Canadian Privacy Law Review

VOLUME 19, NUMBER 12 Cited as (2022), 19 C.P.L.R. NOVEMBER 2022

• CANADA: COURT OF APPEAL UPHOLDS EMPLOYEES' RIGHT TO PRIVACY •

Natalie Garvin, Associate, Filion Wakely Thorup Angeletti LLP

• In This Issue •

Natalie Garvin

On 21 June 2022, the Court of Appeal for Ontario (the "ONCA") issued a decision that reinforces an employee's right to privacy in the workplace, specifically for teachers employed by a public-school board to whom the Charter of Rights and Freedoms (the "Charter") applies. This decision, *Elementary Teachers Federation of Ontario v. York Region District School Board*,[1] overturns an earlier decision by the Ontario Divisional Court that upheld an arbitrator's finding that a school board's search and seizure of its classroom laptops was reasonable.

BACKGROUND FACTS

Two teachers (the "Grievors") employed by the York Region District School Board (the "Board") received written reprimands for maintaining an online log that listed information about their colleagues. The log was created out of the Grievors' concerns about preferential

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

treatment among staff and was stored online on a personal Google drive. The Board discovered the log when the principal entered a classroom after school hours and accessed a classroom laptop that belonged to one of the Grievors. Upon discovering that the log was open on the laptop's screen, the Principal used his cellphone to take screenshots of the approximately 100 entries in the log. Both of the Grievors' classroom laptops were then seized and searched as part of the Board's investigation into the Grievors' alleged misconduct.

THE ARBITRAL AND DIVISIONAL COURT DECISIONS

The Elementary Teachers' Federation of Ontario (the "Union") filed a grievance asserting, inter alia, that the Board violated the Grievors' rights to privacy by accessing digital information without reasonable cause.

At arbitration, Arbitrator Gail Misra held that the Board's right to manage its operations — namely, to maintain order and discipline in the school in accordance with section 265 of the *Education Act* — outweighed the Grievors' personal privacy interests. The Grievors' expectation of privacy was diminished because the online log was left open on a classroom laptop that was provided by the Board and could be accessed by any teacher or the principal. For a detailed summary of the arbitrator's decision, see "Search and Seizure of Workplace Computers did not Breach Employee's Privacy Rights".[2]

Arbitrator Misra's decision was upheld by the Divisional Court on judicial review. The Divisional Court held that the Board did not exercise unfettered discretion in searching the Grievors' classroom laptops but, rather, had reasonable cause to perform the search based on concerns raised by co-workers about the Grievors' online log. For a detailed summary of the Divisional Court of Ontario's judicial review decision, see "Diminished Expectation of Privacy: Employer Justified in Searching Employee's Computer".[3]

THE COURT OF APPEAL'S DECISION

On appeal, the ONCA considered whether public school teachers are protected under section 8 of

the *Charter* from unreasonable search and seizure conducted by their employers.

The ONCA began its analysis by confirming that section 8 of the *Charter* applies to the actions of public school boards and their principals. The Divisional Court had erred in concluding that employees do not have section 8 rights in a workplace environment.

The ONCA then considered whether the Grievors had a reasonable expectation of privacy with respect to their log, having regard to the totality of circumstances and relevant legal factors in the case. The ONCA held that:

- The **subject matter of the search** was the Grievors' personal messages to each other, which were stored "in the Cloud" and were not saved or stored on the Board's laptop or server.
- The Grievors had a **direct interest in the subject matter** because their individual contributions to the log had led to them being disciplined.
- The Grievors had a **subjective expectation of privacy in the subject matter** because they had taken steps to protect the privacy of their communications. In particular, the document was password-protected at all times and reserved for the Grievors' personal use.
- Such **subjective expectation of privacy was objectively reasonable** and deserving of protection, as the log was an electronic record of the Grievors' private conversations (similar to those had over phone, email, and text message or similar in nature to diary entries) and there was a high *potential* for personal information being revealed in these conversations. This reasonable expectation of privacy was not diminished by the Grievors' use of Board-issued computers to access to the log or inadvertent failure to close the document after using it. The Grievors were entitled to record their private thoughts with the expectation that those thoughts would remain private.

