Bulletin | Cybersecurity, Privacy and Data Protection

October 2024

IPC decisions expand cyber incident reporting and notification obligations in Ontario

On July 5, 2024, the Information and Privacy Commissioner Ontario issued four decisions that raise significant new obligations for organizations subject to Ontario's four privacy statutes – the *Personal Health Information Protection Act* (PHIPA), the *Freedom of Information and Protection of Privacy Act* (FIPPA), the *Municipal Freedom of Information and Protection of Privacy Act* (MFIPPA), and the *Child, Youth and Family Services Act* (CYFSA).

The decisions – which are being referred to as the "cyber attack quartet" – set a low threshold for what constitutes a "privacy breach" under Ontario law, in situations where threat actors compromise a network or account but had minimal or no opportunity to view institutional data. In this article, we briefly summarize the decisions and set out their significance.

THE QUARTET

The breach threshold

Only PHIPA and the CYFSA have mandatory breach reporting and notification duties. Three decisions in the quartet are PHIPA decisions and one is a CYFSA decision.

In *Simcoe Muskoka District Health Unit (Re)*, 2024 CanLII 67094, the IPC held that unauthorized access to an e-mail account by malicious threat actor(s) for one hour triggered the unauthorized disclosure and unauthorized use of all personal health information in the e-mail account. It made this finding despite the short period of exposure and the absence of evidence of file level access or theft. This is remarkable given the e-mail account contained approximately 20,000 e-mails, approximately 1,000 of which contained personal health information.

The IPC agreed with the health unit that the PHIPA reporting and notification duties are only triggered when the evidence establishes unauthorized disclosure or unauthorized use on a balance of probabilities.[1] However, the IPC interpreted the evidence through a pessimistic lens. This is most evident in its unauthorized use analysis, in which the IPC inferred handling or viewing of personal health information from facts that most would consider benign:

> In this case, I consider the prevalence of personal health information in the email account, the fact the threat actor had unimpeded access to that information for a considerable period of time, and the threat actor's obvious intention to gain access to valuable information in SMDHU's email systems—which, in the case of a public health unit like SMDHU, clearly includes records of personal health information. In these circumstances, I am satisfied, on a balance of probabilities, that the threat actor used personal health information in the compromised email account during the window of opportunity available to it.

1 Although the IPC did rely on the broadly worded definitions of "disclose" and "use" in PHIPA, its decision is on a question of fact, and implicitly accounts for the probability of informational exposure.

The *Hospital for Sick Children*, 2024 CanLII 67095 (SickKids) and *Kingston, Frontenac and Lennox & Addington Public Health (Re)*, 2024 CanLII 67096 (ON IPC) (KFL&A) and *Halton Children's Aid Society (Re)*, 2024 CanLII 67087 (ON IPC) (Halton CAS) decisions each involved ransomware attacks in which the threat actor(s) only encrypted data without stealing or viewing it. The IPC held that the encryption alone resulted in an unauthorized use and a loss of personal health information. It reasoned that the threat actor(s) "used" personal health information by rendering it unavailable, which it said entails "handling" and "[dealing] with" the files. The IPC also noted that even a temporary loss constitutes a "loss" under PHIPA and the CYFSA when personal [health] information is unavailable because of a malicious attack, as opposed to events like a power outage. The IPC reasoned that such an occurrence is meaningful from a privacy perspective, and that individuals should be informed so they can make inquires, complain, or "seek a remedy."

Notably, in each of these encryption-only cases, the IPC declined to decide whether threat actor access to systems triggered a system-wide disclosure of personal health information analogous to the triggering found in the Simcoe Muskoka District Health Unit decision.

Reporting and notification duties

The IPC endorsed indirect notification of affected individuals in each of the four decisions. It reasoned that the appropriate form of notification can vary based on the circumstances, and that various factors can weigh in favour of pursuing indirect notification – "including the… number of potentially affected individuals, and the difficulty of determining with certainty exactly which individuals, and what information, [has] been affected."

