy Act*, R.S.B.C. 1996, c. 373 at s. 3(2); *Privacy Act*, R.S.S. 1978, c. P-24 at s. 3(c); *Privacy Act*, C.C.S.M., c. P125 at s. 3(c); and *Privacy Act*, R.S.N.L. 1990, c. P-22 at s. 4(c).

9 *Class Proceedings Act*, R.S.B.C. 1996, c. 50.

10 [2022] B.C.J. No. 141, 2022 BCSC 137 (B.C.S.C.).

• SUPREME COURT OF BRITISH COLUMBIA DENIES CERTIFICATION IN FACEBOOK PRIVACY CLASS ACTION •

Mark Gelowitz, Partner, Tristram Mallett, Partner, Robert Carson, Partner, and Lauren Harper, Associate, Osler, Hoskin & Harcourt LLP


Mark Gelowitz


Tristram Mallett


Robert Carson


Lauren Harper

On January 27, 2022, the Supreme Court of British Columbia dismissed an application for class certification in *Chow v. Facebook, Inc.*,[1] a putative privacy class action. Justice Skolrood held that there was no evidence that Facebook had misused the plaintiffs' information for its own benefit. In addition to this "fatal flaw," Justice Skolrood also found that the plaintiffs failed to satisfy the common issues criterion and that a class proceeding would not be the preferable procedure. This decision underscores the importance of the court's "robust gatekeeping function to weed out claims of dubious merit early at the certification stage."

BACKGROUND

The plaintiffs alleged that, without adequate consent, Facebook extracted call and text data from users of its applications on Android smartphones. The plaintiffs' claim involved two different theories of liability: (i) a "front end" allegation that Facebook accessed call and text data based on prompts which were allegedly inadequate to constitute consent; and (ii) a "back end" allegation that Facebook surreptitiously "scraped" call and text data without seeking consent.

JUSTICE SKOLROOD'S REASONS

As a preliminary matter, Justice Skolrood reviewed the evidence and found that there was *no evidence* to support the plaintiffs' central allegation that Facebook used, or misused, the plaintiffs' information for its own benefit. Instead, he noted that the documents relied on by the plaintiffs lent weight to Facebook's submission that, "rather than being a genuine expression of grievance or loss that warrants invoking the complex, time consuming and expensive mechanisms of a class proceeding", the plaintiffs' claim was largely "downloaded from the internet".

Justice Skolrood compared this case to *Simpson v. Facebook*,[2] in which Justice Belobaba denied certification on the basis that there was no evidence of the plaintiffs' core allegation that Canadian users' data was shared with Cambridge Analytica. Justice Skolrood reiterated Justice Belobaba's statement that the onus is on the plaintiffs to adduce some basis in fact for their core allegation. Citing *Simpson* and *Kish v. Facebook*[3] (in which the Court of Queen's Bench for Saskatchewan denied certification of another proposed privacy class action), Justice Skolrood emphasized the need for "robust gatekeeping" to weed out dubious claims early at the certification stage.

In addition to the absence of evidence — which Justice Skolrood described as a "fatal flaw" — Justice Skolrood considered three of the statutory certification criteria and held:

- **cause of action**: Taking the allegations as true, the plaintiffs adequately pleaded a breach of section 1

of the B.C. *Privacy Act*. However, several of the claims, including the unjust enrichment, unlawful means tort and other statutory claims, were not sufficiently pleaded.

- **common issues**: The plaintiffs had not satisfied the common issues criterion because, among other reasons, the alleged breaches of the B.C. *Privacy Act* could not be determined on a class-wide basis. Rather, those claims would require consideration of the individual circumstances of the person claiming a breach.
- **preferable procedure**: A class proceeding was not the preferable procedure because there was no evidence to indicate any *actual loss or harm* to the plaintiffs or to proposed class members. Accordingly, certifying this proposed class action and deploying "considerable judicial resources" would be the "antitheses of judicial economy and would not provide meaningful access to justice."

KEY TAKEAWAY

This case is yet another helpful reminder that certification remains a meaningful screening device and that claims with no chance of success should not be permitted to pass through the certification stage.

Osler represented Facebook, Inc. in this action with a team led by Mark Gelowitz, Tristram Mallett, Robert Carson and Lauren Harper. Osler also represented Facebook, Inc. in the *Simpson* and *Kish* actions described above.

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

***Tristam Mallett's** practice focuses on corporate litigation, class action defence and securities enforcement. He frequently advises clients on contested merger transactions; take-over bid litigation; shareholder dissent and appraisal litigation and shareholder derivative claims; securities misrepresentation, fraud and insider trading matters; prosecutions undertaken by regulatory authorities and industry organizations; and related internal investigations.*

***Robert Carson** has a broad litigation practice with particular emphasis on corporate and securities litigation and class action defence. Robert has experience defending securities, consumer, competition and product liability class actions. His practice also includes mergers and acquisitions litigation, director and officer liability, shareholder disputes, valuation proceedings, oppression claims, Ontario Securities Commission proceedings, and insolvency and restructuring matters.*

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

---

1 [2022] B.C.J. No. 141, 2022 BCSC 137 (B.C.S.C.).

2 Mark Gelowitz, Robert Carson, and Lauren Harper, "Ontario Superior Court Denies Certification of Cambridge Analytica Class Action" (18 February 2021), online: <https://www.osler.com/en/resources/critical-situations/2021/ontario-superior-court-denies-certification-of-cambridge-analytica-class-action>.