Moreover, the ONCA took particular issue with Arbitrator Misra's finding that the log was left in "plain sight" and that the Grievors had only a diminished expectation of privacy as a result. In the ONCA's view, even if he found the log by happenstance, the principal had no legitimate purpose in reading the private conversations in the log or taking screenshots of the log. It was inappropriate for him to "mine" the Grievors' private thoughts to address employment-related concerns.

In the result, the appeal was allowed and the original arbitral decision was quashed.

KEY ACTION POINTS FOR HUMAN RESOURCES AND IN-HOUSE COUNSEL

This decision reinforces an employee's right to privacy in the workplace, especially in respect of public sector employees who may be entitled to the *Charter* protections in their employment relationship. This case is particularly interesting as the Grievors were found to have an expectation of privacy in relation to communications made using technology owned by their employer and that was accessible to others.

The following are key takeaways for employers:

- Employers are encouraged to develop and enforce strong policies that address the use of, and expectations surrounding, employer-owned technology;
- Employers should proceed with caution in investigating information discovered in happenstance and that has the potential to include personal information (which includes an employee's thoughts and opinions); and
- Generally, employers should conduct searches of employer-issued devices only when there is a reasonable basis for doing so, and any such search should not involve accessing employee personal email accounts and files saved "in the Cloud".

[***Natalie Garvin*** *provides advice and representation to private and public sector employers in all areas of management-side labour and employment law, with a focus on labour relations (including construction labour relations), human rights issues, and collective agreement interpretation. Natalie has successfully assisted clients in responding to various labour*

related issues including, but not limited to, union certification, grievance arbitration, complaints of unfair labour practices, jurisdictional and sector disputes, and collective bargaining.]

1 2022 O.J. No. 2824, 2022 ONCA 476 (Ont. C.A.).

2 Lucas Mapplebeck, "Search and Seizure of Workplace Computers did not Breach Employee's Privacy Rights" (6 November 2018), online: Filion Wakely Thorup Angeletti LLP <https://filion.on.ca/insights/search-and-seizure-of-workplace-computers-did-not-breach-employees-privacy-rights/>.

3 Filion Wakely Thorup Angeletti LLP, "Diminished Expectation of Privacy: Employer Justified in Searching Employee's Computer" (24 November 2020), online: Filion Wakely Thorup Angeletti LLP <https://filion.on.ca/insights/diminished-expectation-of-privacy-employer-justified-in-searching-employees-computer/>.

• SUPREME COURT OF CANADA RAISES STANDARD FOR POLICE TO SEARCH A HOME INCIDENT TO ARREST FOR SAFETY, UPHOLDS WARRANTLESS SEARCH OF BASEMENT •

David McKnight, Partner, and Naomi Krueger, Associate, Alexander Holburn Beaudin + Lang LLP

David McKnight

Naomi Krueger

In *R. v. Stairs*,[1] the Supreme Court of Canada recently modified the common law on searches incident to arrest for safety purposes where the search occurs inside the arrested person's home, imposing a higher standard to search parts of a home that are outside the physical control of the arrested person.

FACTS AND PROCEDURAL HISTORY

A civilian made a 911 call reporting a man striking a woman in a car. Three police officers found the car parked and empty in the driveway of a house. They knocked on the door and announced themselves, but nobody answered. They entered the house and went to the basement staircase, sensing activity downstairs. They saw a woman with fresh face injuries come up the staircase; she had emerged from the basement living room area to the right. A man – the accused – also emerged from the right but, instead of climbing the staircase, ran to the left and barricaded himself in the basement laundry room.

The officers arrested the accused in the laundry room. They also conducted a visual "scan" of the other room: the basement living room area, for safety purposes. The officers spotted, in plain view, a clear container and a plastic bag containing methamphetamine, which they seized.

In addition to assault and breach of probation, the accused was charged with possession for the purpose of trafficking. He was convicted of all charges at trial. He appealed. Only the conviction for the drug offence

was at issue, and a majority of the Ontario Court of Appeal upheld the conviction.

The accused appealed his conviction to the Supreme Court of Canada arguing that the police had seized the methamphetamine evidence in breach of his right to be free from unreasonable search and seizure under s. 8 of the *Charter*, and that the evidence should have been excluded by the trial judge.

The Supreme Court of Canada gave three separate reasons in a split judgment. The five-judge majority concluded that the search of the basement was lawful and upheld the accused's conviction.