The IPC held that indirect notification was appropriate for use in responding to the three attacks in which the threat actors only encrypted information, though it made clear that even an indirect notification must include certain information, including information about the right to make an IPC complaint and organizational contact information.

SIGNIFICANCE

Our purpose here is not to critique the quartet, but we comment that the four decisions illustrate that the IPC is struggling with the zero-risk threshold for reporting and notification under PHIPA and the CYFSA. Given these statutes do not contain a harms-based threshold like the "real risk of signficant harm" threshold in consumer privacy statutes (and some Canadian public sector privacy statutes), it is less clear how risk ought to be accounted for in interpreting the scope of the reporting and notification duties.

Enforcement considerations

Encryption and transitory data loss

The IPC is actively enforcing the encryption finding under PHIPA and the CYSFA. That is, its official position is that the encryption of personal information and personal health information triggers an unauthorized use and a loss under these statutes. Whether the IPC will enforce the same position under MFIPPA and FIPPA is less clear, but MFIPPA and FIPPA institutions may wish to voluntarily comply. As we explain below, compliance with the encryption finding ought not be difficult.

Network access

It is less certain that the IPC will enforce the unauthorized disclosure position that it took in the Simcoe Muskoka District Health Unit decision in ransomware encryption cases. Whether the IPC will find that access to an entire network triggers the disclosure of all personal information and personal health information that is stored on the network will depend on the facts.

The IPC's analysis calls for a finding that file-level data exposure is likely, but as seen in the SickKids, KFL&A, and Halton CAS decisions, the IPC is cautious about making such a finding when it comes to network access. It remains important to conduct a duly diligent investigation with a view to determining if personal information or personal health information has been stolen and viewed, if so, what specific personal information and personal health information has been stolen or viewed.

Business e-mail account compromises

This does not rule out application of the Simcoe Muskoka District Health Unit's position in business e-mail compromise cases, and institutions faced with scenarios like that faced by the Simcoe Muskoka District Health Unit should carefully weigh their options. The significance of the IPC position is that file level analysis of an entire e-mail account can be very expensive and time consuming, even when there may no real risk of harm.

Giving notice of encryption

Until now, clients attacked by a ransomware actor and facing encryption of network assets might voluntarily

report to the IPC in the first few days, though it would be presented as an option rather than an imperative. Most would investigate to determine whether personal information and/or personal health information had been exposed, and upon making a determination, develop a notification plan. These plans have typically called for reporting to the IPC shortly before notification.

Given the quartet, and when system encryption is discovered in a ransomware attack, the findings of the quartet call for prompt public notification.

This can be done as part of public communications made in the first few days of an incident. Institutions do not need to alarm, nor necessarily recognize a "privacy breach" by name. If there is no evidence of data theft, this can also be communicated. Institutions should, however, explain that personal information and/or personal health information files in their systems have been encrypted. They should also let individuals know that they can complain to the IPC and should provide organizational contact information to which individuals can address privacy related questions.

Indirect notification as an option

The other significance of the quartet is that it gives insight into when the IPC will accept the indirect notification of affected individuals. Ms. Ryu referred to PHIPA Decision 210, in which the IPC said individual notification is the notification "standard." Despite this nod to individual notification, the IPC has now blessed indirect notification as appropriate in numerous cases and varying scenarios.

Direct, individualized notification is still considered best practice. However, considering the trend made clear in the quartet, it may be worth assessing whether time and money can be saved by foregoing file-level analysis and notifying groups indirectly via public notification when feasible. The best approach will vary depending on the circumstances.

CONCLUSION

The quartet changes how BLG will guide our clients in responding to cyber attacks in which threat actor(s) encrypt data. We welcome inquires about this guidance and continue to stress the importance of engaging with legal counsel at the outset of an incident.

These developments underscore the importance of cautious management and cautious messaging, particularly given dealings with the Ontario regulator will likely come earlier in the response process.

Authors

Daniel Michaluk
T 416.367.6097
dmichaluk@blg.com

Eric Charleston
T 416.367.6566
echarleston@blg.com

Marc Vani
T 416.367.7266
mvani@blg.com

Borden Ladner Gervais