3 [2021] S.J. no. 339, 2021 SKQB 198 (Sask. Q.B.).

• ONTARIO INTRODUCES ELECTRONIC MONITORING LEGISLATION •

Daniel J. Michaluk, Partner, and Shane Morganstein, Associate, Borden Ladner Gervais LLP


Daniel J. Michaluk


Shane Morganstein

On February 28, Ontario issued Bill 88, the *Working for Workers Act, 2022*, a first of its kind workplace electronic monitoring legislation requiring Ontario employers to give notice of "electronic monitoring."

THE NEW REQUIREMENTS

Bill 88, will bring a new part to the *Employment Standards Act, 2000* (the "ESA"), titled "Written Policy on Electronic Monitoring."

The ESA will require all employers with 25 or more employees to create and publish an electronic monitoring policy within six months after Bill 88 receives Royal Assent. The proposed policy must identify whether an employer electronically monitors employees and, if so, it must provide:

- a description of how and in what circumstances the employer may electronically monitor employees, and
- the purposes for which information obtained through electronic monitoring may be used by the employer.

The policy must be dated, track amendment dates and must include other information that may be required by regulation. Employers must provide copies to new and current employees as well as employees assigned by temporary help agencies.

Bill 88 does not define "electronic monitoring," and likely applies to technologies deployed on corporate networks, personal devices governed by "bring your own device" policies, as well as any work tools with embedded sensors (*e.g.,* telematics and similar technologies).

The requirement to disclose the "circumstances" in which monitoring is employed suggests that the disclosure requirement applies to monitoring that occurs on a periodic or non-routine basis, *i.e.*, as part of an investigation or audit.

COMMENTARY

If passed without amendment, the proposed legislation will impose a modest requirement on employers. Employers should consider the following six points.

1. **No limitation.** Bill 88 does not impose a limit on electronic monitoring, which is permissible in Ontario absent an express contractual or collective agreement restriction. Such monitoring restrictions are rare in most sectors. Note that unionized employers continue to face the possibility of grievances alleging that monitoring constitutes a privacy violation under their collective agreements, though most unionized employers are already transparent about their use of monitoring technologies.
2. **List network security tools.** Bill 88 does not distinguish between monitoring via software installed on "endpoints" (workstations and handhelds) and other network devices, and most employers now compile and use a wide range of data for network security purposes. Employers should list applications regardless of where they are installed on the network.
3. **Pick the right level of disclosure.** Organizations typically keep security controls confidential to protect against adversary behavior called "threat shifting" - the shifting of tactics to circumvent existing, known controls. The disclosure that Bill 88 requires is unlikely to create a security risk;

however, employers should be aware of the risk and not take the Bill as an invitation to disclose too much. We see no reason, for example, to identify software make to comply. A simple table that sets out the information should suffice (see example at bottom of page).

4. **Anticipate questions.** Although a monitoring policy does not need to be too detailed, employers should anticipate employee questions and prepare to be transparent. For example, employees may ask if an application is hosted on premise or in the cloud, and where cloud data is stored.
5. **Update your asset map.** Every employer ought to employ "information technology asset management", a process for governing their network hardware and software. Organizations with strong asset management practices will have little difficulty identifying how employees are "monitored". For employers with less than strong asset management practices, Bill 88 is an invitation to improvement and the rooting out of unmanaged applications.
6. **Update your acceptable use policy.** Given the new electronic monitoring policy may need to be produced to prove compliance, it is best written as a stand-alone policy and an adjunct to any existing "acceptable use policy", a policy that sets enforceable rules for employee use of a network. It is a suitable time, however, to update acceptable use policies. Employers should consider moving the privacy provision from their acceptable use policies to their new electronic monitoring policies such that their new policies become the single document that establishes employees' expectation of privacy. Since the Supreme Court of Canada decision that recognized a limited employee expectation of privacy (in *R v. Cole*), we recommend that employers stipulate all purposes for which they may require access to network data, including information in user accounts – *e.g.*, to maintain the network, to investigate misconduct and to support the continuity of work.

Bill 88 imposes new requirements, but also creates an opportunity to revisit and improve several key aspects of network security and information governance.

[***Daniel J. Michaluk*** *is a well-recognized cybersecurity, privacy and information management lawyer, with significant experience working with education and public sector organizations in Canada. Dan helps organizations respond optimally to security and cyber incidents; defend security and privacy complaints, claims and grievances; handle complex freedom of information matters and appeals; and*

Tool	Circumstances	How	Purpose
Endpoint detection and response	Continuous	"EDR" monitors the use of workstations (programs run, files read and written, etc.) and compares it against a baseline to detect abnormalities and potential unauthorized use.	Network security
Vehicle telematics	All fleet vehicles during on shift use	On board sensors detect and report on vehicle location, driver behavior (hard braking, rapid acceleration, etc.) and engine diagnostics. For more information see our Vehicle Telematics Policy.	Fleet management and driver safety and security

address security and other operational issues while minimizing privacy risks.

***Shane Morganstein** practices in the corporate commercial group of BLG, with a focus on privacy, cybersecurity, and mergers and acquisitions. Shane is a Certified Information Privacy Professional (CIPP/C) who regularly advises clients in the public and private sectors on a wide variety of corporate and privacy matters, including in incident response and breach coaching, technology and SaaS contracting, and privacy considerations during corporate transactions.*]