SUPREME COURT RAISES THE STANDARD, BUT DISAGREES ON HOW HIGH

Searches incident to arrest are an exceptional power to search without a warrant. The regular common law standard to justify a search incident to an arrest is well-established:

1. the person searched must have been lawfully arrested;
2. the search must be truly incidental to the arrest in the sense that it is for a valid law enforcement purpose connected to the arrest; and
3. the search must be conducted reasonably.

Notably, the police do not require "reasonable and probable grounds" for the search; they only require "some reasonable basis" that the search is for a valid law enforcement purpose, which may include safety, evidence preservation, or evidence discovery. This lower standard was easily met by the police in this case.

However, the Supreme Court of Canada has confirmed that people have heightened privacy interests in their homes. The accused argued that the standard for searches incident to arrest should be raised when in the arrested person's home due to this heightened privacy interest. The Court has occasionally modified the regular common law standard for searches incident to arrest to better balance privacy interests on one hand, and valid law enforcement objectives on the other. For example, strip searches and cell phone searches require a higher standard, and the seizure of bodily samples is not permitted in a search incident to arrest.

THE NEW TEST

The majority set out the new test. The first question is whether the area searched is within or outside the "physical control" of the arrested person. If the area searched is within the arrested person's physical control, then the regular common law standard applies. If the area searched is outside of their physical control, then:

1. the search must still be "sufficiently proximate" to the arrest (i.e., there must be a link between the location and purpose of the search and the grounds for the arrest);
2. the police must have a "reasonable suspicion" that there is a safety risk to the police, the accused, or the public that would be addressed by the search; and
3. the search must be conducted reasonably, tailored to the heightened privacy interests in a home – the police cannot search "every nook and cranny" of the house. The majority noted that "it would be good practice for the police to take detailed notes after searching a home incident to arrest".

In rejecting a requirement for suspicion of an "imminent" threat, the majority noted that while there is a significant privacy interest in one's home, there are also greater risks at play when police search a home, such as potential victims needing help or additional aggressors posing a safety risk. The majority stated that when assessing police conduct, judges "must be alive to the volatility and uncertainty that police officers face – the police must expect the unexpected", and that the courts must "avoid using twenty-twenty hindsight as the yardstick against which to measure instantaneous decisions made by the police."

Despite the disagreement in the Court, all nine judges agreed that the test to search a home incident to arrest for safety purposes must be stricter because of the heightened privacy interests in a home. The Court has confirmed that it will step in and modify legal standards for searches in order to balance law

enforcement objectives with different types of privacy interests.

UNANSWERED QUESTIONS

The Court only addressed searches for safety purposes – it did not address the standard for searches for other purposes, such as evidence collection or preservation, for which the standard may be higher. Relatedly, the evidence at issue in this case (methamphetamine) was unrelated to the reason the accused was arrested (assault). The seizure was justified on the "plain view" doctrine.

There is also a lingering question as to whether and how the plain view doctrine applies inside a person's home. This issue has been raised in several prior cases, but the Court has declined to address it each time. Because none of the parties argued this issue in this case, the Court has once again left this for another day.

[***David McKnight*** *is a Partner, and the leader of Alexander Holburn Beaudin + Lang LLP's Administrative Law, Cannabis and Defamation + Publication Risk Management Practice Groups. David is also a member of the Insurance and Local Government Practices. His practice is in the area of insurance litigation defence and includes construction litigation, fire loss, police claims, personal injury, property damage, administrative law and defamation. David also regularly provides coverage opinions and handles subrogated claims on behalf of insurers.*

Naomi Krueger *is a member of Alexander Holburn Beaudin + Lang LLP's Administrative Law, Insurance, Health, Defamation + Publication Risk Management and Local Government Practices. Naomi's practice is litigation-based with a focus on municipal, health and administrative law. On a day-to-day basis, Naomi deals with a variety of claims including professional negligence, professional disciplinary matters, personal injury, property damage, occupiers' liability and products' liability.*]

---

[1] [2022] S.C.J. No. 11, 2022 SCC 11 (S.C.C.).

• TAKEAWAYS ON PRIVACY BREACH RISK ASSESSMENT AND DATA SECURITY PROGRAMS: ALBERTA PRIVACY COMMISSIONER ISSUES BREACH REPORT •

Titli Datta, Associate, and David Krebs, Partner, Miller Thomson LLP

Titli Datta

David Krebs

On July 29, 2022, the Office of the Information and Privacy Commissioner of Alberta (the "**OIPC**") issued its report on data breaches (the "**Report**").[1] Alberta has been the leading Canadian jurisdiction with the most long-standing experience when it comes to reviewing, assessing and reporting on data breaches since it began mandatory breach reporting under the *Personal Information Protection Act* (the "**PIPA**")[2] in 2010. The Report is an invaluable resource for organizations regarding the lessons learned from close to 2000 submitted and reviewed breach reports.

This comprehensive Report outlines important learnings and comparisons that, among other things, showcase the evolution of breach reporting in the province.

Here are the key takeaways we see from this Report:

FINDINGS AND TRENDS BASED ON REPORTED BREACHES

General

- There have been 1953 breach reports submitted between 2010 – 2022. 68% of these were found

to have met the "**RROSH**" threshold under PIPA. RROSH means there was a "real risk of significant harm" based on the unauthorized access to, loss or theft of personal information. These decisions are posted publicly on the OIPC website[3] and provide for a treasure trove of guidance for organizations and their advisors.

- There has been a significant increase in breaches meeting the RROSH threshold over the years. For breach reports submitted in the last five years, i.e., between 2017 to 2022, 70% to 80% met the RROSH threshold, whereas for reports submitted between 2010 and 2013, less than half were considered to have implications signifying RROSH.

Causes

- Compromised IT systems caused 37% of all decisions where RROSH was found. The percentage of attacks on IT systems as the cause for data breaches has been increasing rapidly. It is now the cause of close to 50% of RROSH breaches.
- Social engineering and phishing, often leading to compromised IT systems, are the root cause of many privacy breaches reported by organizations. Listed as the fourth leading cause of breaches in the overall 2010-2022 period, this has been moving upwards to become the second leading cause in recent years.
- Notably, 71% of RROSH breaches have been found to be caused by non-accidental and deliberate action or malicious intent, including ransomware attacks (malicious software encrypting a user's files and making it impossible to access the files without a "key", leading to demands for ransom from the user in exchange of the "key") and system hacks. The likelihood of significant harm increases in such instances, usually resulting in RROSH.

Industry-Specific Reporting

- In the early years of breach reporting, (a) Finance; (b) Health Care and Social Assistance; (c) Information; (d) Mining, Quarrying, and Oil and Gas Extraction; and (e) Real Estate and Rental and Leasing were the leading industries reporting breaches. This disparity with other industries has narrowed significantly over time.
- Retail Trade and Accommodation and Food Services have seen an upward trend in breach reporting, almost exclusively due to compromised IT systems. This is likely a result of increased reliance on online transactions.

Individuals and Information Impacted

- Individuals most commonly affected by a RROSH breach are customers or clients (impacted in 56% of reported RROSH breaches), with employees being the second-largest affected group.
- Identity, financial and employment information tend to be compromised in RROSH breaches. The majority of RROSH decisions (between 69% and 81%) involve some basic contact information associated with an individual, such as a telephone number or mailing address. In recent years, email addresses have come to be increasingly compromised, while targeting of medical information has been on the decline.
- Out of the 1,953 reported breaches, personal information was subject to unauthorized access in 42% of all RROSH breaches, unauthorized disclosure in 36%, and loss in 21%. In recent years, more than 50% of RROSH breaches have been found to involve unauthorized access to personal information. In 2010-11, this percentage was 25%. This upward trend aligns with the increase in compromised IT systems.

KEY RECOMMENDATIONS

Based on its review of breach reports, the OIPC has the following key recommendations about what organizations can do to enhance their system security:

- Implement regular and/or immediate security patching on networks, servers and devices;
- Sign up for and review updates from cybersecurity agencies and other professionals to keep up to date on new threats and possible solutions to protect the organization's IT infrastructure;

- Train staff regularly on detecting phishing or social engineering attempts;
- Train staff regularly on protecting personal information contained in laptops or paper documents. For example, repeat the message that no devices or documents should be left in vehicles to reduce breaches caused by theft.

FINDINGS ON NOTIFICATION

- A positive finding of the OIPC is there has been less over-reporting of breaches by organizations, indicating that organizations have become more adept at assessing the likelihood of RROSH resulting from a breach.
- On the flip side, organizations are taking longer to report breaches. While the OIPC noted that there are good reasons why this might be the case – for example, complexity of cyber attacks, or multiple reporting jurisdictions – the fact remains that this is a concern for impacted individuals. Timely reporting is viewed as a key aspect of remediation of the harms of a breach.
- Notification in over 90% of cases was via direct notification; in 4% of the cases indirect notification was authorized. This was mainly the case where there was insufficient contact information at hand.
- PIPA and PIPA Regulations, along with guidance of the Office of the Privacy Commissioner under Canada's *Personal Information Protection and Electronic Documents Act* (**"PIPEDA**"),[4] provide a roadmap to determine the factors that contribute to an assessment of whether there is a real risk of significant harm.
- Risk-increasing factors were noted as follows: deliberate action or malicious intent to cause the breach; personal information was not recovered, returned or destroyed securely; lengthy data exposure; and personal information was exposed and no ability to determine whether information was accessed and where personal information was not encrypted.
- Risk-reducing factors and where no RROSH was found are as follows: accidental or inadvertent cause of the breach; personal information is recovered, the organization confirms that personal information accessed has been destroyed securely, or the organization confirms it has not been used, forwarded or retained; encryption of the personal information; breach is reported to the organization by the unintended recipient(s); unintended recipient of personal information is a known or trusted party; and fewer personal information data elements are at issue and the personal information cannot be used for significant harm.

We should note that in some cases, one factor can be determinative, but in other cases it may simply be one of the considerations. For example, mere presence of malicious intent may not always be sufficient to cause a RROSH determination, whereas cases where data was sufficiently encrypted would generally be viewed as a very strong determining factor that personal information could not be accessed or used and, therefore, no harm can arise.

CONCLUSION

The findings of the Report conform to what our firm has been seeing in this area. Cyberattacks, especially ransomware incidents, email compromise and wire fraud, have been increasing, whereas cases of stolen or lost devices leading to a significant data incident are becoming less prevalent. This decreasing prevalence, in our view, is mainly due to the fact that organizations have been enhancing their protections by limiting data stored on devices, training employees, and increasing device/data encryption.

[***Titli Data*** *has an active practice as a general civil litigator, with experience in matters pertaining to commercial litigation, contractual disputes, family law, regulation of professions, estate litigation, and labour and employment disputes. Titli also has a growing practice in privacy law and is a member of Miller Thomson's National Privacy and Cybersecurity Group.*

David Krebs *has a business law practice with particular focus on privacy, cybersecurity, and technology law. David is the National Co-Leader of the firm's Privacy & Cybersecurity practice and serves as breach coach and counsel in cyber*

incident response for clients across Canada. David regularly advises clients on responding to data breaches, cybersecurity matters, data governance, and data protection/privacy risks in M&A and other commercial transactions.]

1 Office of the Information and Privacy Commissioner of Alberta, "PIPA Breach Report 2022" (July 2022), online: Office of the Information and Privacy Commissioner of Alberta <https://oipc.ab.ca/wp-content/uploads/2022/07/PIPA-Breach-Report-2022.pdf>.

2 S.A. 2003, c. P-6.5.

3 Online: Office of the Information and Privacy Commissioner of Alberta <https://oipc.ab.ca>.

4 S.C. 2000, c. 5.

• PROTECTION OF CRITICAL CYBER SYSTEMS: CANADA INTRODUCES NEW LEGISLATION UNDER BILL C-26 •

Nathalie David, Partner, Ellen Snow, Partner, Laure Bonnave, Senior Counsel, Ayse Gauthier, Senior Counsel, and Cédrik Pierre-Gilles, Associate, Clyde & Co LLP, and Dave Dhillon

Nathalie David

Ellen Snow

Laure Bonnave

Ayse Gauthier

Cédrik Pierre-Gilles

On June 14, 2022 the Government of Canada introduced Bill C-26, *An Act Respecting Cyber Security*, in an effort to "protect Canada's critical infrastructure".[1] While Part 1 of Bill C-26 amends the *Telecommunications Act* and *Canada Evidence Act*, Part 2 enacts the *Critical Cyber Systems Protection Act* ("CCSPA" or the "Act"), which would provide a new framework for the protection of critical cyber systems for services and systems vital to national security or public safety.

As parliamentary business resumed in September 2022 in Ottawa, many stages of the legislative process remain before Bill C-26 is passed and the CCPSA is enacted. Until then, we can expect that a number of provisions will be added, modified or removed. Nevertheless, considering the scope of the regulatory framework to be established and the multiple requirements it entails, impacted organizations should closely monitor the Bill's progression.

We provide a few of the key highlights of the proposed CCSPA below.

I. APPLICABILITY

The Preamble to the proposed CCSPA establishes that the Act serves to impose obligations on organizations that have cyber systems that "are critically important to vital services and vital systems" such that their "disruption could have serious consequences for national security or public safety".

Once enacted, the CCSPA will apply to federally regulated persons, partnerships or unincorporated organizations belonging to a class of operators that will be listed in Schedule 2 of the Act,[2] i.e., designated operators, that own, control or operate a critical cyber system.[3] Schedule 2 will also include a list of regulators corresponding to each class of operators.[4]

While a cyber system is broadly defined as "a system of interdependent digital services, technologies, assets or facilities that form the infrastructure for the reception, transmission, processing or storing of information",[5] the definition of "critical cyber system" further delineates the proposed legislation's scope:

> ***critical cyber system*** means a cyber system that, if its confidentiality, integrity or availability were compromised, could affect the continuity or security of a vital service or vital system.[6]

"Vital services" and "vital systems" are set out under Schedule I of the CCSPA, and the Governor in Council may add a "service that is delivered, or a system that is operated" within the legislative authority of Parliament, if the Governor in Council is satisfied that the service or system is vital to national security or public safety. In this first version of Bill C-26, the following services or systems are referred to under Schedule 1:

- Telecommunications services;
- Interprovincial or international pipeline or power line systems;
- Nuclear energy systems;
- Transportation systems (federally regulated);
- Banking systems; and
- Clearing and settlement systems.

This assessment and the resulting qualification as a "critical cyber system" triggers several new requirements for designated operators. Additional guidance on how to assess whether the compromise of a given cyber system could affect the "continuity" or "security" of those services or systems would be useful.

II. ESTABLISHMENT OF A CYBER SECURITY PROGRAM

The proposed CCSPA provides that a designated operator must, within 90 days after being designated a part of that class, establish a cyber security program in respect of its critical cyber systems, including reasonable steps to:

a. identify and manage any organizational cyber security risks, including risks associated with the designated operator's supply chain and its use of third-party products and services;
b. protect its critical cyber systems from being compromised;
c. detect any cyber security incidents affecting, or having the potential to affect, its critical cyber systems;
d. minimize the impact of cyber security incidents affecting critical cyber systems; and
e. do anything that is prescribed by the regulations.[7]

The designated operator also has to provide its cyber security program to the regulator,[8] as well as periodically review the program and notify the regulator of changes.[9]

III. MITIGATION OF SUPPLY-CHAIN AND THIRD-PARTY RISKS

As soon as a designated operator identifies any cyber security risk associated with its supply chain or its use of third-party products and services, it has an obligation to "take reasonable steps, including any steps that are prescribed by the regulations, to mitigate those risks".[10]

Should Bill C-27 become law, guidance documents or regulations can be expected to provide clarification on how to determine what might constitute reasonable mitigation steps to fulfill this obligation.

IV. REPORTING OF CYBER SECURITY INCIDENTS

A designated operator would have to immediately report a cyber security incident in respect of any of its critical cyber systems to the Communications Security Establishment ("CSE").[11] Established in 2019, the CSE is a national agency that provides the federal government with information technology security and foreign signals intelligence.

This obligation is in addition to similar reporting obligations that exist under other regulatory frameworks, such as privacy legislation. In this regard, we note that the government recently proposed Bill C-27,[12] *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts* ("Bill C-27). Under Bill C-27, the federal government notably proposes to enact a new statute to protect personal information in the private sector. While Bill C-27 will be the subject of a separate article, we note that the reporting obligation under the privacy legislative framework[13] is triggered when a breach of security safeguards involving personal information creates a real risk of significant harm to an individual.

Under the CCSPA, based on the definition of "cyber security incident", the reporting threshold is rather tied to an assessment of the interference (or potential interference) of an incident on (a) the continuity or security of a vital service or system or (b) the confidentiality, the integrity or the availability of the critical cyber system.[14]

We note that reporting a cyber security incident to the CSE does not absolve a designated operator from notifying its regulator.[15]

V. COMPLIANCE

As proposed under Bill C-26, the CCSPA also includes a number of provisions regarding the powers of relevant authorities and the directives and orders they can issue to ensure compliance with the legislation.

Section 20 of the proposed legislation allows the Governor in Council to issue an order directing a designated operator or a class of operators to comply with any measure for the purpose of protecting a critical cyber system.[16] A direction would specify the measures to be taken, the period within which the measures are to be taken, and any conditions imposed on the designated operator.

The Act also includes the power for a regulator, such as the Office of the Superintendent of Financial Institutions, to order a designated operator to conduct an internal audit of its practices, books and other records to determine the designated operator's compliance with the Act or the regulations and to report the results of its audit to the regulator.[17] In addition to internal audit orders, regulators also have the power to order a designated operator to terminate the contravention to any provision of the Act or the regulations and to take any measure to comply with the provision's requirements or mitigate the effects of non-compliance.[18]

Regulators could even enter "a place" to verify compliance or prevent non-compliance with the Act if they have "reasonable grounds to believe that an activity regulated under this Act is being conducted or any document, information or thing that is relevant to that purpose is located". The proposed legislation currently provides broad powers of entry for the regulators, including the right to "examine anything in the place", to use any cyber system for the purpose of examining any information contained in it, and to examine, copy or take extracts of any record, report, data or other document.[19] Except for the requirement to obtain a warrant or the consent of the occupant in the case of a dwelling-house,[20] there appear to be few restrictions on the use of these broad powers.

In reviewing these powers, the objective of establishing regulatory oversight of critical cyber systems is clear. However, in its current form, Bill C-26 raises a number of questions about both the reasonable exercise of these powers and the effective capacity of regulators to use them.

VI. RECORD-KEEPING

The designated operators also have an obligation to keep records respecting (a) any steps taken to implement their cyber security program, (b) every cyber security incident reported to the CSE, (c) any steps taken to mitigate supply-chain or third-party risks, (d) any measures to implement a cyber security direction, and (e) any matter prescribed by the regulations.[21]

VII. VIOLATIONS AND OFFENCES

The proposed CCSPA provides administrative monetary penalties for violations of the Act and its regulations as well as offences for specific contraventions. Administrative monetary penalties could be imposed on any designated operator or other person that contravenes or fails to comply with a provision of the Act or its regulations. The maximum amount for such penalties is currently set at $1,000,000, in the case of an individual, and $15,000,000, in any other case.[22] Directors and officers of a designated operator may also be found liable to a penalty if they directed, authorized, assented to, acquiesced in or participated in the commission of the violation.[23]

Finally, the Act also sets forth a series of offences for the contravention of specific provisions of the Act, such as the reporting obligations for cyber security programs and cyber security incidents.[24] As with administrative monetary penalties, a director or an officer that directed, authorized, assented to, acquiesced in or participated in the commission of the offence is a party to the offence and is liable on conviction to the punishment provided for by the Act.

CONCLUSION

Over the last few years, organizations that operate cyber systems in all sectors have become acutely aware of cyber security issues. Whether in response to a previous security incident or following the evolution of the privacy legislation, many have already implemented organizational and technical measures to further secure their systems.

With the intensification of cyber attacks on critical infrastructure entities, other governments have also adopted legislation requiring these entities to report cyber attacks.[25] The introduction of Bill C-26 reflects the federal government's intention to strengthen the protection of the vital services and systems on which Canadians rely.

Clyde & Co's Cyber Risk team provides a complete solution for all cyberattacks on businesses. Given the potentially far reaching international exposure of cyberattacks and data breaches, clients can benefit from Clyde & Co's multi-jurisdictional expertise and on the ground incident response team drawn from over 60 offices globally.

[***Nathalie David*** *oversees both the cyber insurance coverage and incident response teams at Clyde & Co's Montreal office. She assists insurers and insureds in evaluating data breaches, privacy issues and cyber claims in a variety of sectors, from issues in relation to notification to customers, restoration of data and quantification of loss. Nathalie works with an established network of experts globally who can assist when required.*

Ellen Snow *is a partner in the Toronto commercial litigation group, dealing with a range of complex issues and disputes, with a particular focus on cyber security and privacy issues.*

Ellen regularly advises clients in a wide range of security and privacy events including ransomware attacks, cyber extortion, sophisticated phishing and social engineering fraud schemes and inadvertent security breaches by employees.

Laure Bonnave *has a litigation practice in all areas of insurance, including professional liability, directors and officers liability and construction law, as well as extensive experience in defamation matters. She has pled before Quebec lower courts and the Court of appeal.*

Laure also acts as privacy counsel ("breach coach") in the event of cybersecurity incidents, such a data or privacy breach.

Ayse Gauthier *is a senior lawyer with the litigation and monitoring teams. Her practice focuses on professional liability of lawyers and engineers, particularly in construction matters, as well as cyber insurance coverage. She has also developed an expertise in e-discovery and technology assisted review in large scale litigation.*

Cédrik Pierre-Gilles *Cédrik is a lawyer who practises primarily civil litigation, professional liability and insurance law, with a particular interest in cyber risk insurance. A member of the Quebec Bar since 2020, Cédrik first joined the Clyde & Co team as a student in 2019.*]

---

1 Public Safety Canada, News Release, "Government Introduces New Legislation to Protect Canada's Cyber Security" (14 June 2022), online: Government of Canada, <https://www.canada.ca/en/public-safety-canada/news/2022/06/government-introduces-new-legislation-to-protect-canadas-cyber-security0.html>.

2 While no class of operators is currently included under Schedule 2, we note that section 7 of the proposed CCSPA provides that the Governor in Council may, by order, amend Schedule 2 by adding, amending or deleting classes of operators.

3 Proposed *Critical Cyber Systems Protection Act*, s. 8.

4 The regulators have not yet been included in Schedule 2, but Section 2 of the proposed CCSPA already defines "regulator" as: (a) the Minister of Industry; (b) the Minister of Transport; (c) the Superintendent of Financial Institutions; (d) the Bank; (e) the Canadian Energy Regulator; or (f) the Canadian Nuclear Safety Commission.

5 Proposed *Critical Cyber Systems Protection Act*, s. 2.

6 Proposed *Critical Cyber Systems Protection Act*, s. 2.

7 Proposed *Critical Cyber Systems Protection Act*, s. 9.

8 Proposed *Critical Cyber Systems Protection Act*, s. 10.

9 Proposed *Critical Cyber Systems Protection Act*, s. 13.

10 Proposed *Critical Cyber Systems Protection Act*, s. 15.

11 Proposed *Critical Cyber Systems Protection Act*, s. 17.

12 Bill C-27 *An Act to enact the Consumer Privacy Protection Act, the Personal Information and Data Protection Tribunal Act and the Artificial Intelligence and Data Act and to make consequential and related amendments to other Acts,* 1st Sess., 44th Parl., Canada, 2021 (first reading 16 June 2022), online: Parliament of Canada <https://www.parl.ca/legisinfo/en/bill/44-1/c-27>.

13 Office of the Privacy Commissioner of Canada, "What You Need to Know About Mandatory Reporting of Breaches of Security Safeguards" (revised 13 August 2021), online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/en/privacy-topics/business-privacy/safeguards-and-breaches/privacy-breaches/respond-to-a-privacy-breach-at-your-business/gd_pb_201810/>.

14 Proposed *Critical Cyber Systems Protection Act*, s. 2.

15 Proposed *Critical Cyber Systems Protection Act*, s. 18.

16 Proposed *Critical Cyber Systems Protection Act*, s. 20.

17 For example, proposed *Critical Cyber Systems Protection Act*, s. 34, for the Superintendent of Financial Institutions.

18 For example, proposed *Critical Cyber Systems Protection Act*, s. 36.

19 For example, proposed *Critical Cyber Systems Protection Act*, s. 32, for the powers of the Superintendent of Financial Institutions.

20 Proposed *Critical Cyber Systems Protection Act*, s. 33.

21 Proposed *Critical Cyber Systems Protection Act*, s. 30.

22 Proposed *Critical Cyber Systems Protection Act*, ss. 90-91.

23 Proposed *Critical Cyber Systems Protection Act*, s. 93.

24 Proposed *Critical Cyber Systems Protection Act*, s. 136.

25 See for instance, *Incident Reporting for Critical Infrastructure Act of 2022* (adopted March 2022), online: U.S. Department of Homeland Security CISA Cyber + Infrastructure <https://www.cisa.gov/circia>.